РОЗДІЛ 9
КРИМІНАЛЬНИЙ ПРОЦЕС ТА КРИМІНАЛІСТИКА; СУДОВА ЕКСПЕРТИЗА; ОПЕРАТИВНО РОЗШУКОВА ДІЯЛЬНІСТЬ

УДК 341.1
DOI https://doi.org/10.24144/2307-3322.2022.72.64

ПРОЦЕСУАЛЬНІ ТА ОРГАНІЗАЦІЙНІ АСПЕКТИ ЗБОРУ ЕЛЕКТРОННИХ ДОКАЗІВ ПІД ЧАС МІЖНАРОДНОГО СПІВРОБІТНИЦТВА

Ахтирська Н.М.,
кандидат юридичних наук, доцент,
доцент кафедри кримінального процесу та криміналістики
Навчально-наукового інституту права
Київського національного університету імені Тараса Шевченка
https://orcid.org/0000-0003-3357-7722
Akhtyrska.n@gmail.com

Костюченко О.Ю,
кандидат юридичних наук,
завідувачка кафедри кримінального процесу та
криміналістики Навчально-наукового інституту права
Київського національного університету імені Тараса Шевченка
https://orcid.org/0000-0002-2243-1173

Ахтирська Н. М., Костюченко О. Ю, Процесуальні та організаційні аспекти збору електронних доказів під час міжнародного співробітництва.

Стаття присвячені питанням міжнародного співробітництва під час кримінального провадження та особливостям збору електронних доказів, які знаходяться під управлінням закордонного постачальника послуг. Кримінальний процесуальний кодекс України не містить визначення електронних доказів, проте кримінальне судочинство все частіше стикається з необхідністю збору, оцінки та використання таких доказів для ухвалення вироків. Відсутність нормативної визначеності не сприяє єдності судової практики, особливо гостро постає питання щодо оцінки електронних доказів, одержаних у межах міжнародної правової допомоги. В таких ситуаціях доводиться оцінювати правомірність діяльності правоохоронного органу, дотримання конвенційних гарантій дотримання прав людини, виконання зобов'язань використовувати електронні докази виключно у тому провадженні, на запит у якому вони були одержані, перевіряти факт повторного звернення до центрального органу міжнародного співробітництва в іншій державі з клопотанням про надання дозволу про використання таких доказів в іншому провадженні, коли постала така потреба тощо.

Суди розглядають клопотання прокурора про тимчасовий доступ до електронних даних або про проведення обшуку, при цьому інколи припускаються помилки, вказуючи юрисдикцію, де виникли докази, або де наступили наслідки злочинної діяльності. Процесуальні вимоги, які передбачені міжнародними актами, зумовлюють потребу звернення до держави, на території якої перебуває суб'єкт, який володіє, накопичує та здійснює управління даними.

Зміст клопотання, який надається до суду, повинен змістовно відповідати виду електронного доказу та способу його одержання в іншій юрисдикції, що не завжди враховується (клопотання про з*береження* доказів/*зберігання* доказів).

Збір електронних доказів відбувається шляхом складної процедури взаємодії між правоохоронними органами, постачальниками послуг, офіцерами зв'язку, аташе-офіцерами, які працюють в посольствах різних держав. Тому окрім процесуальних аспектів доцільно враховувати законодавство інших держав для ефективного використання організаційних правил (найбільш ефективних каналів одержання доказів).

Дослідження прогалин в чинному законодавстві та рекомендацій міжнародних експертів сприяє формуванню цілісного теоретичного бачення нормативного закріплення міжнародної взаємної правової допомоги для одержання електронних доказів та внесення пропозицій щодо закріплення такого механізму в спеціальному законі України.

Ключові слова: електронні докази, міжнародна правова допомога, постачальник послуг, особиста інформація абонента.

Akhtyrska N., Kostiuchenko O. Procedural and organizational aspects of electronic evidence collection during international cooperation.

The article is devoted to issues of international cooperation during criminal proceedings and features of electronic evidence collection, which are managed by a foreign service provider. The Criminal Procedure Code of Ukraine does not contain a definition of electronic evidence, but criminal justice is increasingly faced with the need to collect, evaluate and use such evidence for sentencing. The lack of normative certainty does not contribute to the unity of judicial practice, the issue of evaluating electronic evidence obtained within the framework of international legal assistance is especially acute. In such situations, it is necessary to assess the legality of the law enforcement agency's activities, compliance with conventional guarantees of human rights compliance, fulfillment of obligations to use electronic evidence exclusively in the proceedings in which it was obtained, to check the fact of repeated appeals to the central body of international cooperation in another state with a request for permission to use such evidence in other proceedings, when such a need arose, etc.

Courts consider prosecutor's requests for temporary access to electronic data or to conduct a search, sometimes making mistakes in specifying the jurisdiction where the evidence originated or where the consequences of the criminal activity occurred. Procedural requirements, which are provided for by international acts, determine the need to apply to the state in whose territory the entity that owns, accumulates and manages data is located. The content of the request submitted to the court must be substantively consistent with the type of electronic evidence and the method of obtaining it in another jurisdiction, which is not always taken into account (request for preservation of evidence/preservation of evidence).

The collection of electronic evidence takes place through a complex procedure of interaction between law enforcement agencies, service providers, liaison officers, and attaché officers working in the embassies of different states. Therefore, in addition to procedural aspects, it is advisable to take into account the legislation of other states for the effective use of organizational rules (the most effective channels for obtaining evidence).

The study of gaps in the current legislation and the recommendations of international experts contributes to the formation of a holistic theoretical vision of the normative consolidation of international mutual legal assistance for obtaining electronic evidence and the introduction of proposals for the consolidation of such a mechanism in the special law of Ukraine.

Keywords: electronic evidence, international legal aid, service provider, subscriber's personal information.

Вступ. Оскільки злочинці все активніше використовують Інтернет, соціальні мережі та інші системи обміну повідомленнями з функцією шифрування для вчинення злочинних дій, збір доказів від постачальників таких послу має важливе значення. Електронні докази, що зберігаються у постачальників послуг, можуть бути використані для підтвердження вчинення злочину, для встановлення злочинних зв'язків, визначення місця перебування правопорушника, що сприятиме викриттю та притягненню до відповідальності винних осіб. Надзвичайно важливо враховувати можливість запиту доказів у іноземного постачальника послуг шляхом звернення за наданням взаємної правової допомоги. Даний механізм стає все більш перевантаженим, що призводить до тривалих строків виконання таких запитів, що не узгоджується зі стрімким характером використання електронної комунікації для підго-

товки, вчинення та приховання слідів злочинної діяльності. Значна кількість постачальників послуг базується в США, тому співробітникам правоохоронних органів та суддям необхідно враховувати особливості міжнародного співробітництва у сфері збору електронних доказів. Аналіз слідчої та судової практики свідчить про певні складнощі, які, зокрема, зумовлені відсутністю легітимного визначення електронних доказів, ознак, які їм притаманні, складових елементів («електронні реквізити»), строків зберігання, способів збору та оцінки. Актуальність дослідження наведених питань узгоджується з завданнями, визначеними в Стратегії кібербезпеки України, зокрема, щодо посилення спроможності у протидії кіберзлочинності шляхом завершення імплементації в законодавство України положень Конвенції про кіберзлочинність та врегулювання на законодавчому рівні питання щодо електронних доказів, використовуючи кращі практики з цих питань Сполучених Штатів Америки, держав – членів ЄС та враховуючи сучасні виклики і тенденції у сфері кібербезпеки [1].

Злочинці намагаються зберігати власну анонімність, використовуючи для цього найсучасніші технології, що зобов'язує держави та міжнародне співтовариство уніфіковувати та удосконалювати форми міжнародного співробітництва під час кримінального провадження.

Мета дослідження. Внесення пропозицій до кримінального процесуального законодавства України відповідно до нових міжнародних стандартів збору доказів в електронній формі, створення відповідних органів, уповноважених на проведення консультацій та контролю за виконанням запитів на негайне надання інформації у надзвичайних ситуаціях.

Викладення основного матеріалу. Практично будь-який злочин пов'язаний з електронним пристроєм, який має пам'ять або будь-яку форму програмування. Навіть якщо такий пристрій не використовувався безпосередньо в контексті злочину, дії особи, що вчинила злочин, цілком ймовірно, могли бути зафіксовані за допомогою пристрою глобальної системи позиціонування (GPS), що встановлений на мобільному пристрої. Забезпечення отримання електронних доказів за допомогою цифрової криміналістичної експертизи та слідства стало основним інструментом притягнення злочинців до відповідальності. Розвиток «хмарних» обчислень (де програми та дані зберігаються віддалено, за межами країни та в невизначених місцях) означає, що обробка потенційних електронних доказів відповідно до перевірених принципів та практики стає важливішою, ніж будь-коли, що загострює наукову полеміку, скеровану на пошук правових механізмів використання електронних доказів.

Варто погодитись з позицією А.В. Ратнової, яка цілком обґрунтовано доводить, що електроні документи відносяться до самостійного джерела доказів у кримінальному провадженні [2, с. 3]. На нашу думку, така позиції потребує доповнення щодо визначення електронних реквізитів документу, метаданих, за якими визначається достовірність доказів. Спірним вважається висновок В.С. Петренко, згідно з яким електронні докази є елементами інформаційних технологій [3, с. 111]. На нашу думку, електронні докази генеруються, передаються або зберігаються за допомогою технологій, є продуктом (результатом) або об'єктом обробки. М.В. Гуцалюк визначає електронні докази як докази у кримінальних провадженнях, які можна отримати в електронній формі [4, с. 7]. Таке визначення не містить системи ознак, однак влучно, відповідно до міжнародних документів, свідчить про те, що поняття доказу залишається не змінним, специфічною є лише форма їх існування чи зберігання. Електронні докази отримують за допомогою електронних пристроїв, комп'ютерних носіїв інформації, а також комп'ютерних мереж, у тому числі через мережу Інтернет. Вони стають доступними для сприйняття людиною після обробки засобами комп'ютерної техніки.

В Кримінальному процесуальному кодексі України не надано дефініції електронних доказів, але вони (без нормативного визначення) широко використовуються в судочинстві. Відповідно до міжнародних рекомендацій, електронні докази – це будь-яка інформація, що генерується, зберігається або передається в цифровій формі, яка згодом може знадобитися для підтвердження або спростування факту, оскаржуваного в межах провадження. Попри те, що в різних юрисдикціях норми можуть відрізнятися, загалом під час оцінювання електронних доказів для судового розгляду слід враховувати такі критерії: автентичність, повнота, надійність, переконливість, пропорційність.

Практика країн ЄС свідчить про наступне: 1) в рамках більшої частини розслідувань направляється запит на одержання транскордонного доступу до електронних доказів; 2) електронні докази у будь-якій формі мають важливе значення для 85% кримінальних проваджень; 3) майже у двох третинах (65%) розслідуваннях, у рамках яких важливо одержати електронні докази, необхідно направляти запит постачальнику послуг, що знаходиться в іншій юрисдикції [5, с.7]. В 2021 році в судах України на розгляді перебувало 32 провадження за ст. 200 КК України «Незаконні дії з документами на пере-

каз, платіжними картками та іншими засобами доступу до банківських рахунків, обладнанням для їх виготовлення», 391 провадження за ст. 361-363 КК України «Кримінальні правопорушення у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку» [6]. У цих та інших кримінальних провадженнях виникала необхідність одержання доказів на території інших держав. Відповідно до ст. 562 КПК України, якщо для виконання запиту компетентного органу іноземної держави необхідно провести процесуальну дію, виконання якої в Україні можливе лише з дозволу прокурора або суду, така дія здійснюється лише за умови отримання відповідного дозволу в порядку, передбаченому КПК України, навіть якщо законодавство запитуючої сторони цього не передбачає. Підставою для вирішення питання щодо надання такого дозволу є матеріали звернення компетентного органу іноземної держави (ч.1). У разі якщо при зверненні за допомогою в іноземній державі необхідно виконати процесуальну дію, для проведення якої в Україні потрібен дозвіл прокурора або суду, така процесуальна дія потребує надання відповідного дозволу прокурором або судом у порядку лише у разі, якщо це передбачено міжнародним договором або є обов'язковою умовою надання такого виду допомоги за законодавством запитуваної сторони. При цьому строк дії такого дозволу не обмежується, а належно засвідчена копія дозволу долучається до матеріалів запит (ч.2). В 2021 році на розгляді до судів першої інстанції надійшло 208 клопотань про надання спеціального дозволу у порядку надання міжнародної правової допомоги [6].

В чотирьох резолюціях (2322 (2016 р.), 2331 (2016 р.), 2341 (2017 р.) и 2396 (2017 р.)) Рада Безпеки ООН закликала держави-учасниці збирати та зберігати докази задля забезпечення можливості проведення розслідування та притягнення до відповідальності осіб, причетних до терористичної діяльності. В Резолюції 2322 (2016 р.) вказується на збільшення запитів про співробітництво щодо збору доказів у формі цифрових даних з Інтернету, підкреслюється важливість розгляду можливості переоцінки способів та прогресивної практики (в залежності від ситуації), зокрема, пов'язаних з методиками проведення розслідування та електронними доказами.

Електронні докази, які можна одержати в межах міжнародної правової допомоги у кримінальних провадженнях, поділяються на дві категорії:

1) електронні докази, які зберігаються у постачальника послуг: а) основна інформація про абонента/користувача (ОІА) може включати інформацію про тривалість використання абонентом цієї конкретної послуги, IP-адреса, з якої вперше був здійснений вхід в систему, інформація про трафік (без інформації про контент (зміст)); б) інформація про трафік (без інформації про контент (зміст)): метадані, пов'язані з наданням послуг; дані, що стосуються підключення, трафіка або місцезнаходження комунікації (наприклад IP або MAC-адрес); журнали реєстрації доступу, в яких реєструється час та дата здійснення доступу до послуги конкретною фізичною особою, а також IP-адреса, з якої здійснюється доступ до послуги; журнали операцій, в яких фіксується продукти або послуги, одержані конкретною фізичною особою від постачальника послуг або третьої особи (наприклад, придбання місця в хмарному сховищі); в) інформація про зміст: тіло або зміст електронного листа, повідомлення, блогу або поста, відео, зображення або звук, що зберігаються в цифровому форматі (крім даних про абонента або метаданих);

2) електронні докази, які можна збирати в режимі реального часу: а) інформація про трафік (перехоплення інформації про те, з ким контактує об'єкт та звідки –наприклад, статичні та динамічні IP-адреси); б) інформація про зміст (перехоплення тіла та тексту електронного листа, повідомлення, блогу або поста, відео, зображення або аудіо-матеріалів, які зберігаються в цифровому форматі (крім даних про абонента та метаданих).

Для одержання електронних доказів у межах міжнародного співробітництва використовують наступні механізми: 1) звернення до постачальника послуг з клопотанням про збереження електронних доказів, щоб створити можливість для термінового їх одержання; 2) направлення прямого запиту постачальнику послуг або використання механізмів співробітництва між поліцейськими службами для розкриття електронних доказів (без необхідності направляти запит про взаємну правову допомогу), щоб скоротити час надання електронних доказів (з урахуванням національного законодавства США, де базуються основні постачальники послу); 3) термінові запити правоохоронних органів на розкриття інформації постачальниками послуг, щоб запобігти ризику спричинення смерті або тяжких тілесних ушкоджень.

Перш ніж направляти запит про надання електронних доказів, необхідно визначитись з місцем, де постачальник послуг здійснює розпорядження та управління електронними доказами. Надзвичайно

важливим є встановити, куди слід скеровувати запит про забезпечення збереження даних. Постачальник послуг може зберігати дані в різних країнах світу, але це не означає, що запит про забезпечення збереження слід направляти туди, де постачальник послуг їх зберігає. Запит слід скеровувати туди, де постачальник послуг розпоряджається та управляє даними. Щоб встановити місце, куди треба направити запит, необхідно звернутися до керівництва постачальника послуг в порядку взаємодії з правоохоронними органами.

Строки збереження даних в різних юрисдикціях різняться. Деякі постачальник послуг зберігають обмежений обсяг даних упродовж короткого періоду часу. Така інформація про зміст видаляється відразу після перегляду всіма одержувачами або через 30 днів після відправки, якщо повідомлення не було відкрито. WhatsApp не зберігає повідомлення після їх доставки та відкриття, а також інформацію щодо трафіку таких повідомлень. Недоставлені повідомлення стираються з серверів WhatsApp через 30 днів. Отже, перш ніж звертатися з клопотанням за одержанням спеціального дозволу до суду та відправляти запит в іншу юрисдикцію, слід у рамках міжнародної співпраці з'ясувати строки зберігання даних.

Правоохоронні органи мають враховувати, що деякі країни не виконують запити про взаємну правову допомогу щодо злочинів невеликої тяжкості, такі обмеження встановлюються законодавством або практикою. Наприклад, у США, як правило, не виконуються запити про взаємну правову допомогу щодо злочинів, термін ув'язнення за вчинення яких складає 12 місяців та менше, або якими була спричинена шкода на суму менше 5 тисяч доларів США. Отже, перш ніж направляти запит, необхідно з'ясувати у центрального органу міжнародного співробітництва конкретної держави чи входить злочин до переліку тих, за якими здійснюється виконання запиту.

У випадку доцільності направлення звернення про взаємну правову допомогу необхідно одержати відповідний дозвіл (ухвалу) суду. Так, слідчий суддя Печерського районного суду м. Києва розглянув клопотання про тимчасовий доступ до документів, які містять охоронювану законом таємницю, що перебувають у володінні компанії «Facebook, Inc», розташованої за адресою: місто Менло-Парк, вулиця Хакер-уей, 1, штат Каліфорнія, США (1 Hacker Way, Menlo Park, CA 94025, USA). Досудовим розслідуванням було встановлено, що організована група осіб з використанням всесвітньої інформаційної системи загального доступу Інтернет, вчиняють умисні дії, спрямовані на розпалювання національної, расової, релігійної ворожнечі та ненависті, приниження національної честі, гідності та образи почуттів громадян, шляхом розповсюдження повідомлень у соціальних Інтернет-мережах, які містять заклики до порушення рівноправності громадян залежно від їх расової, національної належності або релігійних переконань, використовуючи спеціально створені облікові записи користувачів, з метою впливу на свідомість громадян та формування заздалегідь визначеного переконання. Для встановлення події кримінального правопорушення, осіб, які здійснювали реєстрацію облікових записів та діяли за попередньою змовою з іншими співучасниками злочину для розповсюдження повідомлень у соціальних Інтернет – мережах у ході слідства виникла необхідність в отриманні тимчасового доступу до документів, що перебувають у володінні компанії «Facebook, Inc» (документи щодо IP-адрес реєстрації, входу, інформації зазначеної при реєстрації облікових записів). Для проведення процесуальних дій на території США органом досудового розслідування, відповідно до Договору між Україною та Сполученими Штатами Америки про взаємну правову допомогу у кримінальних справах від 22.07.1998 року, було підготовлено запит про надання правової допомоги у кримінальному провадженні [7].

Наведена категорія кримінальних проваджень потребує ретельної підготовки запиту та попередніх консультацій, оскільки запит про надання взаємної правової допомоги може бути відхилений на підставі національного законодавства у зв'язку з порушенням прав людини, які визнані такими у запитуваній державі. Наприклад, щодо онлайн-пропаганди, яку ведуть терористи або особи, які їм симпатизують, може існувати різниця між *повідомленнями*, *які спонукають до вчинення терористичних актів* та за які повинна передбачатися кримінальна відповідальність у відповідності з міжнародним правом, і *повідомленнями, які вважають законним правом на свободу думки*, совісті, релігії та переконань. Так, у публікації Міністерства юстиції США щодо одержання електронних доказів в США (2012 р.) йдеться про наступне: «… США відхиляє запит про надання допомоги, якщо він стосується фізичної особи, яка використала вислови (письмово, усно, у інший спосіб), котрі підпадають під дію захисту свободи вираження поглядів у рамках Конституції США (наприклад, риторика «ненависті», як правило, захищається Конституцією США, хоча й викликає заперечення), за виключенням випадків, коли

наведені факти, що вказують на вихід за межі допустимої, що підпадає під дію захисту, риторики (наприклад, риторика ненависті, яка включає заклики до негайних жорстоких дій) [5, с. 98]. Оскільки не всі вислови захищені законом, перед складанням запиту доцільно одержати консультацію з державним органом міжнародного співробітництва США.

Більшість постачальників послуг США та Канади зберігають дані упродовж 90 днів, цей строк може бути продовжений ще на 90 днів на підставі письмового запиту, який необхідно подавати до закінчення строку, інакше всі дані будуть видалені. У випадку направлення запиту про взаємну правову допомогу та потребі продовжити строк збереження даних більш ніж на 180 днів, доцільно звернутися до центрального органу міжнародного співробітництва для сприяння у продовженні строку до моменту виконання запиту *за два тижня до закінчення терміну.*

Одержання електронних доказів не в кожному випадку вимагає звернення про надання взаємної правової допомоги. Такі докази можна одержати у інший спосіб: 1) пошук у відкритих джерелах; прямі запити постачальнику послуг; 2) прямий контакт з користувачем облікового запису щодо надання електронних доказів, які він скачує зі свого облікового запису; 3) згода користувача облікового запису або його близького родича, щоб постачальник послуг надав електронні докази з облікового запису (в липні 2018 року Федеральний верховний суд Німеччини ухвалив, що облікові записи в соціальних мережах не відрізняються від особистих листів та щоденників, можуть передаватися у спадок); 4) співробітництво між поліцейськими службами держав в рамках добровільного розкриття даних.

В США існує низка державних відомств, які можуть сприяти у підготовці та направленні запиту постачальнику послуг в США. У надзвичайних ситуаціях, коли необхідно терміново одержати доступ до електронних доказів, доцільно звернутися до представника Управління з міжнародних справ (OIA) Відділу кримінальних справ Міністерства юстиції США (DOJ), які мають своїх аташе, що працюють в посольствах США в Бангкоку, Брюсселі, Лондоні, Манілі, Мехіко, Парижі та Римі. Крім того, деякі правоохоронні органи США мають своїх аташе з питань міжнародного співробітництва в різних країнах (наприклад, ФБР, Управління забезпечення дотримання законів про наркотики, Міграційна та митна поліція або Секретна служба США). Наприклад, у Секретної служби США є Робоча група щодо боротьби з електронними злочинами (ECTF) – слідчий альянс правоохоронних органів, представників науки та приватного сектору. Існує 38 національних та дві іноземні ECTF (Лондон, Рим). Секретна служба США – це слідчий правоохоронних орган, що відіграє центральну роль в забезпеченні захисту банківського та фінансового сектору. Вона діє по всьому світу, займається виявленням та розслідуванням кіберзлочинів (від крадіжок криптовалюти до атак на банки та фінансові установи з метою вимагання).

Міжнародне співробітництво під час кримінального провадження щодо одержання електронних доказів здійснюється в межах співпраці з Європолом на підставі двох типів угод – стратегічних та операційних. Хоча обидва види угод скеровані на співробітництво, відмінність полягає у тому, що *стратегічна угода обмежується обміном загальної інформації*, а *операційна угода передбачає обмін персональними даним*. Відповідна Угода між Україною та Європейським поліцейським офісом про оперативне та стратегічне співробітництво від 14.12.2016 року була ратифікована 12.07.2017 року [8].

Міжнародними документами затверджено правовий стандарт змісту запиту про надання взаємної правової допомоги. Зокрема, в запиті має бути описані конкретні факти для підтвердження необхідності запитуваних даних, що такі докази пов'язані зі злочином: тип інформації, яку треба одержати (повідомлення електронної пошти); підстава, що підтверджує зв'язок такої інформації зі злочином, за яким надісланий запит; належність облікового запису підозрюваному з наявними доказами цього (наприклад, використання облікового запису Google підтверджує свідок, або, що результат прямого запиту до Facebook свідчить, що підозрюваний створив відповідний обліковий запис з використанням адреси електронної пошти, інформація про зміст облікового запису якого запитується). Не рекомендується використовувати такі фрази як «розслідування показало», «вважається, що», в запиті вказується точно про які розслідування йдеться, коли та ким вони проводяться, яким чином докази демонструють доцільність одержання запитуваної інформації.

В запиті обов'язково має бути вказана мета одержання таких доказів та кримінальне провадження, у межах якого надаються електронні докази. Якщо після одержання електронних доказів у запитуючої держави виникне потреба використати їх з іншої метою (у іншому кримінальному провадженні або щодо іншої особи), то на це потрібно одержати згоду запитуваної держави. Невиконання цієї вимоги

може призвести до того, що електронні докази будуть визнані судом неприйнятними, а також створить загрозу для подальшого міжнародного співробітництва під час кримінального провадження.

Міжнародне співробітництво під час кримінального співробітництва досягає ефективності завдяки використанню механізму *термінових запитів, які обґрунтовуються надзвичайною ситуацією.*

Після атаки терористів на редакцію «Шарлі Ебдо» (Charlie Hebdo – французька щотижнева сатирична газета, що публікує карикатури, репортажі, дискусії та анекдоти) у Франції 7 січня 2015 року французька влада звернулась до ФБР, які скерували в Microsoft терміновий запит на розкриття інформації щодо осіб електронних листів з двох облікових записів. Запит був одержаний в електронному виді о 6 годині ранку, і співробітники Microsoft змогли його розглянути, одержати відповідні дані та направити їх ФБР для передачі правоохоронним органам Франції за 45 хвилин.

Другим додатковим протоколом до Конвенції про кіберзлочинність від 17 листопада 2021 року передбачена правова основа для такого прямого співробітництва з постачальниками послуг (ст. ст. 6,7), прискорених форм співробітництва для розкриття інформації про абонента та дані трафіку (ст.8), прискореного співробітництва та розкриття інформації у надзвичайних ситуаціях (ст. ст. 9, 10), передбачені додаткові інструменти взаємної допомоги (ст. ст. 11, 12), захист даних та інші гарантії верховенства права (ст. ст. 13, 14), також вперше дається визначення *«надзвичайної ситуації»*, під якою слід розуміти ситуацію, що створює значний та неминучий ризик для життя або безпеки будь-якої фізичної особи, а «персональними даними» вважається інформація, що має відношення до ідентифікації особи [9].

Висновки. З урахуванням зростання випадків використання інформаційно-комунікаційних технологій зі злочинною метою, збільшення кількості потерпілих від кіберзлочинів та важливість забезпечення правосуддя для захисту прав потерпілих та обов'язку держави нести відповідальність за захист суспільства не тільки в реальному світі, але й в Інтернеті, у тому числі шляхом ефективного використання електронних доказів, які перебувають під юрисдикцією іноземних держав, доцільно: на законодавчому рівні (шляхом прийняття спеціального закону «Про електронні докази») визначити поняття електронних доказів, види, способи збирання, оцінки та використання; встановити процесуальні строки звернення з клопотанням про зберігання електронних доказів (первинне та повторне) з урахуванням законодавства США, оскільки великі постачальними послуг знаходяться під їх юрисдикцією; вказати на необхідність перевірки судами мети первинного звернення за одержанням доказів та кримінального провадження, оскільки використання електронних доказів у іншому кримінальному провадженні може призвести до визнання таких доказів неприйнятними.

Список використаних джерел:

1. Стратегія кібербезпеки України, затв. Указом Президента України від 26 серпня 2021 року № 447/2021. *Офіційний вісник України.* 2021.№ 70. Ст. 4417.

2. Ратнова А.В. Кримінальні процесуальні та криміналістичні основи використання електронних документів у доказуванні: дис. … д. філософії: 12.00.09. Львів. 2021. 225 с.

3. Петренко В.С. Електронні докази як елемент інформаційних технологій Young Scientist. 2018. № 1(53). С. 111 -115.

4. Гуцалюк М.В. Використання електронних (цифрових) доказів у кримінальних провадженнях / М.В. Гуцалюк та ін. Київ : Вид-во Нац. акад. внутр. справ, 2020. 104 с.

5. Practical guide request order Evidence from other countries. OSCE, UN, IAP, UNODC, 2019. 221p.

6. Звіт судів першої інстанції за 2021 рік. URL:/https://court.gov.ua/inshe/sudova_statystyka/zvitnist_21

7. Ухвала Печерського районного суду м. Києва від 6 червня 2018 рок. Справа № 757/25582/18-к. URL: https://reyestr.court.gov.ua/Review/74568504

8. Угода між Україною та Європейським поліцейським офісом про оперативне та стратегічне співробітництво від 14.12.2016 року. *Офіційний вісник України*. 2017. № 62. Ст.1901.

9. Second Additional Protocol to the Convention on Cybercrime on enhanced cooperation and disclosure of electronic evidence [Strasbourg, 17.XI.2022]. URL:https://rm.coe.int/1680a49dab (access date 22.05.2022).