DOI https://doi.org/10.51647/kelm.2020.3.2.48

МІЖНАРОДНИЙ ДОСВІД ПРОТИДІЇ ОБІГУ ПОРНОГРАФІЧНИХ ПРЕДМЕТІВ МЕРЕЖЕЮ ІНТЕРНЕТ ТА ЙОГО ВИКОРИСТАННЯ В ДІЯЛЬНОСТІ ОПЕРАТИВНИХ ТА СЛІДЧИХ ПІДРОЗДІЛІВ НАЦІОНАЛЬНОЇ ПОЛІЦІЇ УКРАЇНИ

Альона Шраго
ад'юнкт кафедри оперативно-розшукової діяльності
Дніпропетровського державного університету внутрішніх справ (Дніпро, Україна)
ORCID ID: 0000-0002-2375-8231

Анотація. Актуальність статті полягає в тому, що широкий розголос численних фактів розпусних дій, скоєних під час використання мережі Інтернет, великий суспільний резонанс і підвищена увага міжнародної спільноти змусили державу визнати існування проблеми web-порнографії. Розповсюдження порнографії, що здійснюється мережею Інтернет, гарантує розповсюджувачу та споживачеві анонімність, відносну доступність способів її оприлюднення та отримання. Широкий попит на злочинну продукцію ускладнює пошук розповсюджувачів та реалізаторів такої продукції, особливо серед іноземців. У роботі проаналізовано окремі положення міжнародного та вітчизняного законодавства щодо протидії кіберзлочинності та порнографії. Наголошено на необхідності розробки актуального спеціалізованого програмного та апаратного забезпечення для провадження оперативно-розшукової діяльності в кіберпросторі із використанням міжнародного досвіду. Визначено пріоритетні напрямки протидії підрозділами Національної поліції України проявам збуту та розповсюдження порнографічних предметів у Інтернет. Зроблено висновок про необхідність: 1) розробки актуального спеціалізованого програмного та апаратного забезпечення для провадження оперативно-розшукової діяльності в кіберпросторі із використанням міжнародного досвіду; 2) удосконалення системи інформаційно-аналітичного забезпечення (створення Єдиної інформаційно-аналітичної системи правоохоронних органів із підсистемами за напрямами, у тому числі з окремим блоком для підрозділів боротьби з кіберзлочинністю); 3) внесення змін до КПК та інших нормативно-правових актів у сфері протидії кіберзлочинам на державному рівні; 4) розробки на міжнародному рівні та імплементація в національне законодавство процесуальних стандартів, що дозволяють ефективно розслідувати злочини в глобальних інформаційних мережах, отримувати, досліджувати і представляти електронні докази з урахуванням транскордонної проблеми; 5) налагодження співробітництво правоохоронних органів при розслідуванні кіберзлочинів на оперативному рівні; 6) вдосконалення механізмів долучення до матеріалів та використання у кримінальних провадженнях електронних доказів за цією категорією кримінальних проваджень; 7) зобов'язання компаній зберігати резервні копії електронних даних для підвищення ефективності розслідування таких злочинів; 9) полегшення доступу правоохоронних органів до електронних банків даних.

Ключові слова: міжнародний досвід, порнографія, порнографічні предмети, Інтернет, збут, розповсюдження, кіберпростір.

INTERNATIONAL EXPERIENCE IN COUNTERACTING THE CIRCULATION OF PORNOGRAPHIC OBJECTS ON THE INTERNET AND ITS USE IN THE ACTIVITIES OF OPERATIONAL AND INVESTIGATIVE DEPARTMENTS NATIONAL POLICE OF UKRAINE

Alona Shraho
Graduate Student at the Department of Operational Search Activity
Dnipropetrovsk State University of Internal Affairs (Dnipro, Ukraine)
ORCID ID: 0000-0002-2375-8231

Abstract. The relevance of the article is that the wide publicity of the numerous facts of lewd acts committed while using the Internet, the great public response and the increased attention of the international community forced the state to recognize the existence of the problem of web-pornography. The distribution of pornography on the Internet guarantees anonymity to the distributor and the consumer, and the relative availability of ways to publish and obtain it. Widespread demand for criminal products makes it difficult to find distributors and sellers of such products, especially among foreigners. The content of the article analyzes some provisions of international and domestic legislation on combating cybercrime and pornography. Emphasis is placed on the need to develop relevant specialized software and hardware for conducting operational and investigative activities in cyberspace using international experience. The priority directions of counteraction by the units of the National Police of Ukraine to the manifestations of sale and distribution of pornographic objects on the Internet have been determined. The conclusion is made about the necessity: 1) development of actual specialized software and hardware for carrying out operative-search activity in cyberspace with the use of international experience; 2) improvement of the system of information and analytical support (creation of the Unified information and analytical system of law enforcement agencies with subsystems by areas, including a separate unit for cybercrime control units); 3) amendments to the Criminal Procedure Code and other regulations in the field of combating cybercrime at the state level; 4) development at the international level and implementation into national legislation of procedural standards that allow to effectively investigate crimes in global information networks, to obtain, investigate and present electronic evidence taking into account the cross-border problem; 5) establishing cooperation between law enforcement agencies in

the investigation of cybercrime at the operational level; 6) improvement of mechanisms for joining materials and using electronic evidence in criminal proceedings in this category of criminal proceedings; 7) the obligation of companies to keep backup copies of electronic data to increase the efficiency of investigation of such crimes; 9) facilitating access of law enforcement agencies to electronic data banks.

Key words: international experience, pornography, pornography objects, Internet, sales, distribution, cyberspace.

MIĘDZYNARODOWE DOŚWIADCZENIE W PRZECIWDZIAŁANIU OBROTOWI PRZEDMIOTÓW PORNOGRAFICZNYCH PRZEZ INTERNET I JEGO WYKORZYSTANIE W CZYNNOŚCIACH OPERACYJNYCH I ŚLEDCZYCH JEDNOSTEK POLICJI NARODOWEJ UKRAINY

Alona Shraho
adiunkt Katedry Działalności Operacyjno-Poszukiwawczej
Dniepropetrowskiego Państwowego Uniwersytetu Spraw Wewnętrznych (Dniepr, Ukraina)
ORCID ID: 0000-0002-2375-8231

Adnotacja. Znaczenie tego artykułu polega na tym, że szeroki rozgłos licznych faktów działań lubieżnych popełnionych podczas korzystania z Internetu, wielki publiczny rezonans i zwiększona uwaga społeczności międzynarodowej zmusiły państwo do uznania istnienia problemu pornografii internetowej. Rozpowszechnianie pornografii przez Internet gwarantuje dystrybutorowi i konsumentowi anonimowość, względną dostępność sposobów jej upublicznienia i otrzymania. Szeroki popyt na produkty przestępcze utrudnia znalezienie dystrybutorów i sprzedawców takich produktów, szczególnie wśród obcokrajowców. W pracy przeanalizowano odrębne przepisy prawa międzynarodowego i krajowego dotyczące przeciwdziałania cyberprzestępczości i pornografii. Zauważono potrzebę opracowania odpowiedniego specjalistycznego oprogramowania i sprzętu do prowadzenia działań poszukiwawczych w cyberprzestrzeni z wykorzystaniem międzynarodowego doświadczenia. Ustalono priorytetowe kierunki przeciwdziałania oddziałami Policji Narodowej Ukrainy przejawom sprzedaży i dystrybucji przedmiotów pornograficznych w Internecie. Wywnioskowano o potrzebie: 1) opracowania odpowiedniego specjalistycznego oprogramowania i sprzętu do prowadzenia działań operacyjnych i poszukiwawczych w cyberprzestrzeni z wykorzystaniem międzynarodowego doświadczenia; 2) poprawy systemu wsparcia informacyjno-analitycznego (stworzenie jednolitego systemu informacyjno-analitycznego organów ścigania z podsystemami na obszarach, w tym z oddzielną jednostką dla jednostek zwalczania cyberprzestępczości); 3) wprowadzenia zmian w Kodeksie Postępowania Karnego i innych przepisach prawnych w zakresie przeciwdziałania cyberprzestępczości na poziomie państwowym; 4) opracowywania na poziomie międzynarodowym i wdrażania standardów proceduralnych w prawie krajowym, które pozwalają skutecznie badać przestępstwa w globalnych sieciach informacyjnych, uzyskiwać, badać i przedstawiać dowody elektroniczne z uwzględnieniem problemu transgranicznego; 5) nawiązywania współpracy organów ścigania w dochodzeniu w sprawie cyberprzestępczości na poziomie operacyjnym; 6) doskonalenia mechanizmów dołączania do materiałów i wykorzystywania w postępowaniach karnych dowodów elektronicznych w tej kategorii postępowań karnych; 7) zobowiązania firm do przechowywania kopii zapasowych danych elektronicznych w celu zwiększenia skuteczności dochodzenia w sprawie takich przestępstw; 9) ułatwienia organom ścigania dostępu do elektronicznych banków danych.

Słowa kluczowe: doświadczenia międzynarodowe, pornografia, przedmioty pornograficzne, Internet, sprzedaż, dystrybucja, cyberprzestrzeń.

Постановка проблеми. Широкий розголос численних фактів розпусних дій, скоєних під час використання мережі Інтернет, великий суспільний резонанс і підвищена увага міжнародної спільноти змусили державу визнати існування проблеми web-порнографії. Розповсюдження порнографії, що здійснюється мережею Інтернет, гарантує розповсюджувачу та споживачеві анонімність, відносну доступність способів її оприлюднення та отримання. Широкий попит на злочинну продукцію ускладнює пошук розповсюджувачів та реалізаторів такої продукції, особливо серед іноземців.

Аналіз останніх досліджень. Методологічним підґрунтям нашого дослідження є праці провідних вітчизняних і зарубіжних вчених у галузі ОРД, кримінального права та процесу, криміналістики (Ю. Аленін, В. Бахін, Р. Бєлкін, І. Возгрін), а також тих, хто безпосередньо студіював проблеми web-порнографії (А. Волобуєв, С. Денисов, Р. Джинджолія, М. Коллінз, С. Кондраніна, О. Манжай, Д. Паляничко, А. Старушкевич, І. Сугаков, О. Хабаров, С. Хільченко) та ін.

Водночас потребують поглибленого та системного дослідження питання протидії цим злочинам у міжнародному аспекті, а також спроби пошуку дієвих юридичних механізмів, здатних врегулювати Інтернет-відносини та запобігти збуту та розповсюдженню порнографічних предметів у мережі Інтернет.

У зв'язку із цим здійснимо спробу дослідити теоретичні, практичні та технічні проблеми правового регулювання проблемних питань протидії кіберзлочинності в аспекті web-порнографії у розрізі міжнародного досвіду та його імплементації, запропонувати комплекс заходів, що дозволив би ефективно протидіяти зазначеній проблемі.

Метою статті є компаративне дослідження теоретико-прикладних проблем, пов'язаних із вивченням міжнародного досвіду протидії обігу порнографічних предметів мережею інтернет та можливостей його використання в діяльності оперативних та слідчих підрозділів національної поліції, визначення комплексу заходів ефективної протидії цьому злочину. Розв'язання поставленої мети зумовлює вирішення таких

завдань: 1) проаналізувати окремі положення міжнародного та вітчизняного законодавства щодо протидії кіберзлочинності та порнографії; 2) запропонувати ефективні правові механізми реалізації організаційно-тактичних основ здійснення заходів із виявлення та розслідування фактів збуту й розповсюдження порнографії в кіберпросторі; 3) визначити пріоритетні напрямки протидії підрозділами Національної поліції України проявам збуту та розповсюдження порнографічних предметів в Інтернет.

23 листопада 2001 року в Будапешті підписана Конвенція Ради Європи про кіберзлочинність (далі – Конвенція), яка була прийнята для протидії комп'ютерним злочинам та для співробітництва й координації діяльності правоохоронних органів різних держав. На сьогодні ратифікована 18 та підписана 25 країнами, у т.ч. й Україною (7 вересня 2005 року) (Pro ratyfikatsiiu Dodatkovoho protokolu do Konventsii pro kiberzlochynnist, yakyi stosuietsia kryminalizatsii dii rasystskoho ta ksenofobnoho kharakteru, vchynenykh cherez kompiuterni systemy, 2006).

Так, у 2017 році прийнято ЗУ «Про основні засади забезпечення кібербезпеки в Україні». У пункті 8 статті 1 наведено визначення поняття кіберзлочин (комп'ютерний злочин) – суспільно небезпечне винне діяння в кіберпросторі та/або з його використанням, відповідальність за яке передбачена законом України про кримінальну відповідальність та/або яке визнано злочином міжнародними договорами України (Pro osnovni zasady zabezpechennia kiberbezpeky v Ukraini, 2017).

Як свідчить аналіз досвіду роботи поліції зарубіжних країн, організаційно боротьба зі злочинами у сфері високих технологій забезпечується двома основними способами: 1) покладення додаткових функцій на вже наявні підрозділи, або 2) створення спеціалізованих галузевих служб.

Виокремлення підрозділів боротьби зі злочинами у сфері високих технологій у спеціалізовані галузеві служби запроваджено в Австралії, Бельгії, Білорусі, Великобританії, Данії, Естонії, Індії, Китаї, Нідерландах, Німеччині, Норвегії, США, Швейцарії, Швеції та ін. (Tropina, 2017; McKenzie, 2006; Mark et al., 2017; Long et al., 2016). Заслуговує на увагу досвід Канадської асоціації провайдерів, якою розроблено Кодекс поведінки в Інтернеті в якості заходу, що дозволяє створити систему саморегулювання і не допустити передачу сумнівних матеріалів. Його мета – допомогти членам Асоціації в дотриманні правових стандартів у роботі. У Франції існує Хартія інтернет, у якій визначаються добровільні обов'язки користувачів і провайдерів в інтернеті. У Німеччині провайдери інтернет зорганізувалися у Freiwillige Selbstcontrolle Multimedia Dienstleanbieter (FSM) – Спілку добровільного саморегулювання служб мультимедіа (Ivanov, 2002). Проте, використання системи Інтернет для розповсюдження порнографії призводить до появи нових способів боротьби зі злочинцями.

Ключову роль у питаннях регулювання контенту в мережі грають не державні органи, а благодійний Фонд спостереження за Інтернетом (Internet Watch Foundation), заснований в 1996 році. Функція IWF зводиться до ведення реєстру заборонених сайтів, що являє собою набір посилань, переважно пов'язаних із дитячою порнографією (Internet Watch Foundation: Homepage, 2020). У свою чергу, в інтернет-провайдерів встановлене спеціальне програмне забезпечення Cleanfeed, яке покликане блокувати доступ до заборонених сайтів. Технічна реалізація системи виглядає таким чином. Існує конфіденційний список заборонених інтернет-сторінок (не сайтів), доступ до якого є тільки у фахівців IWF. Він не доступний ні провайдерам, ні рядовим користувачам. Провайдерам надається список IP-адрес сайтів, на яких розміщені дані сторінки, для того, щоб саме до цих адрес застосовувалися правила фільтрації. Провайдери перенаправляють трафік, що йде на ці адреси, на спеціальні проксі-сервери, які порівнюють HTTP-запити з адресами сторінок, що містяться в реєстрі заборонених адрес. Якщо вони не збігаються – трафік проходить фільтр і користувач потрапляє на запитувану сторінку. Робота Cleanfeed здійснюється у два етапи: 1. Перевірка IP-Адреси, до якої звернений запит. 2. Порівняння сторінки, до якої звертається користувач, зі списком адрес у реєстрі заборонених ресурсів (Havrysh et al. 2017).

Аналіз діяльності підрозділів кіберзлочинності показав, що в умовах сьогодення гострою проблемою міжнародного співробітництва є розбіжності законодавства різних країн та практики його застосування. Таку думку підтримали опитані нами працівники підрозділів протидії кіберзлочинності (75% опитаних) та слідчих (68% опитаних), що спеціалізуються на розслідуванні кіберзлочинів.

У США дитяча порнографія вважається злочином. П. 2252 гл. 110 Федерального кримінального кодексу США забороняє перевезення, відправку чи отримання дитячої порнографії каналами зв'язку, у т.ч. поштові та комп'ютерні засоби (The Legal Regulation of Cybercrime in the United States of America Legislation, 2017). У Данії, у 1998 р. Національний комісаріат поліції відкрив у Інтернет власну веб-сторінку, що дало можливість поліції отримувати від громадян інформацію про дитячу порнографію (Danish police, 1998).

Законодавство Японії карає позбавленням волі на строк до трьох років осіб, які розповсюджують через Інтернет порнографічні зображення дітей (Tsuda, 1997). Канада прийняла закон, згідно з яким пошук дитячої порнографії в Інтернеті – кримінально каране діяння, навіть якщо обвинувачений нічого не знайшов. Порушнику загрожує позбавлення волі до п'яти років (A review of section 264 (criminal harassment) of the Criminal Code of Canada, 1996).

Боротьба з кіберзлочинністю неможлива без глибокого розуміння і правових проблем регулювання інформаційних мереж. У межах проведеного нами опитування працівників кіберполіції НП України та слідчих НП, які спеціалізуються на даному виді злочинів, 29% респондентів вказали на те, що вони мають складність із визначенням предмету комп'ютерного злочину у сфері протидії порнографії, 23% – не мають достатніх спеціальних знань, 10% – не знають про існування наукових рекомендацій, 19% – покладаються на власний досвід, 19% – не використовують методичні рекомендації, бо вважають застарілими. Проведене дослідження вказує на те, що слідчі та оперативні працівники НП все ще не готові до ефективного розкриття

та розслідування подібних злочинів, що є однією із причин низької ефективності розкриття та розслідування злочинів, пов'язаних зі збутом і розповсюдженням порнографічних предметів у мережі Інтернет.

Аналіз спеціальної літератури таких авторів, як Alisdair A. Gillespie, Colton Fehr, Melissa Wells, David Finkelhor, Janis Wolak&Kimberly J. Mitchell та міжнародного досвіду (A Proposal for Police Acquisition of ISP Subscriber Information on Administrative Demand in Child Pornography Investigations, 2019; Gillespie, 2017; Wells et al., 2017), а також опитування працівників кіберполіції та слідчих, що спеціалізуються на розслідуванні злочинів, пов'язаних зі збутом і розповсюдженням порнографічних предметів у мережі Інтернет свідчить, що існує низка проблем, пов'язаних із використанням спеціальних знань з метою пошуку, виявлення, фіксації, вилучення та дослідження слідів даної категорії злочинів відповідно до способів їх утворення на початковому етапі розслідування кримінальних проваджень.

Так, аналіз матеріалів кримінальних проваджень показав, що однією з актуальних проблем протидії цим злочинам є належна та ефективна діяльність щодо виявлення у мережі Інтернет розповсюджувачів порносайтів. Так, аналіз практики протидії кіберзлочинам дозволив виокремити узагальнені способи виявлення кінцевого користувача та розповсюджувача, а також визначити наявні проблеми. Зокрема, провайдер здійснює підключення абонентів 2 способами: 1) з використанням пароля і логіна і 2) без нього. У другому випадку йому потрібна тільки mac-адреса мережевого обладнання абонента (mac-адреса роутера або мережевої картки ПК/ноутбука). Провайдер надає абоненту IP-адресу, яка при відвідуванні веб-ресурсів або сайтів зберігається на сервері/хостингу даних веб-ресурсів або сайтів, відтак, щоб встановити абонента, правоохоронні органи запитують у власника сервера/хостингу IP-адресу, з якої відвідував або реєструвався користувач мережі Інтернет. Однак, знаючи IP-адресу, правоохоронні органи встановлюють провайдера, який надає його абоненту та, відповідно до чинного законодавства, отримують інформацію про абонента. Отже, інформація спочатку спрямовується до провайдера, а від нього – до індивідуальних користувачів. Це дозволяє відшукати конкретний комп'ютер, на який надходила інформація з порносайту.

Однак якщо користувач використовує технологію VPN, яка дозволяє об'єднати декілька географічно віддалених мереж (або окремих клієнтів) в єдину мережу з використанням для зв'язку між ними непідконтрольних каналів, TOR-браузеру, proxy-серверу, що створені для забезпечення анонімності в мережі Інтернет тощо, то на сервері/хостингу користувача відображається не справжня IP-адреса, а IP-адреса засобів анонімності (VPN, TOR, proxy і т.п.). І саме ця обставина ставить під сумнів сам механізм відстеження злочинців у подібний спосіб (таку позицію висловили 90% працівників кіберполіції).

На наш погляд, у цьому контексті доцільним може бути дозвіл провайдерам на ініціювання зняття/вимкнення/блокування сайту, що містить відповідні факти його неправомірності, із подальшим зверненням до суду та прийняттям остаточного рішення. Таку думку підтримали опитані нами працівники підрозділів протидії кіберзлочинності (65% опитаних) та слідчих (68% опитаних), що спеціалізуються на розслідуванні кіберзлочинів.

Криміналістична особливість кіберзлочинів у тому, що їх припинення та розслідування неможливе без використання комп'ютерних технологій. Оперативний пошук має включати низку заходів, які фактично є оперативно-розшуковими (оперативно-пошукові заходи із забезпечення оперативної закупівлі та (або) контрольованого постачання товарів, заборонених для відкритого обігу; **оперативне впровадження у віртуальні соціальні групи**, що мають деструктивні цілі, з метою отримання інформації про їх персональний склад, місця зустрічей, плани та засоби, що використовуються в деструктивній діяльності; оперативно-аналітичні заходи, спрямовані на прогноз розвитку ситуації, розробки заходів з утримання її під контролем, **заходи оперативно-технічного характеру**) і проводитись він має лише тими правоохоронними органами, до компетенції яких віднесено проведення ОРД та (або) НСРД. Вказана позиція напряму випливає з рішення Конституційного суду України від 20.10.2011 № 12рп/2011 по справі № 1-31/2011 за конституційним поданням СБУ щодо офіційного тлумачення ч. 3 ст. 62 Конституції України, яким вирішено, що «в аспекті конституційного подання щодо суб'єктів одержання доказів у кримінальній справі в результаті здійснення оперативно-розшукової діяльності положення першого речення частини третьої статті 62 Конституції України, відповідно до якого обвинувачення не може ґрунтуватися на доказах, одержаних незаконним шляхом, слід розуміти так, що обвинувачення у вчиненні злочину не може ґрунтуватися на фактичних даних, одержаних у результаті оперативно-розшукової діяльності уповноваженою на те особою без дотримання конституційних положень або з порушенням порядку, встановленого законом, а також одержаних шляхом вчинення цілеспрямованих дій щодо їх збирання і фіксації із застосуванням заходів, передбачених Законом України «Про оперативно-розшукову діяльність», особою, не уповноваженою на здійснення такої діяльності» (Rishennia Konstytutsiinoho sudu Ukrainy, 2011).

Із введенням в дію КПК України значно ускладнилася процедура отримання інформації від провайдерів телекомунікаційних послуг. Якщо раніше отримання такої інформації здійснювалося на підставі положень про «Конвенцію про кіберзлочинність» і Закону України «Про міліцію», то зараз така інформація віднесена до категорії документів, що містять охоронювану законом таємницю. А в розумінні статті 505 Цивільного кодексу України така інформація становить комерційну таємницю, яка є одним із об'єктів інтелектуальної власності. Тому суб'єкти протидії позбавлені можливості оперативно і своєчасно отримувати необхідну інформацію через запити правоохоронних органів. Сьогодні рівень і темпи зростання кіберзлочинності вимагають адекватного реагування, в тому числі і на законодавчому рівні. А тому потребують змін положення законодавства про порядок і підстави виконання запитів, отриманих від правоохоронних органів у рамках виконання зобов'язань України, взятих у зв'язку з ратифікацією «Конвенції про кіберзлочинність». Крім того, нагальною проблемою,

про яку зазначають 90% опитаних нами оперативних працівників та 98% слідчих, є поширеність подання сторонами електронних доказів у кримінальних провадженнях, що зумовлено особливостями окремих видів злочинів, спосіб вчинення яких безпосередньо передбачає використання тих приладів та пристроїв, які оперують інформацією в електронному (цифровому) вигляді. Унаслідок цього фактичні дані, на підставі яких слідчий (прокурор) встановлюють наявність чи відсутність фактів та обставин, що мають значення для кримінального провадження та підлягають доказуванню, існують саме в електронній (цифровій) формі.

Ураховуючи викладене, пропонуємо доповнити пункти 1, 7 частини 1 статті 162 Кримінального процесуального кодексу України та викласти їх у такій редакції:

«Стаття 162. Речі і документи, **інформація в електронній (цифровій) формі,** які містять охоронювану законом таємницю

1. До охоронюваної законом таємниці, яка міститься в речах і документах, належать:

1) інформація, **в тому числі в електронній (цифровій) формі,** що знаходиться у володінні засобу масової інформації або журналіста і надана їм за умови нерозголошення авторства або джерела інформації;

7) інформація, **в тому числі в електронній (цифровій) формі,** яка знаходиться в операторів та провайдерів телекомунікацій, **охороняється Законом України «Про захист персональних даних» або передається та зберігається за таких фізичних чи юридичних умов, за яких учасники спілкування можуть розраховувати на захист інформації від втручання інших осіб».**

Крім того, внести відповідні зміни до Закону України «Про телекомунікації» та частину 4 статті 39 викласти в такій редакції:

«Стаття 39. Обов'язки операторів і провайдерів телекомунікацій.

4. Оператори телекомунікацій зобов'язані за власні кошти встановлювати на своїх телекомунікаційних мережах технічні засоби, необхідні для здійснення **уповноваженими підрозділами оперативно-розшукових заходів, негласних слідчих (розшукових) дій та тимчасового доступу до інформації, яка знаходиться в операторів та провайдерів телекомунікацій, про зв'язок, абонента, надання телекомунікаційних послуг, у тому числі отримання послуг, їх тривалості, змісту, маршрутів передавання тощо,** і забезпечувати функціонування цих технічних засобів, а також у межах своїх повноважень сприяти проведенню оперативно-розшукових заходів**, негласних слідчих (розшукових) дій та тимчасового доступу до інформації, яка знаходиться в операторів та провайдерів телекомунікацій, про зв'язок, абонента, надання телекомунікаційних послуг, у тому числі отримання послуг, їх тривалості, змісту, маршрутів передавання тощо, а також** недопущенню розголошення організаційних і тактичних прийомів їх проведення. Оператори телекомунікацій зобов'язані забезпечувати захист зазначених технічних засобів від несанкціонованого доступу».

Як наслідок, одним із пріоритетних напрямків є організація взаємодії і координація зусиль правоохоронних органів, спецслужб, судової системи, забезпечення їх необхідною матеріально-технічною базою. Сьогодні жодна держава не може ефективно протистояти кіберзлочинності самостійно. Нагальною є необхідність активізації міжнародної співпраці в цій сфері та приведення у відповідність національного законодавства.

Висновки. Отже, сьогодні для суб'єктів ОРД необхідною є розробка організаційно-тактичних основ проведення оперативно-розшукової діяльності у кіберпросторі та введення в дію відповідних правових механізмів їх здійснення.

Окрім того, в контексті проведеного дослідження, необхідним є: 1) розробка актуального спеціалізованого програмного та апаратного забезпечення для провадження оперативно-розшукової діяльності в кіберпросторі з використанням міжнародного досвіду; 2) удосконалення системи інформаційно-аналітичного забезпечення (створення Єдиної інформаційно-аналітичної системи правоохоронних органів із підсистемами за напрямами, у тому числі з окремим блоком для підрозділів боротьби з кіберзлочинністю); 3) внесення змін до КПК та інших нормативно-правових актів у сфері протидії кіберзлочинам на державному рівні; 4) розробка на міжнародному рівні та імплементація в національне законодавство процесуальних стандартів, що дозволяють ефективно розслідувати злочини в глобальних інформаційних мережах, отримувати, досліджувати і представляти електронні докази з урахуванням транскордонної проблеми; 5) налагоджене співробітництво правоохоронних органів при розслідуванні кіберзлочинів на оперативному рівні; 6) удосконалення механізмів долучення до матеріалів та використання у кримінальних провадженнях електронних доказів за цією категорією кримінальних проваджень; 7) зобов'язання компаній зберігати резервні копії електронних даних для підвищення ефективності розслідування таких злочинів; 8) полегшення доступу правоохоронних органів до електронних банків даних.

Проведене нами системне і комплексне узагальнення наявних проблем щодо розповсюдження порнографії мережею Інтернет, а також аналіз міжнародного досвіду протидії порнографії, врахування думок практиків, особистий досвід виявлення та розслідування злочинів дозволили запропонувати можливі ефективні напрямки такої протидії:

1) створення нормативної бази, яка б забезпечила нормальну діяльність користувачів Інтернет і звела нанівець можливі правопорушення;

2) посилення санкцій щодо правопорушників;

3) прийняття кодексу поведінки провайдерів в Інтернет та надання їм певних повноважень щодо ініціювання питання про блокування сайту;

4) створення відповідних умов для підготовки кваліфікованих фахівців-правоохоронців із досвідом роботи у IT-сфері;

5) заборона на законодавчому рівні створювати порносайти зі співзвучними доменними назвами Інтернет-ресурсів загального користування;

6) координація зусиль правоохоронців у протидії розповсюдженню порнографічних матеріалів та укладання двосторонніх і багатосторонніх договорів, міжвідомчих угод про співпрацю;

8) юридичне визначення поняття порнографії та ратифікація змін до ст. 34 Конвенції про права дитини;

9) визнання мережі Інтернет засобом масової інформації.

Провівши дане дослідження, ми дійшли висновку, що вирішення, зокрема й окреслених проблемних питань, сприятиме підвищенню ефективності діяльності оперативних та слідчих підрозділів НП України, спрямованої на протидію злочинам у сфері суспільної моралі, а відтак окреслені питання вимагають подальшого поглибленого науково-практичного дослідження.

Список використаних джерел:

1. Іванов В. Правове регулювання інтернет. Деякі аспекти. *Права Людини в Україні. Інформаційний портал Харківської правозахисної групи.* URL : http://khpg.org/index.php?id=1039006699.
2. Особливості виявлення фактів, пов'язаних із незаконним розповсюдженням медійного контенту в мережах провайдерів програмної послуги та інтернет-провайдерів, мережі інтернет: методичні рекомендації / Гавриш О.С., Краснобрижий І.В., Мирошниченко В.О., Прокопов С.О., Рижков Е.В. Дніпро : Дніпроп. держ. ун-т, внутр. справ, 2017. 44 с.
3. Про основні засади забезпечення кібербезпеки в Україні : Закон України від 05.10.2017 № 2163-VIII. *Відомості Верховної Ради України*. 2017. № 45. Ст. 403.
4. Про ратифікацію Додаткового протоколу до Конвенції про кіберзлочинність, який стосується криміналізації дій расистського та ксенофобного характеру, вчинених через комп'ютерні системи : Закон України від 21 липня 2006 р. № 23-V. *Відомості Верховної Ради України*. 2006. № 39. С. 1384. Ст. 328.
5. Рішення Конституційного суду України від 20.10.2011 № 12рп/2011. *Відомості Верховної Ради України*. 2011. URL : https://zakon.rada.gov.ua/laws/show/v012p710-11#Text.
6. Tatiana Tropina (2017)**.** Cyber-policing: the role of the police in fighting cybercrime. URL : http://91.82.159.234/index.php/bulletin/article/view/232.
7. A Proposal for Police Acquisition of ISP Subscriber Information on Administrative Demand in Child Pornography Investigations // Colton Fehr 16 Pages Posted:19 Jun 2019. URL : https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3402632.
8. A review of section 264 (criminal harassment) of the Criminal Code of Canada. URL : https://justice.gc.ca/eng/rp-pr/cj-jp/fv-vf/wd96_7-dt96_7/wd96_7.pdf.
9. Child pornography Alisdair A. Gillespie. URL : https://www.tandfonline.com/doi/abs/10.1080/13600834.2017.1393932.
10. Danish police/ Politi. URL : https://politi.dk/en.
11. Defining Child Pornography: Law Enforcement Dilemmas in Investigations of Internet Child Pornography Possession Melissa Wells , David Finkelhor, Janis Wolak &Kimberly J. Mitchell Pages 269-282. Published online: 12 Jul 2007. URL : https://doi.org/10.1080/15614260701450765.
12. Internet Watch Foundation: Homepage. URL : https://www.iwf.org.uk/.
13. Long, M., Alison, L., Tejeiro, R., Hendricks, E., & Giles, S. (2016). KIRAT: Law enforcement's prioritization tool for investigating indecent image offenders. Psychology, Public Policy, and Law, 22(1), 12–21. URL : https://doi.org/10.1037/law0000069.
14. Mark H. Butler, Samuel A. Pereyra, Thomas W. Draper, Nathan D. Leonhardt &Kevin B. Skinner Pages 127-137 // 27 Apr 2017, Published online: 08 Jun 2017. URL : https://doi.org/10.1080/0092623X.2017.1321601.
15. McKenzie, S. E. H. (2006). Partnership policing of electronic crime: an evaluation of public and private police investigative relationships. PhD thesis, Department of Criminology, University of Melbourne. URL : http://hdl.handle.net/11343/39159.
16. The Legal Regulation of Cybercrime in the United States of America Legislation // Journal. – No: 27. – VIII/2017. – page 1576-1578. URL : https://www.ceeol.com/search/article-detail?id=607305.
17. Tsuda, Mamory. Human rights problems of foreigners in Japan's criminal justice system. Migration World Magazine, Sage Publications, Inc. vol. 24, No 1-2. 1997. p. 22+. Accessed 20 Oct. 2020.

References:

1. Ivanov V. (2002). Pravove rehuliuvannia internet. Deiaki aspekty. *Prava Liudyny v Ukraini. Informatsiinyi portal Kharkivskoi pravozakhysnoi hrupy.*
2. Havrysh O.S., Krasnobryzhyi I.V., Myroshnychenko V.O., Prokopov S.O., Ryzhkov E.V. (2017). Osoblyvosti vyiavlennia faktiv, poviazanykh iz nezakonnym rozpovsiudzhenniam mediinoho kontentu v merezhakh provaideriv prohramnoi posluhy ta internet-provaideriv, merezhi internet [Features of detection of facts related to illegal distribution of media content in the networks of software service providers and Internet providers, the Internet: guidelines]: metodychni rekomendatsii. Dnipro: Dniprop. derzh. un-t, vnutr. sprav, 2017. 44 p.
3. Pro osnovni zasady zabezpechennia kiberbezpeky v Ukraini [On the basic principles of cybersecurity in Ukraine]: Zakon Ukrainy vid 05.10.2017 № 2163-VIII // Vidomosti Verkhovnoi Rady Ukrainy. 2017. № 45. St. 403.
4. Pro ratyfikatsiiu Dodatkovoho protokolu do Konventsii pro kiberzlochynnist, yakyi stosuietsia kryminalizatsii dii rasystskoho ta ksenofobnoho kharakteru, vchynenykh cherez kompiuterni systemy [On the basic principles of cybersecurity in Ukraine]: Zakon Ukrainy vid 21 lypnia 2006 r. № 23-V // Vidomosti Verkhovnoi Rady Ukrainy. 2006. № 39. S. 1384. St. 328.

5. Rishennia Konstytutsiinoho sudu Ukrainy [Decision of the Constitutional Court of Ukraine] vid 20.10.2011 № 12rp/2011 // Vidomosti Verkhovnoi Rady Ukrainy. 2011.
6. Tatiana Tropina (2017). Cyber-policing: the role of the police in fighting cybercrime. URL: http://91.82.159.234/index.php/bulletin/article/view/232.
7. A Proposal for Police Acquisition of ISP Subscriber Information on Administrative Demand in Child Pornography Investigations // Colton Fehr 16 Pages Posted:19 Jun2019. URL: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3402632
8. A review of section 264 (criminal harassment) of the Criminal Code of Canada. URL: https://justice.gc.ca/eng/rp-pr/cj-jp/fv-vf/wd96_7-dt96_7/wd96_7.pdf.
9. Child pornography Alisdair A. Gillespie. URL: https://www.tandfonline.com/doi/abs/10.1080/13600834.2017.1393932.
10. Danish police/ Politi. URL: https://politi.dk/en.
11. Defining Child Pornography: Law Enforcement Dilemmas in Investigations of Internet Child Pornography Possession Melissa Wells , David Finkelhor, Janis Wolak &Kimberly J. Mitchell Pages 269-282. Published online: 12 Jul 2007. URL: https://doi.org/10.1080/15614260701450765.
12. Internet Watch Foundation: Homepage. URL: https://www.iwf.org.uk/.
13. Long, M., Alison, L., Tejeiro, R., Hendricks, E., & Giles, S. (2016). KIRAT: Law enforcement's prioritization tool for investigating indecent image offenders. Psychology, Public Policy, and Law, 22(1), 12–21. URL: https://doi.org/10.1037/law0000069.
14. Mark H. Butler, Samuel A. Pereyra, Thomas W. Draper, Nathan D. Leonhardt &Kevin B. Skinner Pages 127-137 // 27 Apr 2017, Published online: 08 Jun 2017. URL: https://doi.org/10.1080/0092623X.2017.1321601.
15. McKenzie, S. E. H. (2006). Partnership policing of electronic crime: an evaluation of public and private police investigative relationships. PhD thesis, Department of Criminology, University of Melbourne. URL: http://hdl.handle.net/11343/39159.
16. The Legal Regulation of Cybercrime in the United States of America Legislation // Journal. – No: 27. – VIII/2017. – page 1576-1578. URL: https://www.ceeol.com/search/article-detail?id=607305.
17. Tsuda, Mamory. Human rights problems of foreigners in Japan's criminal justice system. Migration World Magazine, Sage Publications, Inc. vol. 24, No 1-2. 1997. p. 22+. Accessed 20 Oct. 2020.

DOI https://doi.org/10.51647/kelm.2020.3.2.49

КЛАСИФІКАЦІЯ СУСПІЛЬНО НЕБЕЗПЕЧНИХ НАСЛІДКІВ КРИМІНАЛЬНОГО ПРАВОПОРУШЕННЯ

Ірина Щербініна
аспірант кафедри кримінального права № 2
Національного юридичного університету імені Ярослава Мудрого (Харків, Україна)
ORCID ID: 0000-0001-6376-3951

Анотація. Стаття присвячена дослідженню актуальних проблем класифікації суспільно небезпечних наслідків кримінального правопорушення. Особлива увага автором звертається на необхідність вироблення наукою повної, точної та універсальної системи класифікації суспільно небезпечних наслідків, яка б обов'язково відповідала принципу науковості та правилам формальної логіки. Встановлено, що при відборі класифікаційних критеріїв для поділу суспільно небезпечних наслідків кримінального правопорушення на види необхідно керуватися найбільш істотними та універсальними ознаками, які б надали змогу поділити усю сукупність суспільно небезпечних наслідків за тими чи іншими суттєвими критеріями. Автором були розглянуті різні підходи та критерії класифікацій суспільно небезпечних наслідків, запропоновані вітчизняними та закордонними вченими-криміналістами. Встановлено, що не усі критерії поділу можна вважати такими, що розкривають реальні, сутнісні характеристики дослідженого явища. На підставі глибокого аналізу законодавчих та доктринальних положень автором запропонована вдосконалена система поділу суспільно небезпечних наслідків кримінального правопорушення, що здатна більш повно, об'єктивно розкрити найважливіші якісні та кількісні характеристики досліджуваного явища та продемонструвати співвідношення суспільно небезпечних наслідків з об'єктами кримінального правопорушення.

Ключові слова: кримінальне правопорушення, класифікація, суспільно небезпечні наслідки, делікти створення небезпеки, істотна шкода, шкода.

THE CLASSIFICATION OF SOCIALLY DANGEROUS CONSEQUENCES OF THE CRIMINAL VIOLATION OF LAW

Iryna Shcherbinina
PhD Student at the Department of Criminal Law № 2
Yaroslav Mudryi National Law University (Kharkiv, Ukraine)
ORCID ID: 0000-0001-6376-3951

Abstract. The article is devoted to the investigation of challenging issues in the classification of socially dangerous consequences of the criminal violation of law. The particular attention of the author is dedicated to the necessity of setting up a full accurate and universal system of socially dangerous consequences of the criminal violation of law classification, which would certainly reflect the principles of science and the rules of regular logic. It was figured out that during