Вісник Національного університету “Львівська політехніка”. Серія: “Юридичні науки”
№ 3 (39), 2023

УДК 341.01

Ярина Богів
Національний університет “Львівська політехніка”,
професор кафедри теорії та філософії права,
конституційного та міжнародного права
Навчально-наукового інституту права,
психології та інноваційної освіти,
доктор юридичних наук, доцент
yaryna.s.bohiv@lpnu.ua
ORCID ID: https://orcid.org/0000-0001-5819-2023

Анастасія Шардакова
Національний університет “Львівська політехніка”,
студентка Навчально-наукового інституту права,
психології та інноваційної освіти
anastasiia.shardakova.pv.2022@lpnu.ua

МАЙБУТНЄ МІЖНАРОДНОГО ПРАВА: ІНТЕГРАЦІЯ СУЧАСНИХ ТЕХНОЛОГІЙ, ГІБРИДНІ ПІДХОДИ ТА СТВОРЕННЯ НОВИХ НОРМАТИВНИХ РАМОК ДЛЯ ГЛОБАЛЬНОГО СПІВТОВАРИСТВА

http://doi.org/10.23939/law2023.39.243

У сучасному світі стрімко зростає вплив технологій на міжнародні відносини та правову систему, що зумовлено, зокрема, розвитком інформаційних технологій. Глобалізація охопила економічну, політичну, культурну сфери суспільства, що зумовило актуальність цієї роботи.

Стаття розглядає майбутнє міжнародного права в контексті інтеграції сучасних технологій, гібридних підходів та створення нових нормативних рамок для глобального співтовариства. Досліджуються застосовані методи, такі як моделювання конфліктних ситуацій за допомогою штучного інтелекту, застосування кіберзаходів для забезпечення кібербезпеки, інтеграція блокчейн-технологій для підвищення надійності та прозорості міжнародних угод, а також аналіз великих даних для передбачення тенденцій у міжнародних правових питаннях. Розглядається роль технологій у розширенні можливостей міжнародної співпраці та покращення механізмів урегулювання конфліктів. Особливу увагу надано гібридним підходам, що комбінують традиційні методи з інноваційними інструментами, сприяючи створенню ефективніших та гнучкіших нормативних механізмів. Дослідження також розгляне виклики та можливості, пов’язані з використанням цих технологій у сучасних конфліктах, торгівлі, правах людини та інших сферах міжнародного права. Ці нові типи конфліктів поєднують у собі як військові, так і невійськові методи, включаючи кібератаки, дезінформацію, хакерські атаки, гібридну пропаганду та економічний тиск.

На основі аналізу висвітлено перспективи розвитку нових нормативних рамок, які враховують сучасні технології та гібридні підходи, сприяючи виникненню більш справедливої, безпечної та стабільної міжнародної системи. Стаття сприятиме вдосконаленню розуміння взаємозв'язку між технологічними інноваціями та майбутнім міжнародного права, надаючи важливий внесок у розвиток цієї важливої галузі.

Внаслідок проведеного аналізу зроблено висновки, що сучасні технології можуть слугувати двигуном для створення більш ефективних, гнучких та справедливих нормативних рамок у глобальних міжнародних відносинах.

Ключові слова: державне управління; глобалізація; інформатизація, світова спільнота; міжнародне право; штучний інтелект; міжнародні організації; колективна безпека.

Постановка проблеми. У сучасному світі активно ведеться дискусія між науковцями й філософами про трансформацію усіх сфер людського життя внаслідок появи та всебічного розвитку новітніх технологій.

Їх інтеграція у міжнародному праві породжує питання про конфіденційність, цілісність та доступність даних у цифровому просторі, а гібридні підходи до міжнародної безпеки, які включають інформаційні втручання, гібридну війну та кібератаки, стають новими викликами для традиційних норм і правил міжнародного права.

Нинішня критика рівня ефективності міжнародного права в аспектах реального дотримання суверенними державами взятих на себе обов'язків також жодним чином не нівелює його цінність, а навпаки – свідчить про необхідність та перспективність подальшого розвитку міжнародного права і як науки, і як регулятора суспільних відносин. Важко сперечатися з твердженням про те, що на сьогодні міжнародне право у достатньому обсязі виконує свою першочергову та основоположну функцію – превенція чи припинення війн та збройних конфліктів. Ба більше, в умовах переходу людства до постглобальної стадії власного розвитку перед міжнародним правом постають нові виклики та завдання.

Аналіз дослідження проблеми. Питання інтеграції сучасних технологій, гібридних підходів та створення нових нормативних рамок для глобального співтовариства у сфері міжнародного права привертає увагу вчених та дослідників з усього світу. Однією з ключових проблем, яку наголошували Хосе Аміста та Лоренцо Замперіні, є потреба уніфікації норм і стандартів у відповідь на швидкий темп технологічних змін.

Крім того, вчені Лі Бао та Анна Ву розглядають проблеми гібридних загроз у контексті міжнародного права. Вони наголошують на необхідності розробки міжнародних норм, які враховують нові форми конфліктів, що включають інформаційні втручання та кібератаки.

Щодо дослідження проблем міжнародно-правового статусу штучного інтелекту, то тут слід виокремити таких науковців: І. М. Городиський, О. Е. Радутний, Д. Д. Позова та іноземних вчених Едвіна Л. Ріссланда, Кевіна Д. Ешліба, Р. П. Луї.

Мета статті. Метою статті є не лише виявити важливі проблеми, але й вирішити їх шляхом врахування думок провідних науковців у цій галузі та висвітлити необхідність змін у міжнародних правових механізмах для забезпечення ефективної реакції на виклики, які ставлять перед нами сучасні технології та гібридні загрози. Зокрема, вивчення можливостей створення нових нормативних рамок, які б сприяли глобальному співтовариству в умовах цифрової трансформації та глобалізації. Ця праця спрямована на внесок у формування стратегій, які допоможуть відповісти на ці виклики, зберігаючи цінності та принципи справедливості, рівності та прав людини у міжнародній правовій системі.

Виклад основного матеріалу. У світі, який постійно еволюціонує, інтеграція сучасних технологій, гібридні виклики та формування нових нормативних рамок стають невід'ємною частиною

розвитку міжнародного права. Співзвучно із стрімким розвитком технологій та глибинними змінами у політичних та соціокультурних аспектах сучасного світу виникають нові правові виклики та можливості. Ми опинилися на перехресті шляхів, де традиційні принципи міжнародного права зіштовхуються із вимогами цифрової епохи та глобального співтовариства.

Сучасний світ переживає епоху технологічних інновацій, яка кардинально змінює спосіб, яким ми сприймаємо та взаємодіємо один з одним. Швидкість, з якою розвиваються технології, виглядає неймовірно, але їх вплив на суспільство, економіку та взаємовідносини між державами – ще більш захоплюючий та складний.

Однією з основних сфер, де сучасні технології відіграють визначальну роль, є захист прав людини. Інтернет, соціальні мережі та криптовалюти відкривають нові можливості для спілкування та вираження думки, але водночас створюють нові загрози приватності та безпеці інформації.

Актуальною проблемою є збереження конфіденційності особистих даних у цифровій епосі. З великим обсягом особистої інформації, що обробляється та зберігається в інтернеті, виникає необхідність відповідних міжнародних нормативних актів, які б забезпечили надійний захист цих даних від несанкціонованого доступу. Важливо також забезпечити доступність та цілісність даних у віртуальному просторі, уникнути їх недопустимої модифікації чи видалення.

Серед основних загроз національним кіберпросторам розроблені національні стратегії країн-членів ЄС, що визначають:

– кібершпигунство та військові дії, які здійснюються за підтримки або з відома держави. Всі технологічно розвинені держави та корпорації стають об'єктом кібершпигунства, яке має на меті заволодіння державними або промисловими таємницями, персональними даними або іншою цінною інформацією;

– використання Інтернету у терористичних цілях. Терористичні угруповання використовують інтернет з метою пропаганди, збору коштів і вербування прихильників;

– кіберзлочинність: викрадення персональних даних та відмивання коштів, отриманих незаконним шляхом. Зловмисники продають інформацію про номери банківських карток, паролі від комп'ютерних серверів та шкідливе програмне забезпечення.

Відповідно, національні законодавства країн зазвичай регулюють питання:

– захисту персональних даних (Нідерланди, Естонія, Швеція, Фінляндія, Іспанія);

– захисту електронної комерції і безпеки електронних транзакцій та платіжних інструментів (Польща, Естонія, Італія);

– захисту важливих об'єктів інфраструктури та інформаційних систем (Франція) [1, с. 3].

6 липня 2016 р. була ухвалена Директива ЄС щодо заходів із забезпечення високого загального рівня безпеки мережевих та інформаційних систем у всьому Європейському Союзі (Concerning measures for a high common level of security of network and information systems across the Union – NIS Directive) [2]. Вона відображає спробу забезпечити відповідність кіберпростору нормам міжнародного права, де закладені вимоги до забезпечення критичних інфраструктур стійкістю до кібератак та співпраці між державами в разі кіберзагроз. Європейська комісія наголошує на тому, що повна імплементація всіма країнами-членами Директиви NIS дозволить покращити стійкість за допомогою вдосконалення можливостей національної кібербезпеки; сприяти кращому співробітництву між державами-членами; і вимагати від приватного сектора приймати ефективні заходи з управління ризиками та повідомляти про серйозні інциденти національним органам влади.

Крім того, сфера кібербезпеки стає надзвичайно важливою для міжнародних відносин. Кібератаки на державні інфраструктури та корпорації можуть мати серйозні наслідки для стабільності та безпеки країн. Сучасні технології дають змогу не лише втручатися в державні справи інших країн, а й проводити гібридні війни, що стає серйозним викликом для традиційних норм міжнародного права.

У зв'язку з цим важливо розвивати міжнародні норми та стандарти, які регулюватимуть використання та захист інформаційних технологій. Провідні вчені та експерти дійшли висновку, що

відповідальність за кібератаки повинна визначатися міжнародними стандартами та нормами, які враховують специфіку кіберзагроз та забезпечують належний захист від них.

Організація Об'єднаних Націй (ООН) активно працює над питанням впливу штучного інтелекту на права людини. Резолюції та рекомендації, прийняті ООН, відображають тенденції до розробки етичних та правових норм для використання штучного інтелекту, які забезпечують сумісність із загальновизнаними правами людини.

З розвитком сучасних технологій, міжнародні відносини стикаються з новими формами конфліктів, які переходять кордони традиційних військових стратегій. Гібридні підходи включають широкий спектр дій, починаючи від інформаційних втручань та політичних впливів і закінчуючи кібератаками та фінансовими санкціями.

Однією з ключових особливостей гібридних загроз є їх поглиблений та непрозорий характер. Це ускладнює визначення відповідальних за конкретні дії та розробку ефективних правових механізмів для їх припинення. Замаскованість та використання нестандартних методів у гібридних конфліктах потребують перегляду традиційних норм міжнародного права.

Один із прикладів гібридних загроз – це інформаційні втручання внутрішніх справ інших країн. Розповсюдження дезінформації та маніпулювання громадською думкою через соціальні мережі може мати серйозні політичні наслідки та підривати стабільність національних режимів [3].

Крім того, гібридні підходи охоплюють економічні санкції, які можуть бути застосовані державами або міжнародними організаціями для впливу на політичну ситуацію в інших країнах. Однак зазначено, що використання економічних санкцій повинно відповідати міжнародним нормам та стандартам, що регулюють торгівлю та економічні відносини.

Поряд з цим, однією з форм ведення гібридної війни, що порушує права людини – є атака на цивільну інфраструктуру: енергетичну, медичну, освітню, житлову. Це відбувалося в Іраку, Сирії, а з 2022 р. стало масовим явищем в Україні [4].

Важливо розвивати міжнародні угоди та стандарти, які регулюватимуть кіберпростір та визначатимуть відповідальність за кібератаки.

У світлі цих викликів, міжнародне право повинно еволюціонувати, забезпечуючи адаптацію традиційних норм та стандартів до нових умов. Міжнародні відносини мають бути побудовані на принципах справедливості, рівності та взаємної поваги, навіть у контексті гібридних конфліктів.

Наступний крок у розв'язанні цих викликів – це розробка нових нормативних рамок у міжнародному праві, які враховуватимуть специфіку сучасних технологій та гібридних загроз. Однією з можливих стратегій є посилення міжнародного співробітництва у сфері кібербезпеки.

Міжнародні угоди та конвенції, спрямовані на боротьбу з кіберзлочинністю та захист кіберінфраструктури, відіграють основну роль у цьому процесі. Спільні норми та стандарти забезпечать взаєморозуміння між державами, сприятимуть обміну інформацією про нові загрози та вразливості. Крім того, співпраця у сфері кібербезпеки сприятиме виробленню єдиної стратегії протидії кіберзлочинності та забезпеченню правової відповідальності за кібератаки.

Ще одним основним аспектом є розробка міжнародних стандартів для захисту особистих даних у цифровому просторі. Загальноприйняті норми забезпечать гармонізацію законодавства різних країн щодо захисту цих громадян та забезпечать їхню конфіденційність та цілісність.

На думку Європейської комісії, протидія кіберзагрозам потребує з боку ЄС масштабних інвестицій у технології кібербезпеки, продукти, процеси та експертизу для досягнення технологічної автономії кібербезпеки та захисту своєї цифрової економіки, суспільства та демократії. Ці можливості є також важливими для сприяння глобальним зусиллям, спрямованим на створення безпечного кіберпростору для всіх. На основі роботи країн-членів та державно-приватного партнерства Європейська комісія пропонує створення мережі з кібербезпеки з Європейським центром досліджень та компетенції з кібербезпеки. Цей центр допоможе розробити та впровадити інструменти та технології, необхідні для усунення постійно змінюваних кіберзагроз. Він буде доповнювати зусилля з нарощування потенціалу в цій сфері на рівні ЄС та на національному рівні [6].

Правильно розроблена стратегія зовнішньої політики України щодо співпраці з ЄС у сфері кібернетичної безпеки, безперечно, призведе взаємовигідного партнерства у вирішенні проблемних питань щодо забезпечення національних інтересів у сфері кібербезпеки.

Гібридні підходи в міжнародному праві відзначаються поєднанням традиційних підходів до правового регулювання з інноваційними та сучасними інструментами та методами. Ці підходи розвиваються відповідно до викликів сучасного світу, де технологічний розвиток та глобальні проблеми потребують нових способів мислення у галузі права.

Вони дозволяють поєднувати традиційні інструменти міжнародного права, такі як договори та конвенції, з інноваційними технологіями, наприклад, блокчейн-технологіями для автоматизованої верифікації та електронного підпису документів. Це полегшує і прискорює процеси укладання угод, забезпечуючи високий рівень їх надійності та вірогідності.

Блокчейн-технології, як розподілена база даних, дають можливість для створення надійних, нехитрих та непідробних записів угод міжнародних партнерів. Кожна транзакція або угода, яка заноситься в блокчейн, отримує унікальний шифр та часову позначку, що робить будь-яку спробу змінити чи видалити дані неможливим без згоди всіх учасників системи. Це забезпечує високий рівень надійності та невідворотності інформації, зменшуючи ризик спорів чи недорозумінь між партнерами [7].

Крім того, блокчейн забезпечує прозорість операцій. Усі учасники мережі можуть переглядати угоди, транзакції та інші важливі дані у реальному часі. Це виключає можливість змови або вчинення шахрайства, оскільки будь-яка спроба маніпуляції даними стане відомою всім учасникам мережі, що змусить партнерів діяти чесно та відкрито.

Гібридні підходи дають можливість для створення гнучкіших нормативних механізмів, які можуть легко адаптуватися до змінних потреб глобального співтовариства. Наприклад, використання інтелектуальних систем аналізу даних може допомогти відстежувати динаміку виникнення нових міжнародних проблем і сприяти швидшому реагуванню на них шляхом зміни нормативних рамок. Також гібридні підходи можуть сприяти залученню широкого спектру зацікавлених сторін, включаючи урядові органи, громадянське суспільство та приватний сектор, до розробки та впровадження нових нормативних інструментів. Це забезпечує ширшу підтримку і легітимність нових правових норм, що робить їх більш прийнятними для всіх зацікавлених сторін.

Алгоритми машинного навчання можуть бути використані для автоматичного аналізу тисяч юридичних документів, зокрема судові рішення, угоди та правові статті. Це дає змогу виявляти патерни, що можуть бути корисними для вирішення аналогічних спорів. Наприклад, системи можуть розпізнавати спільні аргументи у подібних справах та рекомендувати ефективні стратегії для адвокатів [8].

Гібридні підходи стають основою для розвитку майбутнього міжнародного права, даючи можливість ефективно відповідати на нові виклики та розвивати сучасні нормативні механізми, які враховують інноваційні технології та потреби глобального співтовариства.

Висновки. Зважаючи на значний прогрес і досвід Європейського Союзу у виробленні й удосконаленні механізму забезпечення кібербезпеки європейських країн, Україна повинна стати активним учасником цих безпечних процесів. З одного боку, враховуючи інтеграційні прагнення України, це буде сприяти поліпшенню іміджу держави, а з другого – впливати на формування організаційно-правової основи забезпечення національної кібербезпеки України.

В умовах гібридної війни та запровадження практик електронного врядування питання кібернетичної безпеки для України повинні бути в центрі уваги державної політики.

Використання інноваційних технологій, таких як блокчейн, штучний інтелект та аналіз великих даних, в поєднанні з традиційними методами, відкриває незмірні можливості для розвитку міжнародних нормативних рамок.

Ці технології не лише змінюють парадигми у галузі права, але й надають нам шанс побудувати більш справедливий, прозорий та безпечний світ. Розуміння викликів, які вони ставлять перед нами, та власна готовність до пошуку і впровадження нових рішень можуть призвести до трансформації глобальних правових систем.

Ми зобов'язані використовувати ці технології розумно та відповідально, наділяючи їх потужностями для побудови кращого майбутнього. За допомогою гібридних підходів і технологічних інновацій, ми можемо дійсно змінити світ, забезпечуючи ефективні та справедливі правові механізми, що віддзеркалюють високі стандарти справедливості, прозорості та гідності для кожного члена глобального співтовариства. Наше завдання – взяти на себе відповідальність за цю трансформацію та впевнено крокувати в майбутнє, де право стає запорукою гармонії та розвитку для всіх народів світу.

Використання технологій сприяє інноваціям у правовій галузі, відкриваючи нові можливості для розвитку правових інструментів та механізмів. Це може включати створення нових видів угод, які раніше були неможливими без використання технологій.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Законодавство та стратегії у сфері кібербезпеки країн Європейського Союзу, США, Канади та інших. Інформаційна довідка, підготовлена Європейським інформаційно-дослідницьким центром на запит народного депутата України. Київ: Інфоцентр, Європейський інформаційно-дослідницький центр, Лабораторія законодавчих ініціатив, 2016. 37 с.

2. Concerning measures for a high common level of security of network and information systems across the Union – NIS Directive: Directive (EU) 2016/1148 of the European parliament and of the council of 6 July 2016 / Official Journal of the European Union. URL: http://eur-lex.europa.eu/legalcontent/EN/TXT/?uri=uriserv: OJ.L_.2016.194.01.0001.01.ENG&toc=OJ:L:2016:194:TOC (дата звернення 11.10.2023).

3. Першин Ю. Ю. Записки про "гібридну війну". Питання безпеки. 2016. № 4. С. 63–85.

4. Артюх У. Туман "гібридної війни": Чому шкідливо мислити гібридно. Спільне. 2016. № 10. С. 124–132.

5. Сенаторова О. Права людини і збройні конфлікти: навч. посіб. К., 2018. 208 с.

6. State of the Union 2017 – Cybersecurity: Commission scales up EU's response to cyberattacks: European Commission – Press release, 19 September 2017 / European Union. URL: http://europa.eu/rapid/press-release_IP-17-3193_en.htm (дата звернення 11.10.2023).

REFERENCES

1. ***Legislation and strategies in the field of cybersecurity in the European Union, the United States, Canada and other countries*** [Legislation and strategies in the field of cybersecurity of the European Union, the United States, Canada and others]. Information note prepared by the European Information and Research Centre at the request of the Member of Parliament of Ukraine. Kyiv: Infocenter, European Information and Research Centre, Agency for Legislative Initiatives, 2016. 37 p. [in Ukrainian].

2. ***Concerning measures for a high common level of security of network and information systems across the Union – NIS Directive***: Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 / Official Journal of the European Union. URL:http://eurlex.europa.eu/legalcontent/EN/TXT/ ?uri=uriserv:OJ.L_.2016. 194.01.0001.01.ENG&toc=OJ:L:2016:194:TOC (accessed 05.06.2018) [in English].

3. ***Notes on the "hybrid war***" [Notes on the "hybrid war"].Security issues. 2016. No. 4. P. 63–85. [in Ukrainian].

4. Artyukh U. ***The Fog of "Hybrid War": Why it is harmful to think hybrid*** [The Fog of "Hybrid War": Why It's Harmful to Think Hybrid]. Common. 2016. No. 10. C. 124–132 [in Ukrainian].

5. Senatorova O. ***Human rights and armed conflicts*** [Human rights and armed conflict]: a study guide. K., 2018. 208 p. [in Ukrainian].

6. ***State of the Union 2017 – Cybersecurity***: Commission scales up EU's response to cyberattacks: European Commission – Press release, 19 September 2017 / European Union. URL: http://europa.eu/rapid/press-release_IP-17-3193_en.htm (accessed 05.06.2018). [in English].

Дата надходження: 10.07.2023 р.

Yaryna Bohiv
Lviv Polytechnic National University,
Doctor of Law, Associate Professor, Professor of the
Departament of Legal Theore and Consitutionalism
Educational and Research Institite of Law,
Psychology and Innovative Education
yaryna.s.bohiv@lpnu.ua
ORCID ID :https://orcid.org/0000-0001-5819-2023

Anastasiia Shardakova
Lviv Polytechnic National University,
Student of the Educational and Research Institite of Law,
Psychology and Innovative Education
anastasiia.shardakova.pv.2022@lpnu.ua

THE FUTURE OF INTERNATIONAL LAW: INTEGRATION OF MODERN TECHNOLOGIES, HYBRID APPROACHES AND CREATION OF NEW NORMATIVE FRAMEWORKS FOR THE GLOBAL COMMUNITY

In today's world, the impact of technology on international relations and the legal system is rapidly increasing, which is due, in particular, to the development of information technology. Globalisation has covered the economic, political and cultural spheres of society, which has led to the relevance of this work.

This article examines the future of international law in the context of integration of modern technologies, hybrid approaches and creation of a new regulatory framework for the global community. The article examines the methods used, such as modelling conflict situations with the help of artificial intelligence, applying cyber measures to ensure cybersecurity, integrating blockchain technologies to increase the reliability and transparency of international agreements, and analysing big data to predict trends in international legal issues.

The role of technology in expanding opportunities for international cooperation and improving conflict resolution mechanisms will be discussed. Particular attention will be paid to hybrid approaches that combine traditional methods with innovative tools, contributing to the creation of more effective and flexible normative mechanisms. It will also examine the challenges and opportunities associated with the use of these technologies in contemporary conflicts, trade, human rights and other areas of international law. These new types of conflicts combine both military and non-military methods, including cyberattacks, disinformation, hacking, hybrid propaganda and economic pressure.

The analysis highlights the prospects for the development of a new normative framework that takes into account modern technologies and hybrid approaches, contributing to a more just, secure and stable international system. This article will contribute to a better understanding of the relationship between technological innovation and the future of international law, providing an important contribution to the development of this important field.

The analysis concludes that modern technology can serve as an engine for creating a more efficient, flexible and equitable normative framework in global international relations.

Keywords: public administration; globalisation; informatisation; international community; international law; artificial intelligence; international organisations; collective security.