Вісник Національного університету “Львівська політехніка”. Серія: “Юридичні науки”
№ 4 (44), 2024

УДК 341.3:316.42

Олександра БЕЛІЧЕНКО
Національний університет “Львівська політехніка”,
асистентка кафедри теорії права та конституціоналізму
Навчально-наукового інституту права,
психології та інноваційної освіти,
доктор філософії за спец. 081 Право
oleksandra.v.belichenko@lpnu.ua
ORCID: 0000-0001-9423-0488

КОНВЕРГЕНЦІЯ ГЛОБАЛІЗАЦІЇ ПРАВОВОГО ПРОСТОРУ ТА КІБЕРЗЛОЧИННОСТІ

http://doi.org/10.23939/law2024.44.008

Анотація. У статті проведений аналіз проявів, поширення та ролі кіберзлочинності у сучасному глобалізованому суспільстві. Глобалізація світу розглядається як результат розвитку інформаційних технологій, особливо при використанні кіберпростору як електронного комунікаційного середовища для поширення інформації по всьому світу.

Умотивовано, що технічний прогрес, який є результатом діяльності людини і культури, окрім позитивного впливу, у тому сенсі, що використовується на благо людства, також негативно впливає на розвиток людини та цивілізації загалом, а саме: збереження слабких сторін соціально-правової комунікації (вразливостей), які є безумовно, дуже небезпечними. Глобалізація правового простору через розвиток технологій принесла багато позитивів у реалізації громадянином прав та законних інтересів. Серед негативних проявів є загроза виникнення і значного поширення злочинності у віртуальному середовищі, яке стало реальністю світової спільноти, відоме як кіберзлочинність.

Конвергенція глобалізації правового простору та кіберзлочинності вказує на необхідність розробки уніфікованих правових стандартів для ефективної боротьби з кіберзлочинами у глобальному масштабі. Оскільки кіберзлочинність не має географічних кордонів, національні правові системи часто не здатні впоратися з новими викликами, що виникають у кіберпросторі. Глобалізація потребує гармонізації законодавства різних країн, а також міжнародної співпраці, щоб створити спільну базу для протидії кіберзлочинності. Це допоможе не тільки забезпечити правовий захист на світовому рівні, але й зміцнить координацію зусиль між державами у цій сфері.

У висновку авторкою зазначається, що концептуалізація кіберзлочинності є складною задачею, оскільки швидкий розвиток технологій, таких як штучний інтелект, вносить нові виклики у сферу кібербезпеки та правопорядку. Потрібна єдина та узгоджена система класифікації, яка враховуватиме всі аспекти цих злочинів та їх вплив на суспільство. Розробка таких підходів має базуватися на міждисциплінарному

співробітництві та врахуванні різних точок зору учасників, від нормотворців до правоохоронних органів, щоб досягти ефективного реагування на кіберзлочинність.

Ключові слова: глобалізація; злочинність; віртуальний простір; кіберзлочинність; глобальні проблеми; правове регулювання; національне право.

Постановка проблеми. В епоху глобалізації інформаційні технології відіграють дуже важливу роль у державі, економіці та суспільстві, оскільки опановуючи технології та інформацію, країна має достатній капітал, щоб стати переможцем у глобальній конкуренції. Життя сучасного суспільства, особливо після коронавірусної пандемічної загрози, почало зазнавати дуже великих змін та надстрімких витків.

Досягнення технологій та інформації, які зумовлені появою інтернету, і є результатом технологічної революції, що синергетично співпрацює зі всіма технологічними та інтелектуальними досягненнями, у своєму розвитку викликали швидкі зміни в структурі суспільства від аграрної до індустріальної ери, згодом від індустріальної до інформаційної, що зрештою принесла і створила нові моделі, парадигми, ідеології та стилі життя. Сьогодні інформаційні технології є однією з основних частин людського буття. Тому зараз, в епоху глобалізації, якщо у людини відсутнє володіння інформаційними технологіями, то це є синонімом неписьменності.

Право, правова реальність, механізм та апарат держави повинні прилаштовуватися до таких змін. Тому вагомим є дослідження окремих проявів глобалізації через глобальну правову зміну окремих явищ, серед яких віртуальна реальність та злочинність.

Аналіз дослідження проблеми. Проблема глобалізації та правової глобалістики, впливу глобального на право й правову ідентичність було предметом аналізу багатьох науковців, зокрема В. Ковальчука, І. Жаровської, Н. Ортинської та інших. Аспекти злочинності та їх поширення аналізують представники зазвичай кримінального спрямування, зокрема О. Гумін, В. Ортинський, В. Канцір та інші.

Проте наразі проблема злочинності потребує аналізу крізь призму її поширення у віртуальному просторі, тому проблема є малодослідженою й потребує додаткового аналізу у наукових колах.

Метою статті є аналіз проявів, поширення та ролі кіберзлочинності в сучасному глобалізованому суспільстві.

Виклад основного матеріалу. Розвиток науки і техніки все більше спонукає до відновлення зусиль у використанні технологічних результатів. Інформаційні та комунікаційні технології швидко прогресують та впливають на суспільство та державу як глобально, так і регіонально. Ці розробки зрештою полегшили життя світової спільноти, адже світове співтовариство має доступ до всієї інформації та зв'язку навколо за один клік. Проте розвиток інформації та комунікаційних технологій не тільки приносить позитивний вплив, наприклад, легкий доступ до інформації або до вільного спілкування, але також приносить цілу низку негативних впливів, які можуть загрожувати особі та суверенітету країни. Це можна проілюструвати через численні злочини, які відбуваються у кіберпросторі (кіберзлочинність).

У всі історичні епохи люди завжди шукали зручності для покращення свого життя. Це було досягнуто з просуванням різноманітних технологій, в тому числі інформаційних, а швидкий розвиток технології завжди приносить прогрес майже в усі аспекти людського життя. Ці всі аспекти невіддільні, тому зараз вони навіть не можуть бути відокремленими від технологічних розробок взагалі. Особливо в епоху глобалізації, де різноманітні сервіси, речі та послуги пропонуються або продаються на світовому ринку, так що люди в різних частинах світу можуть мати доступ як до корисного, так і до шкідливого інформаційного контенту та технологій.

Цей процес іноземні науковці називають “меню страв”, де людям постійно дають змінну страву, що провокує їх стати іншою людиною, трансформувати людський стиль, який відповідає цілям глобалізації та її режимам [1]. Ми вважаємо за необхідне також погодитися з таким підходом, оскільки трансформація ролі державного суверенітету та віртуалізація суспільного життя будує нову людську ідентичність через додаткові, трансформовані вимоги до її поведінки, кваліфікації, умов життя.

Класик філософії глобалізації Барбара Паркер розуміє глобалізацію як явище, де зростає відчуття того, що події, які відбуваються в усьому світі, збігаються швидко сформувати єдиний інтегрований світ, де економічні, соціальні, культурні, технологічні, бізнесові та інші впливи перетинають традиційні кордони та межі, такі як нації, національні культури, час, простір і бізнесгалузі з дедалі більшою легкістю. Події в усьому світі набувають все більшого значення, швидко об’єднується, щоб сформувати єдиний глобалізований світ, де економічні, політичні, соціокультурні, технічні, ділові та інші впливи на межі, такі як країни, нації, культури, час, простір і різноманітні галузі бізнесу, напрочуд легко та швидко впливають та розвиваються [2].

Глобалізація – це наслідок, якого не уникнути нікому: ні країні, ні окремій людині, як би цього вони не прагнули. Вона робить світ без кордонів, країни конкурують вільно в різних сферах, а іноді перетинають юрисдикцію країни. Глобалізація світу розглядається як результат розвитку інформаційних технологій, особливо при використанні кіберпростору як електронного комунікаційного середовища для поширення інформації по всьому світу. Відкриття інформаційних технологій легко впливає на країну, як-от національний суверенітет, наприклад, щодо усунення торгових бар'єрів з кримінальними справами в кіберпросторі.

Одним із продуктів науки і техніки є інформаційні технології або широко відомі як телекомунікаційні технології. У своєму розвитку з відкриттям комп’ютера як продукту науки і технології їм все легше вдавалося розповсюдитись навколо, в кожній країні, в кожному домі, адже тепер ми не уявляємо свого життя без них. Потім відбулося зближення між телекомунікаційними технологіями, медіа та комп'ютерними науками. Конвергенція комунікаційних технологій, медіа та комп’ютерів призвело до появи нового інструмент під назвою інтернет.

Глобалізація правового простору через розвиток технологій принесла багато позитивів у реалізації громадянином його прав та законних інтересів. Прикладом є використання інтернет-ЗМІ як засобу підтримки при бронюванні квитків (літак, поїзд), готелів, оплата телефонних рахунків, комунальних платежів, отримання адміністративних послуг, це все зробило для споживачів більш комфортну та безпечну побутову сферу.

Технічний прогрес, який є витвором діяльності людини, поєднує у собі як позитивні, так і негативні аспекти, адже завжди має бути якесь але. Даний прогрес використовується в ідеалі на розвиток людства та його величезних потреб, проте він, на жаль, має і негативний вплив на людину та цивілізацію, адже мотивує підтримання слабких сторін соціальної і правової комунікації, що становить велику загрозу зараз та у майбутньому. Адже тепер великого поширення у світовій спільноті набуває віртуальна злочинність – кіберзлочинність, яка стала одним із розповсюджених видів злочину у світі.

Злочини з використанням технологій, особливо інформаційних (кіберзлочинність), досягли тривожної стадії. Адже досягнення неймовірного розвитку в інформаційних технологіях призводить до правопорушень не лише у фінансовій сфері бізнесу та торгівлі, але водночас в інших сферах, що стосуються порнографії, комп’ютерної злочинності, навіть цифрового тероризму, інформаційних війн та хакерських атак.

Така злочинність має транснаціональний характер, тому потребує належного регулювання, протидії та запобіганню злочинним проявам, приносячи великі проблеми у політичній, економічній, соціальній, культурній, оборонній та безпековій сфері країн. Кіберзлочинність, як вплив глобалізації, що спричиняє багато втрат у зазначених сферах, необхідно долати з урахуванням глобальних проблем. Класична злочинність вирішується шляхом застосування національних

засобів та способів боротьби з нею, нині застосувати такий підхід до кіберзлочинності неможливо. Виключно національним правовим регулюванням вирішити проблему нереально. Це так, як вирішувати проблему глобального потепління виключно зусиллям однієї країни, тобто намарно та безрезультатно. Виявити правопорушника в кіберзлочинності набагато важче, ніж простого злочинця, адже інституційні національні органи не мають достатньо повноважень для реалізації таких дій. Попри те кіберзлочинність має конкретний великий негативний вплив на правопорядок кожної окремої країни, якої це стосується, а не тільки глобалізованого суспільства.

Глобальне проникнення інтернету в різні сфери життя людей зросло приблизно на 7 % протягом одного року (з січня 2020 року по січень 2021 року) [3]. Стрімке впровадження цифрових технологій спричинило еволюцію злочинної поведінки, що призвело до збільшення кількості кіберзлочинів. Однак залишається незрозумілим, що саме є кіберзлочинністю.

Більше ніж два десятки років тому були здійснені спроби правового регулювання проблеми кіберзлочинності. Конвенція про кіберзлочинність (ETS № 185) є першим міжнародним договором про злочини, вчинені через інтернет та інші комп’ютерні мережі, зокрема щодо порушень авторського права, комп’ютерного шахрайства, дитячої порнографії та порушень безпеки мережі. Він також містить низку повноважень і процедур, таких як пошук комп’ютерних мереж і перехоплення. Його головною метою, викладеною в преамбулі, є проведення спільної кримінальної політики, спрямованої на захист суспільства від кіберзлочинності, особливо шляхом прийняття відповідного законодавства та сприяння міжнародному співробітництву.

На сьогодні не існує узгодженого розуміння поняття кіберзлочинності, проте загалом погоджено класифікацію таких дій. Вони репрезентуються у наступному: незаконний доступ (навмисний вхід або доступ до комп'ютерної системи без дозволу); незаконне перехоплення (навмисне та незаконне підслуховування або захоплення таємної інформації); втручання в дані (навмисна зміна чи видалення комп’ютерних даних без дозволу); втручання в систему (навмисне несанкціоноване втручання або серйозне втручання у функціонування комп'ютерної системи); неправомірне використання пристроїв, а саме: неправомірне використання комп’ютерної техніки, в т.ч. комп'ютерні програми, комп'ютерні паролі, коди доступу; фальсифікація (умисне та без права введення, зміни, видалення автентичних даних, неавтентичні з наміром використовувати їх як справжні дані); комп'ютерне шахрайство (умисні незаконні дії, що спричиняють втрату благ/багатства шляхом проникнення, зміни, видалення комп’ютерних даних або втручання в роботу функціонування комп’ютерів/комп’ютерних систем з метою отримання економічної вигоди для себе чи інших); злочини, пов’язані з контентом, наприклад проти дітей (поширення дитячої порнографії); правопорушення, пов’язані з порушенням авторського права і суміжних прав, а саме: правопорушення, пов’язані з порушенням авторських прав [4].

Проте така класифікація, як і розуміння потребують постійного оновлення, оскільки в контексті появи нових можливостей штучного інтелекту. Наприклад, Deepfakes або злочини на основі штучного інтелекту можуть використовуватися у різних правопорушеннях.

Також іноземні дослідники вказують на ще одну концептуальну проблему – жодна система класифікації повністю не включала б концепції кіберзлочинності чи точно відображала туманну природу кіберзлочинних діянь. Крім того, широко поширені системи класифікації, як правило, є одновимірними та чітко розрізняють типи кіберзлочинів, у той час як кіберзлочинну та кібердевіантну поведінку, можливо, краще концептуалізувати як існуючу у спектрі. Наразі залишається невизначеність щодо того, що саме є кіберзлочинністю, і концептуалізація кіберзлочинності, ймовірно, і надалі буде проблемою.

Розробка чіткої концептуалізації кіберзлочинності необхідна не тільки для окреслення проблеми, але й для оцінки її впливу на суспільство та розробки ефективних правових і політичних заходів реагування. Для ефективної класифікації поточної та нової поведінки кіберзлочинців необхідна всеохоплююча система класифікації, сумісна з міжнародним і національним законодавством або політикою та злагодженою роботою державного та приватного секторів

кібербезпеки [5]. Труднощі з класифікацією кіберзлочинності перешкоджають запровадженню законів і нормативних актів, що стосуються кіберзлочинності, що, у свою чергу, може створити додаткові проблеми для контролю за кіберзлочинністю через обмежені можливості реагування.

Проаналізувавши пропозиції іноземних науковців та чинне міжнародне регулювання кіберзлочинності, вважаємо за необхідне змінити методологічний підхід у її розв'язанні, акцентувавши увагу на проведенні цілісної глобальної політики протидії та підлаштуванні національної практики під всезагальні вимоги та принципи запобігання та протидії негативним явищам у віртуальному просторі.

Для цього серед іншого необхідні наступні удосконалення та зміни:

По-перше, для ефективної боротьби з кіберзлочинністю необхідно розробити та прийняти універсально узгоджене визначення, яке надає ключову термінологію та сферу застосування, а також "стандартизований метод класифікації кіберзлочинності" (як його називає S. Broadhead [6]) для гармонізації майбутнього прийняття рішень. Запровадження спільної мови стане ключовою особливістю загального визнання концепцій кіберзлочинності, які відповідають міжнародним договорам, а також національному законодавству та політиці.

По-друге, розширеного міждисциплінарного та багатоюрисдикційного підходу, який охоплює ключові зацікавлені сторони на міжнародному та локальному рівнях. Ключові зацікавлені сторони, наприклад, включають нормотворців, галузеві розвідувальні служби та служби безпеки, правоохоронні органи, державний сектор та науковців. Співпраця між цими основними дійовими особами має вирішальне значення для оцінки сталості та ефективності комплексної та цілісної системи класифікації кіберзлочинів.

По-третє, майбутні системи класифікації мають застосовувати підхід на основі спектру, щоб точно відобразити складність злочинів у кіберпросторі та еволюцію поведінки кіберзлочинців. Крім того, науковці вказують, щоб уникнути надто спрощених і редукційних систем класифікації, слід враховувати додаткові визначальні характеристики [7] (наприклад, характеристики злочинців, характеристики жертв, злочинні мотиви та наслідки злочинів).

Висновки. Конвергенція глобалізації правового простору та кіберзлочинності вказує на необхідність розробки уніфікованих правових стандартів для ефективної боротьби з кіберзлочинами у глобальному масштабі. Оскільки кіберзлочинність не має географічних кордонів, національні правові системи часто не здатні впоратися з новими викликами, що виникають у кіберпросторі. Глобалізація потребує гармонізації законодавства різних країн, а також міжнародної співпраці, щоб створити спільну базу для протидії кіберзлочинності. Це допоможе не тільки забезпечити правовий захист на світовому рівні, але й зміцнить координацію зусиль між державами у цій сфері.

Концептуалізація кіберзлочинності є складною задачею, оскільки швидкий розвиток технологій, таких як штучний інтелект, вносить нові виклики у сферу кібербезпеки та правопорядку. Потрібна єдина та узгоджена система класифікації, яка враховує всі аспекти цих злочинів та їх вплив на суспільство. Розробка таких підходів має базуватися на міждисциплінарному співробітництві та врахуванні різних точок зору учасників, від нормотворців до науковців, служб безпеки установ та організацій і правоохоронних органів, щоб досягти ефективного реагування на кіберзлочинність.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Siregar G., Sinaga S. (2021). The law globalization in cybercrime prevention. International Journal of Law Recontruction. Vol. 5, No. 2, September. DOI : http://dx.doi.org/10.26532/ijlr.v5i2.17514 (Accessed: 11.09.2024)

2. Parker B. (1997). Evolution and Revolution from International Business to Globalization in Hand Book of Organization Studies, London, P. 67.

3. Kemp S. (2021). Digital 2021: Global Overview Report. URL: https://datareportal.com/reports/digital-2021-global-overview-report (Accessed: 11.09.2024)

4. The Convention on Cybercrime (Budapest Convention, ETS No. 185) and its Protocols. Retrieved from: https://www.coe.int/en/web/cybercrime/the-budapest-convention (Accessed: 11.09.2024)

5. Akdemir N., Sungur B., Başaranel B.U. (2020). Examining the Challenges of Policing Economic Cybercrime in the UK. *Güvenlik Bilimleri Derg. (Int. Secur. Congr. Spec. Issue), Özel Sayı*, pp. 113–134.

6. Broadhead S. (2018). The contemporary cybercrime ecosystem: A multi-disciplinary overview of the state of affairs and developments. *Comput. Law Secur. Rev.*, *34*, pp. 1180–1196.

7. Marcum, C.D.; Higgins, G.E. (2019). Cybercrime. In *Handbooks of Sociology and Social Research*, 2nd ed.; Krohn, M.D., Hendrix, N., Hall, G.P., Lizotte, A.J., Eds.; Springer: Cham, Switzerland, pp. 459–475.

REFERENCES

1. Siregar G., Sinaga S. (2021). ***The law globalization in cybercrime prevention. International Journal of Law Recontruction.*** Vol. 5, N.2. DOI : http://dx.doi.org/10.26532/ijlr.v5i2.17514 (Accessed: 11.09.2024) [In English]

2. Parker B. (1997). ***Evolution and Revolution from International Business to Globalization in Hand Book of Organization Studies***, London, P. 67. [In English]

3. Kemp S. (2021). Digital 2021: ***Global Overview Report. Retrieved from:*** https://datareportal.com/reports/digital-2021-global-overview-report (Accessed: 11.09.2024) [In English]

4. ***The Convention on Cybercrime*** (Budapest Convention, ETS No. 185) and its Protocols. (2001). Retrieved from: https://www.coe.int/en/web/cybercrime/the-budapest-convention (Accessed: 11.09.2024). [In English]

5. Akdemir N., Sungur B., Başaranel B. U. (2020). ***Examining the Challenges of Policing Economic Cybercrime in the UK. Güvenlik Bilimleri Derg***. (Int. Secur. Congr. Spec. Issue), Özel Sayı, pp. 113–134. [In English]

6. Broadhead S. (2018). ***The contemporary cybercrime ecosystem: A multi-disciplinary overview of the state of affairs and developments.*** Comput. Law Secur. Rev. 34, pp. 1180–1196. [In English]

7. Marcum, C. D.; Higgins, G. E. Cybercrime. (2019). ***In Handbooks of Sociology and Social Researc***h, 2nd ed.; Krohn, M. D., Hendrix, N., Hall, G. P., Lizotte, A. J., Eds.; Springer: Cham, Switzerland, pp. 459–475. [In English]

Дата надходження статті: 16.09.2024 р.

Oleksandra BELICHENKO
Lviv Polytechnic National University,
Educatinoal and Rasearch Institute of Law,
Psychology and Innovative Education,
Assistan Professor of the Theory of Law
and Constitutionalism Department,
Ph.D. in Law
oleksandra.v.belichenko@lpnu.ua
ORCID: 0000-0001-9423-0488

CONVERGENCE OF GLOBALIZATION OF LEGAL SPACE AND CYBERCRIME

Abstract. The article analyzes the manifestations, spread and role of cybercrime in modern globalized society. The globalization of the world is considered as a result of the development of information technologies, especially when using cyberspace as an electronic communication medium for the dissemination of information around the world.

It is reasoned that technical progress, which is the result of human activity and culture, in addition to a positive impact, in the sense that it is used for the benefit of humanity, also has a negative

impact on human development and civilization, namely the preservation of the weak sides of socio-legal communication (vulnerabilities), which are definitely very dangerous. Globalization of the legal space due to the development of technologies has brought many positives in the realization of rights and legitimate interests by citizens. Among the negative manifestations is the threat of the appearance and significant spread of crime in the virtual, which has become a reality of the world community, known as cybercrime.

The convergence of the globalization of the legal space and cybercrime indicates the need to develop unified legal standards to effectively combat cybercrime on a global scale. As cybercrime knows no geographical boundaries, national legal systems are often unable to cope with the new challenges emerging in cyberspace. Globalization requires the harmonization of the legislation of different countries, as well as international cooperation to create a common basis for countering cybercrime. This will help not only to ensure legal protection at the global level, but also to strengthen the coordination of efforts between states in this area.

In the conclusion, the author notes that conceptualizing cybercrime is a difficult task, as the rapid development of technologies such as artificial intelligence introduces new challenges to the field of cyber security and law enforcement. A single and coherent classification system is needed that takes into account all aspects of these crimes and their impact on society. The development of such approaches must be based on interdisciplinary collaboration and take into account the different perspectives of actors, from policymakers to academics and law enforcement agencies, to achieve an effective response to cybercrime.

Keywords: globalization; crime; virtual space; cybercrime; global problems; legal regulation; national law.