УДК 330.8 / 342.95
DOI https://doi.org/10.24144/2307-3322.2024.85.4.37

МІЖНАРОДНО-ПРАВОВИЙ АСПЕКТ ПРОТИДІЇ ДОКСИНГУ В ЦИФРОВУ ЕПОХУ

Ковальчук А.Ю.,
доктор юридичних наук, професор
ORCID: 0000-0003-4807-2436

Чернявська Б.В.,
PhD, доцент кафедри теорії та історії держави і права
Національної академії управління,
запрошений дослідник юридичного факультету
Вільного Університету Амстердаму
ORCID: 0000-0001-8263-7483

Ковальчук А.Ю., Чернявська Б.В. Міжнародно-правовий аспект протидії доксингу в цифрову епоху.

Авторами підіймається проблема забезпечення безпеки персональних даних, а саме їх складові – ідентифікуючої інформації у мережі Інтернет. Доксинг, як злочин, що виражається у незаконному зборі інформації і використання її у публічному просторі без дозволу на це власника, набув популярності у соціальних мережах де ідентифікуюча інформація може швидко розповсюджуватись і використовуватися проти жертв. Великі мовні моделі (LLM) та Штучний інтелект є елементами багатьох програмних забезпечень, який залучається з метою збереження персональних даних, разом з тим, вивчаючи масштабні витоки інформації, автори ставлять питання про відповідальність осіб, які не забезпечили їх збереження, особливо якщо кіберінцендент сталися у наслідок застосування ШІ. Такі негативні тенденції підживлює популяризація Штучного інтелекту. У 2023 році з'явилося кілька мовних моделей, завдяки яким стало можливим збирати інформацію, й узагальнювати її одночасно. Автори виражають серйозне занепокоєння щодо збереження конфіденційності даних користувачів та забезпеченні інформаційної безпеки в умовах розповсюдження пошуку інформації за відкритим кодом, та подальше використання отриманої інформації. В епоху, коли персональні дані є надзвичайно затребуваним товаром їх захист стає першочерговим завданням перед будь-якою державою. Виходячи з такої тези, автори ставлять перед собою мету – висвітлити й узагальнити зарубіжний досвід правового захисту права людини на приватність й врегулювання відносин щодо захисту персональної (ідентифікуючої) інформації в мережі Інтернет. Методологічну основу складають загальнонаукові методи пізнання, метод компаративістики й моделювання. У результаті автори роблять висновки про те, що кібератаки, викрадення персональних даних, активна популяризація розвідки з відкритих джерел, пронизування усіх соціально-економічних процесів засобами цифрової ідентифікації, розповсюдження Інтернету речей становлять реальні загрози для приватності особи і безпеки її ідентифікуючої інформації, як елементу персональних даних.

Ключові слова: безпека, загроза, вразливість, доксинг, персональні дані/ ідентифікуюча інформація, інформаційна безпека, кібервійна, кіберзлочини, кіберпереслідування.

Kovalchuk A.Yu., Cherniavska B.V. International legal aspects of combating doxing in the digital age.

The authors explore the issue of safeguarding personal data, particularly its identifying components, in the context of the Internet. Doxing, a criminal act involving the unauthorized collection of information and its public dissemination without the owner's consent, has gained significant traction on social media platforms, where identifying information can be quickly spread and misused against individuals. Large language models (artificial intelligence) are integrated into many software programs designed to

protect personal data. However, in light of large-scale data breaches, the authors raise concerns about the liability of entities or individuals who fail to adequately secure such data, especially when cyber incidents are linked to the use of AI. The rapid advancement and widespread use of artificial intelligence contribute to these growing concerns. In 2023, the emergence of several language models facilitated both the manipulation and aggregation of data, exacerbating the problem. The authors express serious concerns about ensuring user privacy and information security in a landscape increasingly shaped by open-source intelligence and the further exploitation of such data. In an era where personal data has become a highly valuable commodity, protecting it has become a priority for governments worldwide. In light of this, the authors aim to examine and synthesize international legal approaches to safeguarding the right to privacy and regulating the protection of personal (identifying) information on the Internet. The study relies on general scientific methods of inquiry, including comparative analysis and modelling. The authors conclude that cyberattacks, the theft of personal data, the increasing use of open-source intelligence, the penetration of digital identification technologies into all socio-economic processes, and the proliferation of the Internet of Things pose real threats to individual privacy and the security of identifying information as a critical component of personal data.

Key words: security, threat, vulnerability, doxing, personal data / identifying information, information security, cyberwar, cybercrime, cyberstalking.

Постановка проблеми. В епоху, коли цифровий простір став продовженням суспільного та приватного життя, існує нагальна потреба в правових реформах щодо захисту не лише персональних даних, конфіденційної інформації, але й ідентифікаційної інформації в мережі Інтернет. У багатьох контрактах, правилах і умовах використання продуктів Google [1] для аналітики й реклами згадується термін «ідентифікаційна інформація» яка набуває особливого значення. Особливим вважається те, що ця інформація відрізняється від «персональних даних», на які посилається Загальний регламент захисту даних ЄС (GDPR). Це інформація, за допомогою якої можна ідентифікувати особу в мережі Інтернет, зв'язатися з нею або точно визначити її місцезнаходження. Згідно формулювання довідкового центру Google така інформація включає: електронні адреси; поштові адреси; номери телефонів; точні місцеположення, як-от GPS-координати тощо [1]. Проблема на сьогодні полягає у можливостях несанкціонованого доступу до такої інформації. Великі мовні моделі виявилися трансформуючими в багатьох програмних забезпеченнях, що викликає серйозні занепокоєння щодо збереження приватності користувачів та забезпеченні особистої інформаційної безпеки. В епоху, коли персональні дані є і найзатребуванішим товаром, їх захист стає першочерговим завданням перед будь-якою державою.

Кібератаки, викрадення персональних даних, активна популяризація розвідки з відкритих джерел, пронизування усіх соціально-економічних процесів елементами штучного інтелекту, розповсюдження Інтернету речей становлять реальні загрози для приватності особи та збереженню їх персональних даних від злочинних посягань. У 2017 році злочинці зламали систему безпеки Equifax[1] та викрали персональну інформацію понад 145 мільйонів клієнтів компанії. У 2020 році стався один із найбільших витоків даних в історії. Хакерам вдалося потрапити в систему компанії CAM4 — платформи «для дорослих», яку відвідує понад 2 мільярди користувачів щорічно. У результаті витоку було відкрито 7 терабайтів даних, які включали імена та прізвища, IP-адреси, паролі, геолокацію та інші дані користувачів. В тому числі в руках хакерів опинилися близько 11 млрд. записів з електронними листами та хешованими паролями [2]. Кібератаки та витоки даних стають дедалі частим явищем для українців та українського бізнесу. Для розуміння масштабів можливих витоків даних слід розуміти, що користувачами лише мобільного застосунку «Дія» є 13,5 млн. українців. Можна з впевненістю сказати, що майже кожен українець хоча б раз у житті відображав ідентифікуючу інформацію про себе у кіберпросторі.

Мета статті полягає у проведені аналізу загроз приватності в Інтернеті, практику убезпечення ідентифікуючої інформації у мережі Інтернет, в зарубіжних країнах з метою захисту прав і свобод людини.

Окремо на наш погляд, потребує з'ясування питання чи визнається ідентифікаційна інформація, отримана приміром, за допомогою файлів cookies чи IP-адреса, з даних GPS-навігаторів,

[1] Equifax – американське бюро кредитної історії. Equifax збирає інформацію про більш ніж 800 мільйонів фізичних осіб і більш ніж 88 мільйонів компаній по всьому світу. URL:https://www.equifax.com.

getcontact тощо персональними даними особи і яка відповідальність становить за її розголошення й публічне поширення без згоди на те власника.

Стан опрацювання проблематики. Питанням правового захисту персональних даних присвячено багато наукових праць дослідників: В. Брижка, Д. Василенко, А. Гевлича, Ю. Крилової, А. Пазюка, В. Селиванова, В. Теремецького, А. Чернобая, В. Пилипчука, В. Проценко, М. Швеця та ін. Нині ж швидкі темпи розвитку інформаційно-комунікативних технологій, розповсюдження впровадження штучного інтелекту породили нові можливості для злочинних маніпуляцій з персоналізованою інформацією. Влучно цитує Ю. Крилова, статтю В. Брижка: «У нинішній час розповсюдження маркетингу, персональні дані зазнають найбільшої загрози. За оцінкою американських фахівців, річний ринок персональних даних складає не менш як 3 мільярдів доларів. Тобто нелегальний інформаційний бізнес спеціалізується на зборі, обробці і продажу персональних даних, застосовуючи при цьому засоби інформаційно-комп'ютерних технологій та телекомунікаційних мереж»[3]. Кримінальним кодексом України, КУпАП визначені протиправні діяння, але на сьогоднішній день, більшість вчених, зазначають про значні колізії й прогалини щодо захисту персональних даних. Питання ж ідентифікуючої інформації і її захисту підіймається лише технічними фахівцями.

Кримінально-правової характеристики кримінального правопорушення з точки зору порушення недоторканності приватного життя, передбаченого ст. 182 КК України, певною мірою розробляли такі вітчизняні і зарубіжні вчені, як: П.П. Андрушко, В.І. Антипов, А.П. Бабій, А.Л. Васін, Ю.В. Гродецький, О.І. Зінченко, М.В. Мазур, Л.Г. Мачковський, С.Х. Нафієв, І.Л. Петрухін, А.В. Савченко, О. Семенюк, В.І. Тютюгін, М.І. Хавронюк та ін. Питання яке залишилось поза увагою науковців, це розголошення і поширення ідентифікуючої інформації яку зібрано з відкритих джерел, але без прямої чи опосередкованої згоди на те власника даних. У європейських, американських наукових колах такий делікт – доксинг, визначається як кримінальний проступок. В Україні такий делікт не передбачений ані адміністративним кодексом, ані кримінальним.

Викладення основного матеріалу. На тлі тотальної цифровізації виникають поширення такого негативного явища як доксинг. Доксинг зазвичай включає в себе навмисне поширення в Інтернеті розкриття ідентифікаційної інформації, яка дозволяє ідентифікувати особу, без згоди, завдаючи жертві ризику емоційної, професійної та навіть фізичної шкоди. З початку 2020 року доксинг все частіше використовують як інструмент кіберсталкінгу, шахрайства та вчинення інших злочинів. Доксінг активно застосовують для цькування, переслідування людей за будь-які протилежні погляди. Доксинг (іноді можна зустріти як «доксінг») (від англ. «doxing» або «doxxing») – це практика збору, публікації та розповсюдження приватної, ідентифікуючої інформації про людину без її згоди, з метою завдання шкоди, залякування або завдання репутаційних втрат. Фахівці Харківський національний університет імені В.Н. Каразіна Колованова Є.П., Малахов С.В., Чорна Т.Е. аналізуючи значний обсяг технічної літератури, та практики доксингу виділяють основні методи які використовуються доксерами для збору даних: відстеження імен користувачів; переслідування в соціальних мережах; пошук WHOIS по доменному імені; фішинг; відстеження IP-адрес; зворотній пошук мобільного телефону; аналіз пакетів (парсинг та сниффинг(аналіз трафіку)); аналіз і узагальнення вмісту й структури даних таргетованих сайтів (сайт парсинг); використання т.з. «брокерів даних» тощо [4]. Така варіативність збору ідентифікуючої інформації свідчить про популярність збору інформації, інше питання як ця інформація використовується.

Доксинг набув популярності соціальних мережах де ідентифікуюча інформація може швидко розповсюджуватись і використовуватись проти жертв. Такі негативні тенденції підживлює розповсюдження Штучного інтелекту. У 2023 році з'явилося кілька мовних моделей [5], які стало можливим використовувати для доксінгу. Наприклад, чат-бот генерує реалістичні листи від банків чи державних органів нібито для уточнення інформації. Так жертва сама віддає приватні дані шахраєві. Дехто вважає ці моделі чудовими хаками для продуктивності, які революціонізують шахрайські методи та майже «автоматизують» створення текстів, коду, документів, маркетингових кампаній тощо [5; 6]. Сучасні пошукові Інтернет сервіси це теж алгоритми з елементами штучного інтелекту, що складаються з двох складових: акумулювання бази даних та система запит-відповідь. Пошукові сервіси постійно сканують мережу на предмет нових сайтів, індексують та вносять їх до бази даних, відстежують зміни, ведуть статистику, оцінюють корисність та безпечність сайтів для користувачів. Для пошуку інформації використовуються запити. Самі по собі запиті можуть не ідентифікувати користувача, однак за наявності контек-

сту чи у сукупності це може стати можливим. Наприклад, за сукупністю запитів «Купити дитячу коляску, Київ», «Задня ліва фара Audi A4 B8» та «Туристичні місця, Львів» можливо зробити припущення, які допоможуть ідентифікувати особу з великою ймовірністю. І з кожним запитом точність ідентифікації зростатиме. Наприклад Google формує перелік асоціацій та вподобань кожного користувача на основі частих, та цікавих користувачу запитів. Таким чином в акаунті створюється унікальний відбиток, що додатково може бути прив'язаний до соціальних мереж, веб-сайтів чи додатків. Отже, виникає питання про захист ідентифікуючої інформації у випадків коли інформація, отримана за допомогою файлів cookies, фішінгових листів створених у тому числі за допомогою Штучного інтелекту, IP-адреси тощо. Так, наприклад, кожен пристрій має IP-адресу, за якою можна дізнатися ваше місцезнаходження. IP-логінг працює через електронні листи, в які логгер закладає невидимий код. Якщо відкрити цей лист, IP-адреса надсилається доксеру. У разі зламу засобів захисту мережі WI-FI стає можливим перехопити файли, що пересилаються по мережі (Сниффинг). Отримання інформації за допомогою getcontact: облікові записи, ваші ім'я, прізвище, вік тощо. Також, багато ідентифікуючої інформації знаходиться у відкритому доступі на сторінках у соцмережах. Використовуючи цю інформацію, зловмисники можуть скористатися нею з метою вимагання грошей, погроз, шантажу, дискредитації або навіть піддавати фізичній небезпеці жертв доксингу.

Нажаль, дана проблема на науково-правовому рівні в Україні не висвітлювалась. Значні прогалини містяться й теорії і на практиці у відмежуванні кримінального правопорушення, передбаченого ст. 182 КК України від суміжних кримінальних правопорушень щодо захисту інформації у кіберпросторі та дотичних адміністративних правопорушень. Ця проблема має на наш погляд з поширенням різноманітності ідентифікуючої інформації. Поняття «персональних даних» висвітлено у Регламенті Європейського Парламенту і Ради (ЄС) 2016/679 від 27 квітня 2016 року «Про захист фізичних осіб у зв'язку з опрацюванням персональних даних і про вільний рух таких даних (General Data Protection Regulation, GDPR)» [7], визначає, що «особу можна ідентифікувати прямо чи опосередковано, зокрема вказавши такі ідентифікатори, як ім'я, ідентифікаційний номер, дані щодо місцезнаходження, онлайн ідентифікатор чи інші особливості фізичної, фізіологічної, генетичної, духовної, економічної, культурної чи соціальної ідентичності такої фізичної особи». Разом з тим, GDPR вимагає цільового обмеження, мінімізації даних, обмеженого зберігання та забезпечення конфіденційності, однак коли мова йде про повноцінні системи GPS- навігації, то визначити обсяг мінімально необхідної інформації важко у контексті запису впровадження штучного інтелекту і збереження ідентифікуючої інформації. Наприклад, автомобіль несе підвищену небезпеку для оточення, відповідно необхідно додаткове стеження за ефективністю роботи алгоритмів та корегування процесу навчання штучного інтелекту через аналіз логів та записів оточення за різних обставин та непередбачуваних подій. Окрім технічної інформації такі записи побічно будуть містити особисті дані власника (типові маршрути, місця паркування) та третіх осіб (пішоходів, інших учасників дорожнього руху). У такому контексті дотримання актів, як GDPR значно сповільнить, або навіть унеможливить імплементацію повністю автономних транспортних засобів. Вирішити таку проблему можна шляхом створення спеціалізованих регламентів для штучного інтелекту який впроваджений у даних GPS- навігаторів.

Окремо потребує уваги інформація «розпізнання». Технологія розпізнавання обличчя є частиною нашого життя. Через майже нульову вірогідність існування двох осіб з повністю однаковими біометричними даними, цей спосіб є найкращім для ідентифікації особи. Потужність алгоритмів розпізнавання обличчя дозволяє ідентифікувати глядачів кінотеатрів чи відвідувачів супермаркетів, присвоювати їм унікальні номери та надалі підв'язувати через різні механізми бонусних карток. Дещо подібне, але у світовому масштабі здійснила компанія Clearview AI. Європейські та Британські контролюючі органи виявили значні порушення GDPR та GB GDPR продуктом Clearview AI. Компанія використовувала зображення з пошукових систем, сайтів новин та соціальних мереж і створювала профайли на основі біометрії обличчя. Пропустивши зображення людини через алгоритм будь-хто мав можливість отримати інші зображення особи та ресурси де вони опубліковані, а завдяки соціальним мережам легкістю її ідентифікувати. Суть у тому, що користувачі соціальних мереж не давали згоди на подібну обробку та використання їх ідентифікуючих даних. Окрім того, їм не було відомо та не могло бути відомо про подібні дії Clearview AI. В результаті на компанію було накладено штраф у розмірі 7,5 млн. фунтів [8]. За логікою компанії всі оброблені дані були у відкритому доступі та не вимагали жодних додаткових дій чи маніпуля-

цій з надання дозволу на їх використання. Разом з тим, компанія не мала платформи або партнерів, які могли б забезпечити належне для їх цілей джерело біометричних даних. Це призвело до таких порушень: непрозоре використання персональної інформації; відсутність законних підстав для збору інформації; відсутність підстав для необмеженого зберігання інформації.

Штучний інтелект для спілкування – це алгоритм, що націлений імітувати людське мислення в процесі спілкування. Йдеться про формування, абстрактного мислення, розпізнавання емоційного окрасу, впровадження гумору, розвиток ланцюгів аргументації та інших аспектів спілкування. Такі алгоритми з елементами AI, як Siri, Google, Alexa та Cortana імплементовані в операційні систем, та наділені певним рівнем доступу до процесів, файлів та налаштувань системи. В першу чергу, вони створені, як додатковий інтерфейс, а вже потім для спілкування на вільні теми. При тому асистенти несуть значно більшу загрозу безпеці особистої інформації ніж інші подібні системи. У більшості випадків обробка даних відбувається у хмарі, а пристрій постійно прослуховує оточення в очікуванні запиту. Теоретично, дані отримані в ході спілкування з алгоритмом або у фоновому режимі досить легко використати не за прямим призначенням, чи для формування профайлів користувачів. Поточне прослухування алгоритмом дозволяє визначити актуальні для покупця теми та товари, що можливо використати в маркетингу та рекламі.

Доксинг і порушення недоторканності приватного життя мають багато спільного, але їх розділяють як окремі делікти через кілька відмінностей у контексті, методах і мети вчинення правопорушення. Загалом статтею 182 Кримінального кодексу України передбачається відповідальність за порушення недоторканності приватного життя, дана форма кримінального проступку передбачає збір, зберігання або розголошення конфіденційної інформації без згоди людини. Основною метою є вторгнення в особисте життя і отримання приватної інформації, незалежно від того, чи буде вона публічно розкрита. Це може бути незаконне спостереження, злом облікових записів або отримання інформації через несанкціоновані джерела. Але, доксинг більш ширше поняття, він може приймати різні форми залежно від злочинця та жертви. Іноді це трапляється в публікації в соціальних мережах, яка викриває анонімного коментатора, або в незручному відкритті в групі чату [9]. В інших випадках атаки є серйознішими та небезпечнішими, включаючи крадіжку особистих даних, беззгодний обмін інтимними зображеннями або потенційно небезпечну практику, відому як «SWATting» (де доксери повідомляють про фіктивні злочини). Особливість Доксингу у публічному розголошенні ідентифікуючої інформації, з наміром завдати шкоди, переслідувати або залякувати людину. Зловмисники прагнуть зробити інформацію доступною широкій аудиторії, часто з наміром організувати цькування, переслідування, що підвищує ризик реальної загрози для жертви. Особливо це небезпечно по відношенню до неповнолітніх. Які будь яку інформацію про себе у публічному просторі сприймають болісно.

Здебільшого з метою доксингу використовується інформація, яка вже є у відкритому доступі або може бути зібрана з різних відкритих джерел (соціальні мережі, публічні реєстри, форуми). Хоча доксинг не завжди передбачає незаконний збір інформації, він підсилює небезпеку через публічне розповсюдження.

У доксингу об’єкт нападу є не лише приватність, але й безпека жертви. Публікація особистих даних може призвести до прямих загроз фізичної або психологічної шкоди, що робить доксинг небезпечнішим у деяких випадках. Особливістю є негативні наслідки, у результаті доксингу має колективний вплив, оскільки доксинг часто використовується для організації онлайн-атаки проти людини з боку багатьох людей (тролінг, кібербулінг). Це може призвести до значних соціальних та психологічних наслідків, і жертва може бути піддана масовому переслідуванню.

Отже, доксинг виділяють в окремий делікт, оскільки він має свої унікальні риси – публічне розголошення інформації з метою заподіяння шкоди, викликання загрози та переслідування жертви. При чому незалежно, поширена була приватна чи публічна інформація про людину без її згоди. Кожна особа має не лише право на приватність, а й право на забуття. Право на забуття (право бути забутим, англ. «right to be forgotten») – право особи, на видалення даних про неї із загального доступу через пошукові системи, тобто посилань на ті дані, які, на її думку, можуть завдати їй шкоди. Хоча він часто включає елементи порушення приватності, сам факт масового поширення даних і мета створити небезпеку роблять доксинг особливо небезпечним і тому виділяють його як окремий вид злочину.

У США доксинг може потрапляти під дію різних законів, включаючи закони про кіберпереслідування, переслідування та погрози. Наприклад, у деяких штатах, таких як Каліфорнія та Нью-

Йорк, є закони, які безпосередньо стосуються публікації особистої інформації з метою переслідування або залякування.

У Великій Британії доксинг може бути розглянутий у рамках «Закону про захист даних» (Data Protection Act). Кожен, хто відповідає за використання персональних даних, повинен дотримуватися суворих правил, які називаються «принципами захисту даних». Вони повинні переконатися, що інформація: використовується справедливо, законно та прозоро; використовується для певних, явних цілей; використовується таким чином, що є адекватним, актуальним і обмеженим лише тим, що необхідно; дані повинні оновлюються зберігається не довше, ніж це необхідно (право на забуття) обробляються у спосіб, який забезпечує належну безпеку, включаючи захист від незаконної або неавторизованої обробки, доступу, втрати, знищення або пошкодження [10]. Особисті дані не можуть бути розповсюджені без згоди, якщо це може нанести шкоду людині. Закон про шкідливі комунікації (Malicious Communications Act) також може бути застосований до тих, хто використовує особисті дані для переслідування або залякування. Закон забороняє надсилання листів чи інших статей з метою спричинити страждання чи занепокоєння одержувача. Закон поширюється як на електронні, так і на письмові повідомлення та використовувався для судового переслідування та засудження користувачів соціальних мереж [11].

У Німеччині порушення конфіденційності регулюється кримінальним кодексом, а також Загальним регламентом ЄС із захисту даних (GDPR). Публікація особистих даних без згоди може спричинити серйозні штрафи або кримінальні покарання. Крім того, доксинг може вважатися кіберпереслідуванням (Cyberstalking), що карається законом.

Французьке законодавство також передбачає покарання за несанкціоноване розповсюдження персональних даних. Відповідно до Кримінального кодексу Франції, незаконне розголошення приватної інформації може призвести до штрафу або тюремного ув'язнення.

В Австралії законодавства щодо захисту ідентифікуючої інформації знаходиться у стані розробку та удосконалення. Разом з тим, у 2022 році Федеральний суд Австралії зобов'язав місцевий підрозділ Google Alphabet Inc виплатити штраф у розмірі 60 млн. австралійських доларів (42,7 млн. доларів США) за введення користувачів в оману при збиранні їх особистих даних про місцезнаходження [12]. Публікація особистої інформації для того, щоб завдати шкоди людині, може призвести до кримінальної відповідальності. З цього приводу Австралія хоче зобов'язати соцмережі розкривати дані анонімів та інтернет-тролів [13].

28 липня 2023 року були прийняті поправки до Кримінального кодексу Нідерландів (Wetboek van Strafrecht, WvSr) і Кримінально-процесуального кодексу (Wetboek van Stravordering, WvSv), які передбачають кримінальну відповідальність за «доксинг». У 2023 році 2,3 мільйона голландців стали жертвами тієї чи іншої форми онлайн-злочинності, включаючи кіберзлочинність. Оскільки життя стає все більш цифровим, онлайн-злочинність не зникне, а лише буде удосконалювати власний інструментарій вчинення злочинів. Вплив на жертв величезний й небезпечний. Відповідно, до запиту суспільства розвивається й законодавство. Ця правова новела стосується використання персональних даних (ідентифікуючої інформації) з метою залякування, переслідування і навіть вчинення як морального так і фізичного тиску (доксингу), а саме отримання, розповсюдження або іншим чином надання доступу до персональних даних іншої особи або третьої сторони з наміром викликати страх у цієї іншої особи, завдати серйозних незручностей йому або значно перешкодити жертві у виконанні його посадових функцій. У Нідерландському законодавстві «Доксинг» означає оприлюднення ідентифікаційної інформації про особу, такої як адреса чи номер телефону, з метою залякування, спричинення «серйозних порушень» або серйозних перешкод цій особі у виконанні її обов'язків чи професії. (WvSr, стаття 285d, абзац 1 (новий)). Поправки набули чинності 1 січня 2024 року. Згідно з поправками, доксинг каратиметься позбавленням волі на строк до двох років або штрафом четвертої категорії, тобто штрафом до 22 500 євро (WvSr ст. 23, п. 4; ст. 285d, п. 1 (нова)). Якщо доксинг вчиняється проти конкретних перелічених осіб, таких як політики, юристи, журналісти чи офіцери поліції, максимальний термін ув'язнення буде збільшено на одну третину. (Стаття 285d, параграфу 2): «Параграф 2 статті 285d Кримінального кодексу передбачає посилення покарання, якщо злочин вчинено проти особи, яка виконує функції міністра, державного секретаря, королівського уповноваженого, виконавчого органу провінції, мера, члена генерального представника органу, судовий службовець, адвокат, журналіст чи публіцист у контексті збору новин, поліцейський чи спеціальний слідчий. Прокуратура також застосовуватиме принципи винесення покарання, зазначені в пункті 2, якщо залучені інші посадові особи» [14].

Висновки. Отже, можна констатувати, що практика виділення такого делікту у світі існує, але знаходиться лише на стадії формування. Разом з тим, технічні характеристики сучасного програмного забезпечення свідчать про значне випередження інженерії порівняно з правом. Сьогодні будь хто може за допомогою інтелектуальних програм, які об'єднують штучний інтелект, управління бізнес-процесами та роботизовану автоматизацію процесів для оптимізації прийняття рішень застосувати задля власних цілей та отримання певних переваг. Разом з тим, у гонитві за прибутком нівелюються право особи на приватність, право на забуття тощо. Так, наприклад, у Європі понад 80% ретейлерів очікують, що їхні компанії використовуватимуть інтелектуальну автоматизацію до 2025 року, а 40% повідомили, що їхні організації вже використовують ту чи іншу форму автоматизації інформації. Таке розповсюдження збору інформації містить у собі ризики її неналежного використання й можливість використання ідентифікуючої інформації у злочинних цілях.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. Довідковий центр Google: URL: https://support.google.com/ analytics/answer/7686480?hl=uk.
2. 10 найпотужніших кібератак та витоків даних за всю історію (2024).URL: https://gigatrans.ua/ua/news/10-naypotuzhn-shih-k-beratak-ta-vitok-v-danih-za-vsyu-stor-yu.
3. Крилова Ю.І. Захист персональних даних: вітчизняний та зарубіжний досвід. Інформація і право. № 3(22)/2017. URL: http://il.ippi.org.ua/ article/view/273050.
4. Колованова Є.П., Малахов С.В., Чорна Т.Е. (2023) Передумови та основні складові з протидії доксингу персональних даних. *Technical sciences trends of young scientists regarding the development of science*. URL: https://isg-konf.com/wp-content/uploads/ 2023/07/TRENDS-OF-YOUNG-SCIENTISTS-REGARDING-THE-DEVELOPMENT-OF-SCIENCE.pdf.
5. Luiza Jarovsky (2023) ChatGPT And Large Language Models Are A Privacy Ticking Bomb. URL: https://www.linkedin.com/pulse/chatgpt-large-language-models-privacy-ticking-bomb-luiza-jarovsky.
6. Почапська О.І. (Не)безпека в цифровому світі. Навчальний посібник. Київ: Академія української преси, Центр вільної преси, 2024. 59 с.
7. Personal Data. General Data Protection Regulation 2016/679. 27.04.2016. URL: https://gdpr-info.eu.
8. Персональні дані у контексті обробки штучним інтелектом. URL: https://legalitgroup.com/personalni-dani-u-konteksti-obrobki-shtuchnim-intelektom.
9. Doxxing Statistics in 2024: 11 Million Americans Have Been Victimized. URL: https://www.safehome.org/family-safety/doxxing-online-harassment-research.
10. The Data Protection Act (2018). URL:https://www.gov.uk/data-protection.
11. Malicious Communications Act 1988 definition. URL: https://www.lexisnexis.co.uk/legal/glossary/malicious-communications-act-1988.
12. Australian court orders Google to pay $43 million for misleading users (2022). URL: https://www.reuters.com/technology/google-pay-427-mln-penalties-misleading-users-australian-watchdog-2022-08-12.
13. Australian government's 'anti-troll' legislation would allow social media users to sue bullies (2021). URL: https://www.theguardian.com/australia-news/2021/nov/28/coalition-bill-would-force-social-media-companies-to-reveal-identities-of-online-bullies.
14. Richtlijn voor strafvordering doxing (2023R008). URL: https://www.om.nl/ onderwerpen/beleidsregels/richtlijnen-voor-strafvordering-resultaten/richtlijn-voor-strafvordering-doxing-2023r008.