УДК [343.3/7:004](075.8)
DOI

Сергій ЧВАНКІН
доктор юридичних наук, доцент, голова Асоціації слідчих суддів України,
голова Київського районного суду м. Одеси, вул. Варненська 3б, м. Одеса, Україна, 65080
ORCID: 0000-0002-9800-854X
Scopus Author ID: 58860607900
DOI: 10.32782/LST/2024-1-8

Бібліографічний опис статті: Чванкін, С. (2024). До питання гармонізації законодавства у сфері збирання електронних доказів та протидії кіберзлочинності. *Law. State. Technology*, 1, 52–59, doi: 10.32782/LST/2024-1-8

ДО ПИТАННЯ ГАРМОНІЗАЦІЇ ЗАКОНОДАВСТВА У СФЕРІ ЗБИРАННЯ ЕЛЕКТРОННИХ ДОКАЗІВ ТА ПРОТИДІЇ КІБЕРЗЛОЧИННОСТІ

Статтю присвячено висвітленню питань гармонізації законодавства у сфері збирання електронних доказів та протидії кіберзлочинності.

Метою статті є визначення форм гармонізації законодавства у сфері збирання електронних доказів та протидії кіберзлочинності.

Зазначається, що 95% держав-членів ООН залучені до реформування свого законодавства щодо кіберзлочинності та електронних доказів, однак досі відсутній єдиний міжнародний нормативний акт, який містить комплексне регулювання даної сфери. Крім того, що кожен національний правопорядок формує власний правовий режим електронних доказів, порядок їх збирання та дослідження, паралельно відбуваються процеси унормування даної сфери на міжнародному рівні. Вказується, що державам та міжнародним організаціям притаманний підхід унормування або окремих видів електронних доказів, або конкретної сфери, де такі електронні докази застосовуються, що створює проблеми у міжнародній співпраці, адже законодавство про електронні докази має бути технологічно нейтральним, щоб відповідати технологічним досягненням, що розвиваються, та має бути сумісним із законодавством інших країн.

Відзначається, що процес гармонізації законодавства у сфері збирання електронних доказів та протидії кіберзлочинності відбувається як на міждержавному рівні, так і на регіональному рівні (наприклад Регламент Європейського парламенту та Ради ЄС про європейські ордери на пред'явлення та європейські ордери на збереження електронних доказів у кримінальному провадженні та для виконання покарань у вигляді позбавлення волі після кримінального провадження). Деякі регіональні ініціативи набувають характеру універсальних, прикладом чого є Конвенція про кіберзлочинність (Будапештська конвенція) Ради Європи, до якої приєдналися ще 22 країни, які не є країнами-учасницями Ради Європи (США, Канада, Аргентина тощо). Поряд із цим, відбуваються спроби для врегулювання протидії кіберзлочинності на рівні ООН. Поміж цим, залишаються країни, які не беруть участі в жодному із напрямів гармонізації, що створює ризики використання таких країн як «сірих зон» для кіберзлочинців.

Ключові слова: *кіберзлочинність, електронні докази, гармонізація законодавства, міжнародна співпраця.*

Serhii CHVANKIN
Doctor of legal sciences, associate professor head of the Investigative Judge Association of Ukraine, head of the Kyivskyi District Court of Odesa, 3b, Varnenska str., Odesa, Ukraine, 65080
ORCID: 0000-0002-9800-854X
Scopus Author ID: 58860607900
DOI: 10.32782/LST/2024-1-8

To cite this article: Chvankin, S. (2024). Do pytannia harmonizatsii zakonodavstva u sferi zbyrannia elektronnykh dokaziv ta protydii kiberzlochynnosti [On the issue of harmonization of legislation in the sphere of collecting electronic evidence and combating cybercrime]. *Law. State. Technology,* 1, 52–59, doi: 10.32782/LST/2024-1-8

ON THE ISSUE OF HARMONIZATION OF LEGISLATION IN THE SPHERE OF COLLECTING ELECTRONIC EVIDENCE AND COMBATING CYBERCRIME

The article is dedicated to matters of harmonization of law concerning collection of electronic evidence and cybercrime prevention.

Purpose of the article is to determine forms of harmonization of law concerning collection of electronic evidence and cybercrime prevention.

It is stated that 95% of the UN member states are involved in reforming their law concerning cybercrime and electronic evidence, yet still there is no uniform international regulation containing comprehensive guidelines for this sphere. Each national law enforcement system creates its own legal regime for electronic evidence, procedure for collection and examination thereof, and at the same time processes are in place for standardization of this sphere at the international level. It is further noted that the states and international organizations tend to standardize certain types of electronic evidence or a specific sphere where such electronic evidence is applied, which creates problems in international cooperation, since law on electronic evidence should be technologically neutral in order to keep up with developing technological advances and be compatible with laws of other countries.

It is stated that harmonization of law in the sphere of collection of electronic evidence and cybercrime prevention occurs both at the international and regional levels (for instance, Regulation of the European Parliament and EU Council on European Production Orders and European Preservation Orders for electronic evidence in criminal proceedings and for the execution of custodial sentences following criminal proceedings). Certain regional initiatives acquire universal status, such as the EU Council Convention on Cybercrime (Budapest Convention), joined by 22 countries that are not member states of the European Council (USA, Canada, Argentina, etc.). At the same time there have been attempts to regulate cybercrime prevention at the UN level. And yet, still there are countries that are not involved in any kind of harmonization, which creates risks that such countries will be used as grey zones by cybercriminals.

Key words: *cybercrime, electronic evidence, harmonization of law, international cooperation.*

Постановка проблеми та її актуальність. Гармонізація процесуального законодавства та законодавства про кіберзлочинність сприяє, серед іншого, глобальному збору електронних доказів та обміну ними через міжнародне співробітництво. Оновлений побіжний огляд глобального стану законодавства про кіберзлочинність, підготовлений Офісом програми боротьби з кіберзлочинністю Ради Європи (C-PROC), свідчить про те, що станом на середину грудня 2023 року 95% держав-членів ООН залучені до реформування свого законодавства щодо кіберзлочинності та електронних доказів (The global state of cybercrime legislation 2013–2023, 2023: 3).

Правовий режим та система електронних доказів динамічно розвиваються, однак досі відсутній єдиний нормативний акт, який містить комплексне регулювання даної сфери. І цілком імовірно, що такий акт взагалі не може бути прийнято, адже особливості кожного виду електронних доказів настільки визначальні, що уніфікованого підходу щодо правил створення, зберігання, збирання та подання доказів – не може існувати.

Аналіз останніх досліджень і публікацій. Дослідженню питань гармонізації законодавства щодо електронних доказів та протидії кіберзлочинності присвячені праці А. Борка, О.Волобуєвої, В. Неходченка, І. Хараберюша (Andrii Borko, Vadym Nehodchenko, Olena Volobuieva, Ivan Kharaberiush, Yevheniia Lohvynenko, 2019), Д. Кнітель (Knytel Dagna, 2020), Ш. Шольберга (Stein Schjølberg, 2008), М. Босковіч (Matić Bošković M., 2019) та інших. Але попри наявні численні публікації вчених комплексне вирішення питання правового режиму електронних доказів і досі не вироблено.

Метою статті є визначення форм гармонізації законодавства у сфері збирання електронних доказів та протидії кіберзлочинності.

Виклад основного матеріалу дослідження. Кластерний підхід регулювання правового режиму електронних доказів характерний і законодавству іноземних країн: наприклад, у Китаї система нормативних актів щодо електронних доказів є відносно розпорошеною та заплутаною, а проблема ієрархії законодавства про електронні докази в основному втілюється в трьох аспектах 1) між різними рівнями законодавства про електронні докази бракує координації; 2) відмінність у правовому режимі електронних доказів та практиці їх застосування різними правоохоронними та судовими органами; 3) відсутність уніфікованого спеціального закону (Stein Schjølberg, 2008).

Подібного підходу дотримуються і міжнародні інституції, обираючи для унормування або окремий вид електронного доказу, або конкретну сферу, де такі електронні докази застосовуються: наприклад, Регламент Європейського парламенту та Ради (ЄС) № 910/2014 про електронну ідентифікацію та довірчі послуги для електронних транзакцій на внутрішньому ринку та про скасування Директиви

1999/93/ЄС, Директива Європейського парламенту та Ради (ЄС) 2018/1972 про запровадження Європейського кодексу електронних комунікацій тощо. Прийнявши Директиву 2014/41/ЄС 3 квітня 2014 року, додатково Європейський Парламент і Рада Європейського Союзу намагаються врегулювати міжнародне співробітництво у цій сфері, запровадивши Європейський порядок розслідування у кримінальних справах на основі принципу взаємного визнання електронних доказів.

Як зазначає Дагна Кнітель, безліч законодавчих інструментів, які були прийняті в останні десятиліття, залишили по собі мозаїку нормативних актів, які перешкоджали ефективному розгляду та виконанню, тому європейські законодавці мали на меті виправити цей стан справ і забезпечити ефективну співпрацю шляхом запровадження принципу взаємного визнання також для збору доказів (Knytel Dagna, 2020: 67). При цьому рушійною силою розвитку правового регулювання збору та застосування електронних доказів є саме кримінально-процесуальна сфера та інституційні заходи протидії кіберзлочинності. Пояснюється це більш високим стандартом доказування, який має виключати будь-які обґрунтовані сумніви щодо винуватості особи, потребою в оперативності, а також суспільною небезпекою.

Природа сучасних комунікацій така, що навіть якщо правопорушник і жертва перебувають в одній юрисдикції, докази правопорушення ймовірно пройшли через інші юрисдикції або зберігалися в них. А оскільки в багатьох випадках електронні докази характеризуються транскордонністю (як правило, створюються, обробляються чи зберігаються в різних юрисдикціях), правила поводження з ними мають бути стандартизовані. Одночасно із цим законодавство про електронні докази має бути технологічно нейтральним, щоб відповідати технологічним досягненням, що розвиваються, та має бути сумісним із законодавством інших країн.

Ризику кіберзлочинності і подоланню нерозумінню природи електронних доказів почали приділяти увагу з моменту масового поширення інформаційно-комунікаційних технологій: Штайн Шельберг відзначає, що дослідження комп'ютерної злочинності та безпеки велося з 1970-х років, а в 1979 році було видано перший федеральний посібник для правоохоронних органів у США: «Computer Crime – Criminal Justice Resource Manual». Першою міжнародною ініціативою щодо комп'ютерної злочинності в Європі стала Конференція Ради Європи з кримінологічних аспектів економічної злочинності в Страсбурзі в 1976 році, на якій введено кілька категорій комп'ютерної злочинності (Stein Schjølberg, 2008: 2).

В результаті більш ніж шістнадцяти років підготовчої роботи Ради Європи Конвенція про кіберзлочинність (Будапештська конвенція) набрала чинності 1 липня 2004 р. та стала першою багатосторонньою міжнародною угодою щодо подолання кіберзлочинності. Хоча Конвенція про кіберзлочинність залишається найбільш ґрунтовним актом у цій галузі, держави-учасниці на міжнародному, регіональному та національному рівнях доповнюють її положення.

Загальновизнано, що належний ступінь гармонізації між країнами важливий для досягнення ефективного регулювання кіберзлочинності. Як зазначається, у широкому сенсі гармонізація важлива з двох причин: 1) усунути або принаймні зменшити кількість «безпечних гаваней». Якщо поведінка не криміналізована в певній країни, особи в цій країні можуть діяти безкарно, вчиняючи злочини, які можуть вплинути на інші юрисдикції. Мало того, що немає можливості притягнути до відповідальності у національній юрисдикції ймовірні зусилля зі збору доказів та екстрадиції будуть зірваним за відсутності подвійного визнання злочином; 2) гармонізація має вирішальне значення для ефективної співпраці між правоохоронними органами (Clough Jonathan, 2014: 701).

Збирання електронних доказів у цивільному судочинстві доволі утруднено, особливо якщо мова йде про транскордонний характер доказу: вітчизняні суди вимушені застосовувати такий інструмент як судове доручення, яке надсилається у порядку, встановленому ЦПК України або міжнародним договором, згода на обов'язковість якого надана Верховною Радою України, а якщо міжнародний договір не укладено – через Міністерство юстиції України, яке надсилає доручення Міністерству закордонних справ України для передачі дипломатичними каналами. Тобто, при виникненні необхідності звернення з таким дорученням першочерговим для суду є перевірка наявності міжнародного договору або конвенції, учасницею якого (якої) є Україна та країна, куди необхідно спрямувати документи. З огляду на таку складну процедуру надсилання судового доручення, його виконання та зворотного надсилання до суду, який його видав, тривалість судового розгляду суттєво затягується.

Електронні комп'ютерні дані дуже мінливі, декількома натисканнями клавіш або за допомогою автоматичних програм вони можуть бути

видалені, унеможливлюючи відстеження злочинця до його виконавця або знищуючи важливі докази провини, завдаючи завдано значної шкоди особі або майну, якщо докази не будуть швидко зібрані. Зважаючи на це, Будапештська конвенція передбачає, що у таких екстрених випадках не тільки запит, але й відповідь має бути зроблена в оперативному порядку, метою Конвенції є сприяння прискоренню процесу отримання взаємної допомоги, щоб критична інформація чи докази не були втрачені через те, що вони були видалені до того, як запит про допомогу можна було підготувати, передати та відповісти на нього шляхом надання Сторонам права надсилати термінові запити про співпрацю за допомогою прискорених засобів зв'язку, а не за допомогою традиційної, набагато повільнішої передачі письмових запечатаних документів через дипломатичну пошту або системи доставки пошти; та вимагати від запитуваної Сторони використовувати прискорені засоби для відповіді на запити за таких обставин (Explanatory Report to the Convention on Cybercrime. EuropeanTreaty Series-No. 185).

Країни-учасниці Конвенції на взаємній основі надають один одному можливість отримати максимальну правову допомогу з метою ведення розслідування або судового розгляду у зв'язку з кримінальними правопорушеннями, пов'язаними з комп'ютерними системами та даними, або збору доказів у кримінальному провадженні в електронній формі. Кожна Сторона може в екстрених ситуаціях надсилати запити про взаємну допомогу або повідомлення, пов'язані з такими запитами, використовуючи оперативні засоби зв'язку, включаючи факсимільний зв'язок або електронну пошту, з наступним офіційним підтвердженням, якщо цього вимагає запитувана Сторона. Запитувана Сторона приймає такий запит та відповідає на нього за допомогою будь-яких аналогічних оперативних засобів зв'язку (ст. 25 Конвенції) (Про ратифікацію Конвенції про кіберзлочинність, 2005). Як і у випадку добровільної співпраці, це положення визнає, що ефективне міжнародне співробітництво є важливим не лише для «кіберзлочинів» у вузькому розумінні, а й для всіх злочинів, пов'язаних із цифровими доказами.

Відповідно до Закону України «Про ратифікацію Конвенції про кіберзлочинність» та Закону України «Про внесення зміни до Закону України "Про ратифікацію Конвенції про кіберзлочинність"» в Україні органами, відповідальними за надсилання запитів про взаємну допомогу, надання на них відповідей, їх виконання або передачу уповноваженим органам, є Міністерство юстиції України (щодо доручень судів) та Генеральна прокуратура України (щодо доручень органів досудового слідства). Органом, на який покладаються повноваження щодо створення та функціонування цілодобової контактної мережі для надання невідкладної допомоги при розслідуванні злочинів, пов'язаних з комп'ютерними системами та даними, переслідуванні осіб, що обвинувачуються у вчиненні таких злочинів, а також збирання доказів в електронній формі, є Міністерство внутрішніх справ України (Про внесення зміни до Закону України «Про ратифікацію Конвенції про кіберзлочинність»). Під час війни Росії проти України кожна людина може стати небезпечною зброєю в руках країни-агресора, оскільки викрадені електронні дані можуть завдати шкоди державній безпеці України і підірвати обороноздатність. В умовах війни кіберзлочини здійснюються з метою дестабілізації ситуації в країні, дезінформації серед населення (Orlovskyi R., Kharytonov S., Samoshchenko Yu., Us O. and Iemelianenko V., 2023: 894), саме тому пришвидшений обмін інформацією важливий не тільки з точки зору розслідування, а й національної безпеки.

Однак процес гармонізації законодавства не можна вважати завершеним: із вдосконаленням технологій не тільки вирішуються проблеми збору й аналізу електронних доказів, а й створюються нові способи обходу впроваджених методів протидії кіберзлочинності. Це призводить до триваючого процесу міжнародної співпраці і узгодження подальших дій: органи ЄС тривалий час готували пропозиції щодо двох правових інструментів: у грудні 2018 року Рада ЄС більшістю голосів схвалила запропоновані Європейською комісією проекти Регламенту про європейські запити на отримання та забезпечення збереження електронних доказів у кримінальних справах та Директиви про встановлення правил призначення юридичних представників з метою збирання доказів у кримінальному процесі (Proposal for a Regulation of the European Parliament and of the Council on European Production and Preservation Orders for electronic evidence in criminal matters). У порівнянні з іншими інструментами ЄС, що забезпечують пряму комунікацію між державними органами, запропоновані інструменти спрямовані на розширення повноважень правоохоронних органів запитувати, отримувати доступ і обмінюватися даними, які зберігаються постачальниками послуг за кордоном (Matić Bošković M., 2022: 459). Однак обидві пропозиції були піддані критиці за порушення стандартів прав

людини (Matić Bošković M., 2021: 132–135). І лише у липні 2023 року ці напрацювання покладено в основу прийнятого Європейським парламентом та Радою Регламенту про європейські ордери на пред'явлення та європейські ордери на збереження електронних доказів у кримінальному провадженні та для виконання покарань у вигляді позбавлення волі після кримінального провадження (Regulation (EU) 2023/1543).

На відміну від Будапештської конвенції, яка охоплює не тільки європейські країни, а й Австралію, деякі країни Америки, Африки, Регламент ЄС спирається на вже інтегровані у багатьох сферах державні правопорядки країн-учасниць ЄС, а тому має можливість більш ефективно врегульовувати питання збирання доказів. Це дозволило цікавим чином обійти питання юрисдикції, яке повсякчас виникає в ході збирання електронних доказів, які зберігаються поза межами запитуючої країни, або якщо провайдер послуг не є резидентом запитуючої країни: оскільки провайдер без значних перешкод може швидко змінювати місце зберігання електронних даних, встановлення юрисдикції через місце зберігання (як це притаманно речовим чи письмовим доказам) не розглядається як ефективне. Враховуючи це, було запропоновано механізм, за якого питання юрисдикції вирішувати було б не потрібно: 1) електронні докази запитуються заінтересованою державою безпосередньо у провайдера, при цьому держава, в якій знаходиться даний провайдер, не залучається до процесу запиту та його виконання, крім певних випадків; 2) щоб подолати проблему зовнішньої юрисдикції, коли провайдер зареєстрований за межами ЄС, вводиться інститут призначення юридичних представників провайдерів, до яких і надсилається запит. Тобто, в якій би із країн не знаходився провайдер послуг, інша країна може запитати у нього інформацію напряму чи через представника.

На противагу європейському механізму співпраці у сфері кіберзлочинності, ООН також виявляє наміри розробити глобальну угоду щодо кіберзлочинності. Договір пропонує міжнародну співпрацю щодо збору електронних доказів для будь-яких серйозних злочинів, а не лише кіберзлочинів, визначених у договорі. Але деякі уряди виступають проти поглибленого рівня співпраці: у вересні 2023 року уряди завершили переговори щодо запропонованої глобальної угоди про кіберзлочинність, однак не досягнули консенсусу щодо таких фундаментальних питань як сфера застосування угоди, що є кіберзлочинністю та яку роль, якщо така є, мають відігравати права людини в реалізації угоди. Не дивлячись на зовнішню привабливість врегулювання міжнародної співпраці на рівні країн-учасниць ООН, критика запропонованої угоди є доволі значною. Відзначається, що Росія, ініціювавши резолюцію ООН про створення комітету експертів для розгляду нової угоди ООН про кіберзлочинність насправді має намір на заміну Будапештської конвенції Ради Європи, яка є єдиним міжнародним документом, що стосується цього питання. Нова угода, на думку експертів, може призупинити прогрес у міжнародному співробітництві з кіберзлочинності, адже резолюція Росії та її проект конвенції викликають серйозні проблеми з правами людини, запропоновані формулювання є надзвичайно розпливчастим, що, швидше за все, стане прикриттям для авторитарних урядів для переслідування своїх політичних опонентів (Hakmeh Joyce, Peters Allison, 2020). Однак переговори щодо проекту конвенції тривають, їх планується завершити на початку 2024 року: протягом обмеженого часу, що залишився, уряди повинні працювати над тим, щоб забезпечити відповідність цієї угоди їхнім міжнародним зобов'язанням у сфері прав людини, зокрема, звужуючи сферу застосування конвенції та включаючи лише основні кіберзлочини, а також гарантії захисту від зловживання.

Натомість, залишаються країни, які уникають глобальної співпраці у цій сфері, не доєднавшись до жодної із широких ініціатив. Правова гармонізація кіберзаконів в Асоціації держав Південно-Східної Азії необхідна для боротьби з транснаціональним характером кіберзлочинності та вимагає від усіх держав-членів домовитися про єдину динамічну нормативно-правову базу щодо кіберзлочинності, визначаючи недоліки статичної конвенції. Для даного регіону виділяють і лінгвістичну перепону: у випадку Брунею, Малайзії, Філіппін і Сінгапуру правові системи використовують англійську мову, інші шість країн Асоціації держав Південно-Східної Азії використовуються різноманітні мови, а тому ухвалення модельних законів не оцінюється дослідниками як ефективний спосіб гармонізації законодавства та співробітництва. Кращим варіантом, на думку Р. Сміта, має розглядатися договір або конвенція, які встановлюватимуть сферу дії та мінімальні вимоги, які необхідно включити до місцевого законодавства, а також зобов'язання щодо співпраці один з одним (Robert Smith, 2019: 273).

Як можлива модель гармонізації дослідником пропонується Конвенція про кіберзлочин-

ність (Будапештська конвенція), однак через відсутність одностайного консенсусу держави Південно-Східної Азії (крім Філіппін) не приєдналися до неї, тому наразі розробляються альтернативні шляхи регулювання, одним із яких розглядається варіант створення регіонального суду з кіберзлочинності, який може стати альтернативою досягненню міжнародного консенсусу. Виходячи з концепції міжнародного загального права, якщо деякі учасники не змогли дійти згоди у широкій угоді, замість цього сторони можуть погодитися на неглибокі правила для створення інституції, уповноваженої розглядати справи та таким чином формулювати правила (Iu, K.Y., Wong, V.MY, 2023). Фактично, Кван Юн та Ванесса Вонг підтримують вищевикладену позицію Р. Сміта щодо доцільності розроблення рамкової угоди у регіоні Південно-Східної Азії, однак як один із варіантів дослідниками обґрунтовується доцільність створення регіонального Суду з кіберзлочинності Асоціації держав Південно-Східної Азії, що може бути альтернативним підходом до досягнення гармонізації законодавства, коли узгодження положень здійснюється не шляхом прийняття міжнародного нормативно-правового акту, а формується судовою практикою.

Висновки. Процес гармонізації законодавства у сфері збирання електронних доказів та протидії кіберзлочинності відбувається як на міждержавному рівні, так і на регіональному рівні (наприклад Регламент Європейського парламенту та Ради ЄС про європейські ордери на пред'явлення та європейські ордери на збереження електронних доказів у кримінальному провадженні та для виконання покарань у вигляді позбавлення волі після кримінального провадження). Деякі регіональні ініціативи набувають характеру універсальних, прикладом чого є Конвенція про кіберзлочинність (Будапештська конвенція) Ради Європи, до якої приєдналися ще 22 країни, які не є країнами-учасницями Ради Європи (США, Канада, Аргентина тощо). Поряд із цим, відбуваються спроби для врегулювання протидії кіберзлочинності на рівні ООН. Поміж цим, залишаються країни, які не беруть участі в жодному із напрямів гармонізації, що створює ризики використання таких країн як «сірих зон» для кіберзлочинців.

ЛІТЕРАТУРА:

1. The global state of cybercrime legislation 2013–2023: A cursory overview, Bucharest, 8 December 2023 / Provisional version prepared by the Cybercrime Programme Office of the Council of Europe (C-PROC) URL: https://rm.coe.int/3148-1-3-4-cyberleg-global-state-dec-2023-v4-public/1680adadf0.

2. Borko A., Nehodchenko V., Volobuieva O., Kharaberiush I., Lohvynenko Ye. Fighting against cybercrime: problems and prospects in ukraine and the world. *Journal of Legal, Ethical and Regulatory Issues*. 2019. Vol. 22, Special Issue 2. P. 1–5. URL: https://dspace.univd.edu.ua/server/api/core/bitstreams/ a665d914-104b-42d7-b5d0-3fc456e11f46/content.

3. Wang Xue-Guang. Research on Legal Norm Problems of Electronic Evidence Legislation Hierarchy. *Proceedings of the 2nd Annual International Conference on Social Science and Contemporary Humanity Development*. P. 718. DOI: 10.2991/sschd-16.2016.137.

4. Knytel Dagna. Evidence Gathering in the European Union: The Transposition of Directive 2014/41/ EU into French and German Legislation. European Criminal Law Review. 2020. 10. 66–92. DOI: 10.5771/2193-5505-2020-1-66.

5. Schjølberg Stein. The History of Global Harmonization on Cybercrime Legislation – The Road to Geneva. *Journal of International CommercialLaw and Technology.* 2008. vol. 1, no. 12. P. 1–19.

6. Clough Jonathan. A World of Difference: The Budapest Convention On Cybercrime And The Challenges Of Harmonisation. *Monash University law review. Monash University. Faculty of Law.* 2014. 40(3). P. 668–736. URL: https://www.researchgate.net/publication/277892666_A_World_of_Difference_The_Budapest_Convention_On_Cybercrime_And_The_Challenges_Of_Harmonisation/

7. Explanatory Report to the Convention on Cybercrime. EuropeanTreaty Series-No. 185. URL: https://rm.coe.int/16800cce5b.

8. Про ратифікацію Конвенції про кіберзлочинність: Закон України від 07.09.2005 № 2824-IV // База даних «*Законодавство України*» / *Верховна Рада України*. URL: https://zakon.rada.gov.ua/go/2824-15.

9. Про внесення зміни до Закону України «Про ратифікацію Конвенції про кіберзлочинність»: Закон України від 21.09.2010 № 2532-VI // База даних «*Законодавство України*» / *Верховна Рада України*. URL: https://zakon.rada.gov.ua/go/2532-17.

10. Orlovskyi R., Kharytonov S., Samoshchenko Yu.,Us O. and Iemelianenko V. Countering Cybercrime Under Martial Law. *Journal of Cyber Security and Mobility*. 2023. Vol. 12 (6). P. 893–910.

11. Proposal for a Regulation of the European Parliament and of the Council on European Production and Preservation Orders for electronic evidence in criminal matters // COM/2018/225 final-2018/0108 (COD); Proposal for a Directive of the European Parliament and of the Council laying down harmonised rules on the appointment of legal representatives for the purpose of gathering evidence in criminal proceedings. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2018%3A225%3AFIN.

12. Matić Bošković M. Cybercrime money laundering cases and digital evidence. *Strani pravni zivot*. 2022. 66(4). P. 451–467. DOI: 10.56461/SPZ_22406KJ.

13. Matić Bošković M. Impact of Modern Technologies on Free Movement ofEvidence in European Union. *Journal of Criminology and Criminal Law.* 2021. 59(3). P. 123–140. URL: https://doi.org/10.47152/rkkp.59.3.6.

14. Regulation (EU) 2023/1543 of the European Parliament and of the Council of 12 July 2023 on European Production Orders and European Preservation Orders for electronic evidence in criminal proceedings and for the execution of custodial sentences following criminal proceedings PE/4/2023/REV/1. *Official Journal of the European Union.* L 191/118. ELI: http://data.europa.eu/eli/reg/2023/1543/oj.

15. Hakmeh Joyce, Peters Allison. A New UN Cybercrime Treaty? The Way Forward for Supporters of an Open, Free, and Secure Internet. *Council on Foreign Relations.* 2020. URL: https://www.cfr.org/blog/new-un-cybercrime-treaty-way-forward-supporters-open-free-and-secure-internet.Smith Robert. Harmonisation of Laws in ASEAN: The Issue of English. *International Seminar on Politics, Administration and Development 2019 (INSPAD2019) Walailak University*, THAILAND, 7-8 November 2019. 273–282. http://dx.doi.org/10.2139/ssrn.4323491.

16. lu K.Y., Wong V.MY. The trans-national cybercrime court: towards a new harmonisation of cyber law regime in ASEAN. *Int. Cybersecur. Law Rev. 2023*. URL: https://doi.org/10.1365/s43439-023-00105-x.

REFERENCES:

1. The global state of cybercrime legislation 2013–2023 : A cursory overview, Bucharest, 8 December 2023 / Provisional version prepared by the Cybercrime Programme Office of the Council of Europe (C-PROC). Retrieved from https://rm.coe.int/3148-1-3-4-cyberleg-global-state-dec-2023-v4-public/1680adadf0.

2. Borko, A., Nehodchenko, V., Volobuieva, O., Kharaberiush, I. & Lohvynenko, Ye. (2019). Fighting against cybercrime: problems and prospects in ukraine and the world. *Journal of Legal, Ethical and Regulatory Issues*. Vol. 22, Special Issue 2. 1–5. Retrieved from https://dspace.univd.edu.ua/server/api/core/bitstreams/a665d914-104b-42d7-b5d0-3fc456e11f46/content.

3. Xue-Guang, Wang. Research on Legal Norm Problems of Electronic Evidence Legislation Hierarchy. *Proceedings of the 2nd Annual International Conference on Social Science and Contemporary Humanity Development*. P. 718. DOI: 10.2991/sschd-16.2016.137.

4. Knytel, Dagna (2020). Evidence Gathering in the European Union: The Transposition of Directive 2014/41/EU into French and German Legislation. European Criminal Law Review. 10. 66–92. DOI: 10.5771/2193-5505-2020-1-66.

5. Schjølberg, Stein (2008). The History of Global Harmonization on Cybercrime Legislation – The Road to Geneva. *Journal of International CommercialLaw and Technology.* vol. 1. no. 12. 1–19.

6. Clough, Jonathan (2014). A World of Difference: The Budapest Convention On Cybercrime And The Challenges Of Harmonisation. *Monash University law review. Monash University. Faculty of Law.* 40(3). 668–736. Retrieved from https://www.researchgate.net/publication/277892666_A_World_of_Difference_The_Budapest_Convention_On_Cybercrime_And_The_Challenges_Of_Harmonisation/

7. Explanatory Report to the Convention on Cybercrime. EuropeanTreaty Series-No. 185. Retrieved from https://rm.coe.int/16800cce5b.

8. Pro ratyfikatsiiu Konventsii pro kiberzlochynnist [On the ratification of the Convention on Cybercrime]: Zakon Ukrainy [Law of Ukraine] from 07.09.2005 № 2824-IV. Verkhovna Rada Ukrainy. Retrieved from https://zakon.rada.gov.ua/go/2824-15. [in Ukrainian].

9. Pro vnesennia zminy do Zakonu Ukrainy «Pro ratyfikatsiiu Konventsii pro kiberzlochynnist» [On Amendments to the Law of Ukraine «On the Ratification of the Convention on Cybercrime»]: Zakon Ukrainy [Law of Ukraine] from 21.09.2010 № 2532-VI. Verkhovna Rada Ukrainy. Retrieved from https://zakon.rada.gov.ua/go/2532-17. [in Ukrainian].

10. Orlovskyi, R., Kharytonov, S., Samoshchenko, Yu., Us, O. and Iemelianenko, V. (2023). Countering Cybercrime Under Martial Law. *Journal of Cyber Security and Mobility*. Vol. 12 (6). 893–910.

11. Proposal for a Regulation of the European Parliament and of the Council on European Production and Preservation Orders for electronic evidence in criminal matters // COM/2018/225 final-2018/0108 (COD); Proposal for a Directive of the European Parliament and of the Council laying down harmonised rules on the

appointment of legal representatives for the purpose of gathering evidence in criminal proceedings. Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/ ?uri=COM%3A2018%3A225%3AFIN.

12. Matić Bošković, M. (2022). Cybercrime money laundering cases and digital evidence. *Strani pravni zivot*. 66(4). 451–467. DOI: 10.56461/SPZ_22406KJ.

13. Matić Bošković, M. (2021). Impact of Modern Technologies on Free Movement ofEvidence in European Union*. Journal of Criminology and Criminal Law.* 59(3). P. 123–140. Retrieved from https://doi.org/10.47152/rkkp.59.3.6.

14. Regulation (EU) 2023/1543 of the European Parliament and of the Council of 12 July 2023 on European Production Orders and European Preservation Orders for electronic evidence in criminal proceedings and for the execution of custodial sentences following criminal proceedings PE/4/2023/REV/1. *Official Journal of the European Union.* L 191/118. Retrieved from http://data.europa.eu/eli/reg/2023/1543/oj.

15. Hakmeh Joyce, Peters Allison (2020). A New UN Cybercrime Treaty? The Way Forward for Supporters of an Open, Free, and Secure Internet. *Council on Foreign Relations.* Retrieved from https://www.cfr.org/blog/new-un-cybercrime-treaty-way-forward-supporters-open-free-and-secure-internet.

16. Smith, Robert (2019). Harmonisation of Laws in ASEAN: The Issue of English. *International Seminar on Politics, Administration and Development 2019 (INSPAD2019) Walailak University*, THAILAND, 7–8 November 2019. 273–282. Retrieved from http://dx.doi.org/10.2139/ssrn.4323491.

17. Iu, K.Y., Wong, V.MY (2023). The trans-national cybercrime court: towards a new harmonisation of cyber law regime in ASEAN. *Int. Cybersecur. Law Rev.* Retrieved from https://doi.org/10.1365/s43439-023-00105-x.