

Діяльність судового експерта із забезпечення цифрових прав особи та її вплив на кримінально-правову кваліфікацію

Михайло Шепітько

доктор юридичних наук, професор, професор кафедри кримінального права, Національний юридичний університет імені Ярослава Мудрого МОН України; провідний науковий співробітник, НДІ вивчення проблем злочинності імені академіка В. В. Сташиса НАПрН України, м. Харків, Україна, ORCID: <https://orcid.org/0000-0002-7164-8037>, e-mail: shepitko.michael@gmail.com

Звернено увагу на проблему визначення цифрових прав особи та їх захист від незаконних посягань. Проаналізовано допомогу у виокремленні закликів і злочинів проти основ національної безпеки за допомогою висновків експерта, які вкажуть на зміст повідомлень, місце, час, обстановку, засоби та знаряддя вчиненого злочину.

Ключові слова: цифрові права особи; діяльність судового експерта; судова експертиза; найтяжчі міжнародні злочини; кримінально-правова кваліфікація.

The Role of a Forensic Examiner in Safeguarding Individual Digital Rights and Its Implications for Criminal Law Classification

Mykhaylo Shepitko

The identification and protection of individual digital rights against unlawful infringements has become a pressing issue. An analysis of appeals and crimes that jeopardize national security was conducted through expert assessments, which illuminate the content of communications, along with the temporal, spatial, contextual, and instrumental dimensions of the offenses committed.

Keywords: individual digital rights; forensic activities; forensic examination; serious international crimes; criminal law classification.

Розвиток цифрових технологій призвів до появи великого блоку цифрових прав, які потребують особливого правового захисту та встановлення міжнародних та національних стандартів. До цифрових прав особи прийнято вважати належними такі

права: 1) доступ до інтернету та відсутність дискримінації в цій сфері; 2) свобода слова та інформації; 3) забезпечення онлайн-доступу до освіти та знань; 4) особливий захист дітей та молоді під час користування інтернетом [1].

Реалізація цифрових прав особи почала відігравати настільки важливу роль у житті суспільства та держави, що необхідність їх захисту стала відображатися в міжнародних та національних документах. 2014 р. ПАРЄ прийняла резолюцію (1987) щодо права на доступ до інтернету, пов'язуючи його із правом на освіту, правом на участь у культурному житті та правом на об'єднання та зібрання [2].

Комітет із прав людини ООН ще 2016 р. відзначив, що ті самі права, що людина має офлайн, мають бути так само захищені онлайн: 1) *свобода висловлення 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, недоторканості приватного життя та інших прав людини в інтернеті* мають бути захищені державами відповідно до міжнародних зобов'язань у сфері прав людини через національні демократичні інститути таким чином, щоб забезпечити свободу та безпеку в інтернеті з тим, щоб вона могла залишитися активною силою, яка створює економічний, соціальний та культурний розвиток. До того ж Комітет із прав людини ООН підкреслює важливість *боротьби з пропагандою ненависті, яка є підбурюванням до дискримінації та насильства в інтернеті*, закликає до терпимості та діалогу, а також розроблення на

державному рівні політики, пов'язаної з інтернетом, метою якої є доступ до прав людини та їх реалізація [3].

Право на доступ до інтернету стало предметом розгляду багатьох справ у Європейському суді з прав людини під час захисту насамперед свободи висловлення поглядів (ст. 10 Конвенції про захист прав людини і основоположних свобод [4]). Так, у справі Ченгіз та ін. проти Туреччини (*Cengiz and Others v. Turkey*, 1 December 2015, §§ 49 and 52) зазначено, що «*на сьогодні інтернет став одним із головних засобів, за допомогою якого люди здійснюють своє право отримувати та передавати інформацію та ідеї, забезпечуючи тим самим необхідні інструменти для участі в діяльності та обговореннях політичних питань і питань загального інтересу*» [5].

В Україні немає окремого документу, який би міг проголосити та закріпити право на доступ до інтернету. Проте 2021 р. було прийнято Стратегію кібербезпеки України [6] та Стратегію інформаційної безпеки [7].

У Стратегії інформаційної безпеки зазначено, що «*інформаційні потреби на місцевому рівні належним чином не задовольняються, зокрема через низьку спроможність забезпечення населення послугами з доступу до інтернету*» [7]. У Стратегії кібербезпеки України було визначено пріоритети та цілі. Пріоритети забезпечення кібербезпеки України: *убезпечення кіберпростору для захисту суверенітету держави та розвитку суспільства; захист прав,*

свобод і законних інтересів громадян України в кіберпросторі; європейська і євроатлантична інтеграція у сфері кібербезпеки [6]. Ознайомлення з даною стратегією свідчить, що вона формувалася не так із метою забезпечення цифрових прав особи, як із загальною метою захисту держави під час тривалої повномасштабної російської агресії проти України.

Під час агресії проти України було зафіксовано випадки масової пропаганди війни, публічних закликів до вчинення агресії та геноциду, здійснення воєнних злочинів та злочинів проти людяності, які здійснювалися із використанням ЗМІ, інтернету, месенджерів та соціальних мереж. Це давало змогу надавати неправдиву інформацію обом сторонам, розпалювати ненависть та підбурювати до вчинення найтяжчих міжнародних злочинів.

Учинення таких злочинів супроводжується застосуванням комп'ютерної техніки, програмних продуктів та електронної комунікації. З одного боку, винуваті у вчиненні найтяжчих злочинів зловживають своїми цифровими правами, а з іншого — здійснюють незаконний вплив на населення з метою знищити державність та основи національної та міжнародної безпеки. Тому під час досудового розслідування таких діянь призначається судова експертиза комп'ютерної техніки, програмних продуктів, а також електронної комунікації. Важливим дослідженням стає лінгвістична експертиза мовлення (авторознавчі та семантико-текстуальні дослідження).

Судовий експерт, формулюючи свій висновок, безпосередньо впливає на кримінально-правову кваліфікацію, оскільки саме від нього часто залежить установа місця, часу, обстановки, засобів та знарядь злочину, а найголовніше — виокремлення публічних закликів до вчинення злочину (геноциду, агресії, пропаганди війни, воєнних злочинів, злочинів проти людяності, злочинів проти основ національної безпеки України).

Загалом слід зазначити, що навіть під час війни держава має зберігати розумний баланс між дотриманням цифрових прав особи та обмеженням ворожих ресурсів, користуванням доступом до інтернету як зброєю проти України. Невипадково в міжнародно-правових актах та рішеннях містяться не тільки декларації окремих прав, пов'язаних із цифровою сферою, але й обмовки щодо можливості їх обмеження (пропаганда ненависті, підбурювання до дискримінації та насильства). Очевидним стає й необхідність формулювання окремої кримінальної політики (стратегії) та закону в сфері забезпечення цифрових прав особи, які комплексно дали б можливість сформулювати зрозумілі правила обмеження таких прав за наявності відповідних загроз.

Перелік джерел посилання

1. Your Digital Rights in Brief. Guide to Human Rights for Internet Users. URL: <https://rm.coe.int/1680301b6e> (дата звернення: 05.09.2024).
2. The right to Internet access. PACE Resolution 1987 (2014). URL: <https://>

- assembly.coe.int/nw/xml/XRef/Xref-XML2HTML-en.asp?fileid=20870 (дата звернення: 05.09.2024).
3. The promotion, protection and enjoyment of human rights on the Internet. Human Rights Council. URL: https://www.article19.org/data/files/Internet_Statement_Adopted.pdf (дата звернення: 05.09.2024).
 4. Європейська конвенція з прав людини від 04.11.1950 р. № 995_004, ратиф. Законом України від 17.07.97 р. № 475/97-ВР. URL: https://zakon.rada.gov.ua/laws/card/995_004 (дата звернення: 05.09.2024).
 5. Access to Internet and freedom to receive and impart information and ideas. ECtHR, June 2024. URL: https://www.echr.coe.int/documents/d/echr/FS_Access_Internet_ENG (дата звернення: 05.09.2024).
 6. Стратегія кібербезпеки України : увед. в дію Указом Президента України від 26.08.2021 р. № 447/2021. URL: <https://zakon.rada.gov.ua/laws/show/447/2021#Text> (дата звернення: 05.09.2024).
 7. Стратегія інформаційної безпеки : увед. в дію Указом Президента України від 28.12.2021 р. № 685/2021. URL: <https://zakon.rada.gov.ua/laws/show/n0080525-21#Text> (дата звернення: 05.09.2024).