Шепітько Михайло Валерійович,
професор кафедри кримінального права Національного юридичного університету імені Ярослава Мудрого, провідний науковий співробітник НДІ вивчення проблем злочинності імені академіка В. В. Сташиса НАПрН України, доктор юридичних наук, професор

ЦИФРОВІ ВИКЛИКИ КРИМІНАЛЬНОГО ПРАВА ТА КРИМІНАЛІСТИКИ

Розвиток цифрових технологій дозволяє досягати не тільки очевидного науково-технічного прогресу в XXI ст., але й становить нові виклики для кримінального права та криміналістики, що пов'язується із створенням нових можливостей для вчинення злочинів. Останнім часом стає прийнятим виокремлення цифрових прав, до яких відносять:

1) доступ до інтернету та відсутності дискримінації в цій сфері

2) свободу слова та інформації;

3) забезпечення онлайн-доступу до освіти та знань;

4) особливий захист дітей та молоді під час користування інтернетом [1].

Комітет з прав людини ООН ще в 2016 р. відзначив, що ті самі права, що людини має офлайн, вони мають бути так само захищені онлайн, як-то:

1) свобода вираження поглядів, яка застосовується незалежно від кордонів та через будь-які ЗМІ за власним вибором відповідно до ст. 19 Загальної декларації прав людини та Міжнародного пакту про цивільні та політичні права;

2) свобода вираження поглядів, свобода об'єднань, недторканості приватного життя та інших прав людини в інтернеті мають бути захищені державами відповідно до міжнародних зобов'язань в сфері прав людини таким через національні демократичні інститути таким чином, щоб забезпечити свободу та безпеку в інтернеті, з тим, щоб він міг залишитися активною силою, що створює економічний, соціальний та культурний розвиток [2].

У Щорічному звіті щодо порушень цифрових прав 2022–2023 Балканської слідчої звітної мережі «BIRN» наголошується на типових порушеннях цифрових прав в Албанії, Боснії та

Герцоговині, Косово, Північної Македонії, Румунії, Сербії, Туреччини, Угорщині, Хорватії та Чорногорії. Найбільш типовими кримінальними правопорушеннями в цій сфері називаються:

1) комп'ютерне шахрайство (Албанія, Північна Македонія, Сербія, Хорватія, Угорщина);

2) знищення та крадіжка (персональних) даних та програм (Албанія, Хорватія);

3) публічні заклики ненависті та дискримінації (Албанія, Північна Македонія, Сербія, Туреччина, Чорногорія);

4) публікація фальсифікованої інформації в ЗМІ (Косово, Румунія, Угорщина, Чорногорія);

5) образа та безпідставне обвинувачення (Туреччина, Чорногорія) [3].

В Україні відстуній окремий документ, який би міг регулювати та захистити право на доступ до інтернету та пов'язані із ним свободи слова та інформації, забезпечення онлайн-доступу до освіти та знань та особливого захисту дітей та молоді під час користування інтернетом. У Стратегії кібербезпеки (2021–2025), затвердженої Указом Президента України від 26 серпня 2021 р. № 447/2021, зазначається, шо «кібератаки Російської Федерації спрямовані, насамперед, на інформаційно-комунікаційні системи державних органів України та об'єкти критичної інформаційної інфраструктури з метою виведення їх з ладу (кібердиверсія), отримання прихованого доступу і контролю, здійснення розвідувальної та розвідувально-підривної діяльності» [4]. Також в цій Стратегії відзначається поширення використання кіберпростору для вчинення злочинів проти основ національної безпеки України та кримінальних правопорушень, пов'язаних із легалізацією доходів, одержаних злочинним шляхом, торгівлею людьми, незаконним поводженням зі зброєю, бойовими припасами або вибуховими речовинами, незаконним обігом наркотичних засобів, психотропних речовин, їх аналогів або прекурсорів та інших предметів і речовин, які загрожують життю та здоров'ю людей» [4].

Чинний КК України виокремлює розділ XVI Особливої частини «Кримінальні правопорушення у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку» (ст.ст. 361–363-1), однак він не здатний об'єднати всі прояви таких кримінальних правопорушень, які визначаються як кіберзлочинність, цифрові злочини, комп'ютерне шахрайство (інтернет-шахрайство), викрадення персональних даних порушення авторських та суміжних прав в мережі інтернет, тощо. Цілий комплекс

кримінальних правопорушень стосується прямого блокування журналістської діяльності, сайтів та доступу до мережі Інтернет. Під час війни Інтернет простір став засобом поширення дезінформації, фейків, пропаганди, дискримінації та ненависті. Ці злочинні прояви стають ще більш небезпечними, оскільки їх вчинення передує вчиненню злочину агресії, геноциду, воєнних злочинів та злочинів проти людяності вже в реальній дійсності. Поява такої великої кількості кримінальних правопорушень, які вчиняються в мережі Інтернет, з використанням комп'ютерів, гаджетів та їх мереж, вказує на те, що з'являється необхідність розширення розділу XVI Особливої частини КК України «Кримінальні правопорушення у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку» та уточнення його назви. У перспективі такий інститут Особливої частини кримінального права може сформувати окреме вчення та отримати власну назву «цифрове кримінальне право» (*cybercrime law* [5]), створивши та визначивши власний предмет та метод як на загальному, так і спеціальному рівні.

Розслідування злочинів, що пов'язується із використанням комп'ютерної техніки, програмних продуктів та електронної комунікації, потребує використання засобів цифрової криміналістики (*digital forensics*) [6, p. 129] та спеціальних знань у відповідній сфері. Під час досудового розслідування таких діянь призначається та проводиться судова експертиза комп'ютерної техніки та програмних продуктів, а також електронної комункації [7]. Від проведення подібних судово-експертних досліджень часто залежить, – встановлення місця, часу, обстановки, засобів та зарядь вчиненного злочину.

Слід наголосити, що навіть під час війни держава має зберігати розумний баланс між дотриманням цифрових прав та блокуванням (обмеженням) ресурсів. Невипадково в міжнародно-правових актах та рішеннях містяться не тільки декларації окремих цифрових прав, але й обмовки щодо можливості їх обмеження. Очевидною стає й необхідність формулювання окремої кримінальної політики (стратегії) та закону в сфері забезпечення цифрових прав особи, які комплексно дали би можливість сформулювати прозорі зрозумілі правила обмеження таких прав при наявності відповідних загроз. При цьому цифрове кримінальне право може визначити ці кримінальні правопорушення та покарання для осіб, які їх вчиняють, а цифрова криміналістика –

надати ефективні засоби дослідження цифрових доказів в кримінальному провадженні.

Список використаних джерел

1. Your Digital Rights in Brief. Guide to Human Rights for Internet Users. *Council of Europe*. URL: https://rm.coe.int/1680301b6e

2. The promotion, protection and enjoyment of human rights on the Internet, A/HRC/32/L.20 (2016) at para 1. *UN Human Rights Council*. URL: https://www.article19.org/data/files/Internet_Statement_Adopted.pdf

3. Digital Rights in a Time of Crisis: Authoritarianism, Political Tension and Weak Legislation Boost Violations. Digital Rights Violations Annual Report 2022-2023. BIRN, 2023. P. 29-130.

4. Стратегія кібербезпеки (2021-2025), затверджена Указом Президента України від 26 серпня 2021 р. № 447/2021.

5. Justia. URL: https://www.justia.com/criminal/offenses/other-crimes/cybercrimes/

6. Shepitko V., Shepitko M. Criminal Law, Criminalistics and Forensic Sciences: Encyclopedia. Kharkiv, 2021. P. 129.

7. Інструкція про призначення та проведення судових експертиз та експертних досліджень та Науково-методичних рекомендацій з питань підготовки та призначення судових експертиз та експертних досліджень від 8 жовтня 1998 р. № 53/5, зареєстрована в Міністерстві юстиції України 3 листопада 1998 р. за № 705/3145.

Самодін Артем Володимирович,
заступник начальника правового відділу Департаменту міжнародного поліцейського співробітництва Національної поліції України, кандидат юридичних наук, доцент

ПИТАННЯ ІМПЛЕМЕНТАЦІЇ АКТІВ ПРАВА ЄВРОПЕЙСЬКОГО СОЮЗУ В НАЦІОНАЛЬНУ СИСТЕМУ ЗАКОНОДАВСТВА ЩОДО АВТОМАТИЗОВАНОГО ПОШУКУ ТА ОБМІНУ ДАНИМИ В МЕЖАХ СПІВПРАЦІ ПРАВООХОРОННИХ ОРГАНІВ

В межах переговорного процесу про вступ України до Європейського Союзу (далі – ЄС) та адаптації законодавства України до права ЄС, Україною взято на себе зобов’язання забезпечити приведення у відповідність до стандартів ЄС власного національного законодавства у сфері співпраці