УДК 341.231.145
DOI: 10.31359/1993-0909-2023-30-3-156

Олег Сергійович Гиляка

Національна академія правових наук України
Харків, Україна
Кафедра прав людини та юридичної методології
Національний юридичний університет імені Ярослава Мудрого
Харків, Україна

Анастасія Муслімівна Мерник

Науково-дослідний інститут
державного будівництва та місцевого самоврядування
Національна академія правових наук України
Харків, Україна

Кафедра теорії права
Національний юридичний університет імені Ярослава Мудрого
Харків, Україна

ДЕЯКІ ПИТАННЯ РЕАЛІЗАЦІЇ ПРАВА НА ПРИВАТНІСТЬ ТА КОНФІДЕНЦІЙНІСТЬ В УМОВАХ СУЧАСНИХ ЦИФРОВИХ ТЕХНОЛОГІЙ

Анотація. *У статті наголошується на тому, що відстеження особистих даних громадян урядами країн та компаніями в усьому світі, збільшення кількості особистих даних в Інтернеті та поява нових форм стеження за людьми, заснованих на штучному інтелекті спричинили актуальність питання захисту права на приватність та конфіденційність у сучасних умовах. Зазначені три передумови умовно можна назвати технологічними викликами праву на приватність. Проте слід звернути увагу й на теоретичні та концептуальні ускладнення у вивченні проблематики конфіденційності та відсутність емпіричного обґрунтування впливу та шкоди порушення права на приватність. Усе це створює загрози праву людини на приватність та конфіденційність, як в Інтернеті, так і в реальному житті. У рамках статті ставиться ціль вивчити питання особливостей реалізації та забезпечення права на приватність і конфіденційність у сучасних умовах, захисту персональних даних у цифровому суспільстві, права бути забутим. Для досягнення поставленої мети у роботі використовується система методів наукового пізнання, зокрема загальнонаукові (аналізу, синтезу), приватні (порівняльний, кількісного й якісного аналізу, апроксимації), а також спеціально-юридичні (формально-юридичний, порівняльно-правовий). Наголошується на тому, що в сучасному світі завдяки розповсюдженням публічної інформації щодо фактів корупції, намагання задовольнити особистий інтерес за рахунок публічного дозволяє уникнути правопорушень та злочинів, зловживання правом з боку впливових осіб. Тому мова має йти про дотримання певної межі між публічним та приватним життям людини, використання новітніх технологій не має «переступати» за межі загальноприйнятої пристойності та брати участь у розповсюдженні не-*

правди. По суті «право на приватність» у сучасних умовах є «правом бути залишеним у спокої» від використання новітніх технологій. За результатом дослідження зроблено висновок, що у світі зростає визнання необхідності спільних зобов'язань щодо гарантування права на приватність та конфіденційність. Зіткнувшись із загальною проблемою, пов'язаною з конфіденційністю та захистом даних в Інтернеті та пов'язаних із ним цифровими технологіями, експерти та регулятори визнають необхідність радикального перегляду регулювання публічного поводження з конфіденційною інформацією. Нові інноваційні виклики праву на приватність мають призводити не до зневіри у можливості існування цього права, а до сприяння більш широкому захисту конфіденційності як в Інтернеті, так і поза ним.

Ключові слова: *право на приватність, право бути забутим, конфіденційність, цифрові технології.*

Oleh S. Hyliaka
National Academy of Legal Sciences of Ukraine
Kharkiv, Ukraine
Department of Human Rights and Legal Methodology
Yaroslav Mudryi National Law University
Kharkiv, Ukraine

Anastasiia M. Mernyk
Scientific Research Institute of State Building and Local Government
of the National Academy of Legal Sciences of Ukraine
Kharkiv, Ukraine
Department of Theory of Law
Yaroslav Mudryi National Law University,
Kharkiv, Ukraine

SOME ISSUES OF IMPLEMENTATION OF THE RIGHT TO PRIVACY AND CONFIDENTIALITY IN THE CONDITIONS OF MODERN DIGITAL TECHNOLOGIES

Abstract. *The article emphasizes that the tracking of personal data of citizens by governments and companies around the world, the increase in the amount of personal data on the Internet and the emergence of new forms of tracking people based on artificial intelligence have caused the issue of protecting the right to privacy and confidentiality to be relevant in today's conditions. The mentioned three prerequisites can be conditionally called technological challenges of the right to privacy. However, attention should also be paid to the theoretical and conceptual complications in the study of privacy issues and the lack of empirical substantiation of the impact and harm of the violation of the right to privacy. All this creates threats to the human right to privacy and confidentiality, both online and in real life. Within the framework of the article, the goal is to study the issues: peculiarities of the implementation and provision of the right to privacy and confidentiality in modern conditions, the protection of personal data in the*

digital society, the right to be forgotten. To achieve the goal, the work uses a system of methods of scientific knowledge, in particular general scientific (analysis, synthesis), private (comparative, quantitative and qualitative analysis, approximation), as well as special-legal (formal-legal, comparative-legal). It is emphasized that in today's world, due to the dissemination of public information about the facts of corruption, efforts to satisfy personal interest at the expense of the public allows to avoid offenses and crimes, abuse of rights by influential persons. Therefore, it should be about observing a certain boundary between a person's public and private life, the use of the latest technologies should not «cross» the boundaries of generally accepted decency and participate in the spread of lies. In essence, the «right to privacy» in modern conditions is the «right to be left alone» from the use of the latest technologies. Based on the results of the study, it was concluded that the world is increasingly recognizing the need for joint obligations to guarantee the right to privacy and confidentiality. Faced with the overall challenge of privacy and data protection on the Internet and related digital technologies, experts and regulators recognize the need for a radical overhaul of the regulation of public handling of sensitive information. New innovative challenges to the right to privacy should not lead to despair in the possibility of the existence of this right, but to the promotion of broader protection of privacy both on and off the Internet.

Key words: *right to privacy, right to be forgotten, confidentiality, digital technologies.*

ВСТУП

Народження сучасного уявлення про конфіденційність та права на приватність можна пов'язати зі статтею Уоррена та Брандейса «Право на конфіденційність», що вийшла ще у 1890 року [1, с. 193]. Проте вже через відносно невеликий проміжок часу почали з'являтися публікації, в яких обґрунтовувалася думка щодо неможливості забезпечення людині права на приватність. Цю тезу можна продемонструвати через вирази генерального директора Sun Microsystems Скотта Макнілі: «у нас нульова конфіденційність… це треба подолати» [2, с. 693] та генерального директору Facebook Марка Цукерберга, який у власній цитаті про приватність у 2010 році зазначив, що «приватність більше не є соціальною нормою» [3, с. 222].

Які причини такого фаталізму щодо права на приватність та конфіденційність? Серед передумов можемо визначити: 1) уряди та компанії в усьому світі займаються відстеженням і профілюванням в Інтернеті; 2) кількість особистих даних осіб в Інтернеті щохвилини зростає і вже вимірюється в ексабайтах; 3) з'являються нові форми складного виявлення та стеження за людьми, засновані на штучному інтелекті, машинному навчанні та аналітиці великих даних. Зазначені три передумови умовно можна назвати технологічними викликами праву на приватність. Проте слід звернути увагу й на теоретичні та концептуальні ускладнення у вивченні проблематики конфіденційності та відсутність емпіричного обґрунтування впливу та шкоди порушення права на приватність. Усе це створює загрози праву людини на приватність та конфіденційність, як в Інтернеті, так і реальному житті.

Безумовно, найважливішим фактором, який впливає на реалізацію та забезпечення права на приватність у сучасних умовах є новітні технології. Ще напри-

кінці дев'ятнадцятого століття один із коментаторів газет, зазначав, що телеграф і незліченні газети зробили світ одним величезним вухом Діонісія – вічною галереєю шепоту [4, с. 57]. Серед цих технологічних інновацій були технології масового друку – ротаційний прес, лінотип і автоматичне згортання, що зробило газети довшими та донесло їх до більшої кількості людей. Крім того, бездротовий телеграф і нові технології камери/плівки, які дозволили нові форми стеження, спостереження та масового обміну інформацією, викликали нові проблеми конфіденційності. На цьому етапі постає дихотомія між правом на приватність та правом на свободу слова, правом на інформації. В сучасному світі завдяки розповсюдженням публічної інформації щодо фактів корупції, намагання задовольнити особистий інтерес за рахунок публічного дозволяє уникнути правопорушень та злочинів, зловживання правом з боку впливових осіб. Тому, скоріше мова має йти про дотримання певної межі між публічним та приватним життям людини, використання новітніх технологій не має «переступати» за межі загальноприйнятої пристойності та брати участь у розповсюдженні неправди. По суті «право на приватність» у сучасних умовах є «правом бути залишеним у спокої» від використання новітніх технологій.

Додатковою динамікою цього технологічного фактору стає злиття державної влади, їх ресурсів з можливостями новітніх технологій, створенням інформаційних систем даних (наприклад, єдиний державний реєстр права власності на нерухоме майно тощо). Сучасними урядами використовуються «інвазивні» форми збору і зберігання даних та інформації, які можуть передбачати перетин межі між приватним та публічним життям людини.

Безсумнівно, важливим кроком для захисту персональних даних – важливої проблеми для сучасних країн, стало затвердження у 2016 році Загального регламенту захисту даних (GDPR) [5], що сприяє розгляду захисту персональних даних людини на абсолютно новому рівні. На додаток до нового набору правових вимог, які вимагають як організаційних, так і технологічних заходів, GDPR став застосовуватися майже до кожної глобальної організації, яка збирає або обробляє дані про осіб.

1. ОГЛЯД ЛІТЕРАТУРИ

Окремі аспекти права на приватність та конфіденційність у сучасних умовах стали предметом наукового розгляду О. Гиляки [6, с. 16], Ф. Паскуале [7, с. 63], М. Гал [8, с. 4], Ю. Размєтаєвої [9, с. 58], С. Шаумбург-Мюллер [11, с. 1146], Дж. Доннеллі [12, с. 282] та ін.

С. Шаумбург-Мюллер у ствоїй статті наголошує на розгалуженій системі законодавства щодо прав та відповідальності людини, але не з'ясованості питання відповідальності у зв'язку з порушенням прав людини в Інтернеті [10, с. 104]. Слід зазначити, що така проблематика, як розуміння соціальних медіа, також залишається не вирішеною. Вони схожі на традиційні медіа, це провайдери інтернет-по-

слуг чи щось інше? Говорячи про відповідальність за порушення прав людини потрібно розуміти, що тут задіяні антагоністичні інтереси різних соціальних груп: починаючи від великих компаній, які хотіли б зберегти свою бізнес-модель значною мірою звільненою від зобов'язань по захисту прав людини; інтернет-активістів, які відстоюють свободу слову, але при цьому не завжди готові нести відповідальність за свої мовні дії; до інтернет-тролів, які мають свій особистий інтерес у штучному створенні проблем. Законодавство щодо відповідальності за порушення прав людини в Інтернеті суттєво різниться та створює основу для існування різних та частково неспівмірних режимів відповідальності, починаючи від відмінностей між внутрішнім законодавством різних країн і продовжуючи колізіями з міжнародним публічним правом та умовами транснаціонального права, що пропонуються великими онлайн-компаніями, які в основному прагнуть обійти внутрішнє законодавство країн та не нести жодної відповідальності за правопорушення в Інтернеті.

С. Восугі та Д. Рой наголошують, що анонімність в Інтернеті є важливою цінністю, але вона має бути збалансована з іншими правами та інтересами та не нести в собі небезпеку для прав людини сторонніх осіб [11, с. 1146]. Це стосується великої кількості шахраїв в Інтернеті. Хоча анонімність спроможна сприяти вільному потоку ідей та інформації в Інтернеті, вона також здатна сприяти вільному потоку навмисної дезінформації та організованих нападів на людей, ідей і навіть установ. Онлайн-дезінформація поширюється набагато швидше, ніж онлайн-інформація.

Дж. Доннелі звертає увагу, що всім державам доводиться мати справу зі складними питаннями відповідальності за порушення прав людини в Інтернеті, і не існує єдиного правильного способу це зробити. Дійсно, у кожної держави формуються індивідульні правові норми, що регулюють порядок захисту прав людини в Інтеренеті, проте всі вони мають відповідати загальним страндартам прав людини.

Життя в Інтернеті є життям спільноти, тому існує необхідність «жити разом», і повинна бути можливість ідентифікувати учасників, особливо, якщо вони залучені до нападів на інших осіб або беруть участь у більш анти-соціальній діяльність, таких як мова ненависті, підрив демократичних процесів тощо.

Тому за загальним принципом, інтернет-ЗМІ повинні бути вільними у вирішенні редакційного розсуду щодо публікації статей, коментарів і листів, поданих приватними особами. Проте можуть бути виняткові обставини, за яких вони законно зобов'язані опублікувати спростування, вибачення або рішення судів у справах про наклеп.

2. МАТЕРІАЛИ ТА МЕТОДИ

Для здійснення дослідження було застосовано систему методів наукового пізнання, зокрема загальнонаукові (аналізу, синтезу), приватні методи наукового пізнан-

ня, що застосовуються у галузях багатьох наук (порівняльний, кількісного й якісного аналізу, апроксимації), а також спеціально-юридичні (формально-юридичний, порівняльно-правовий). Загальнофілософський (універсальний) метод пізнання використано на всіх етапах пізнавального процесу.

За допомогою методу аналізу розкриті характерні ознаки та вивчені окремі особливості прав людини в умовах використання сучасних цифрових технологій. Порівняльний аналіз надав можливість виявити різні підходи до поняття «конфіденційність». Так, конфіденційність можна умовно поділити на три види: фізична або просторова; конфіденційність прийняття рішень; інформаційна.

За домогою методу узагальнення виділено фактори, які дозволяють подолати сучасні виклики праву на приватність. До них можна віднести: нові емпіричні ідеї щодо шкоди від порушень права на приватність; новітня практика судів у справах за позовами про порушення конфіденційності; зближення підходів у різних країнах до розуміння категорії «конфіденційність»; створення нових інноваційних засобів захисту конфіденційності, репутації та захисту даних.

Метод дедукції надав можливість на основі доктринальних поглядів науковців вивести загальний висновок щодо характерних ознак захисту персональних даних особи. Вони полягають у тому, що дані можна зберігати лише стільки часу, скільки це необхідно для мети, для якої вони були зібрані; існує потреба обмежити коло осіб, хто може переглядати та використовувати дані осіб, лише людьми в організації, для яких цей доступ є критичним; коли сталося порушення персональних даних, необхідно встановити ймовірність і серйозність ризику для прав людини.

Індуктивний метод пізнання норм чинного законодавства щодо реалізації права на приватність та конфіденційність в умовах сучасних цифрових технологій надав можливість одержати загальний висновок щодо характерних ознак порушення персональних даних особи. Яке можна загалом визначити як інцидент безпеки, який вплинув на конфіденційність, цілісність та/або доступність персональних даних.

Історичний метод пізнання посприяв розкриттю телеологічних передумов формування норм права щодо захисту права на приватність та конфіденційність в умовах використання сучасних цифрових технологій. Перші публікації, в яких обґрунтовувалась думка щодо неможливості забезпечення людині права на приватність в умовах функціонування сучасних технологій, з'являються ще у 1890 року.

У статті застосовувалися також й спеціально-юридичні методи, зокрема формально-юридичний і системно-структурний, які було використано під час розробки та вивчення термінологічного апарату даної роботи, а саме при з'ясуванні змісту категорій «право бути забутим», а також для розкриття особливостей зазначеної дефініції.

Нормативна база для цього дослідження включає Загальний регламент захисту даних (GDPR) [5], Хартію основних прав Європейського Союзу [13], Дирек-

тиву Європейського Союзу про захист даних [14], Загальну декларацію прав людини [15], Конвенцію про захист прав людини і основоположних свобод [16] та практику Європейського суду з прав людини. Наприклад, відповідальність держави за порушення прав людини в Інтернеті можна проілюструвати на прикладі справи ЄСПЛ «Ганновер проти Німеччини» від 24 червня 2004 року [17], коли Суд наголосив на тому, що держава має створити реальний механізм дотримання справедливого балансу інтересу людини на приватне життя та публічного інтересу громадськості на інформацію, у тому числі за особливих обставин, стосовно приватного життя публічних осіб; рішення Європейського суду з прав людині по справі «K. U. проти Фінляндії» від 2 грудня 2008 року [18]. За матеріалами справи хлопчик, якому було 12 років, нібито розмістив оголошення в Інтернеті та шукав чоловіків для стосунків. Суд визнав порушення статті 8 Конвенції про права і свободи людини і громадянина, оскільки на той час у Фінляндії не було жодного правового засобу, який передбачав можливість ідентифікувати особу (або осіб), які завантажили наклепницьке оголошення.

Окрім цього, в роботі використовуються доктринальні джерела, що розкривають зміст права на приватність та конфіденційність в умовах сучасних цифрових технологій.

3. РЕЗУЛЬТАТИ ТА ОБГОВОРЕННЯ

3.1. Особливості реалізації та забезпечення права на приватність і конфіденційність у сучасних умовах

У 1969 році Джеррі Розенберг у книзі «Смерть конфіденційності» стверджував, що з розвитком технологій централізоване накопичення даних стає легшим, винагорода за вторгнення збільшується, а контроль переходить до маленької кількості людей [19, с. 13]. Тому відомий канадський медіа-філософ Маршалл Маклюен заявив у 1981 році, що «електронний банкінг» стане «смертю конфіденційності» [20, с. 14].

Уявлення про конфіденційність та виклики їй у майбутньому базуються й на висвітленні Едварда Джозефа Сноудена інформації про масове онлайн-спостереження за телекомунікаціями, яке здійснюють уряди, а також звинувачень компаній Facebook та Cambridge Analytica у тому, що завдяки даних, отриманих від компанії Facebook, Cambridge Analytica втручалася у вибори по всьому світу, використовуючі в соцмережах персональні дані потенційних виборців і маніпулюючи їх думкою за допомогою інформаційних технологій.

Оскільки з кожною новою технологією та практикою використання даних конфіденційність переосмислюється, розширюється та вдосконалюється, то й визначення права на приватність завдання не з простих. Ще в 1890 році в американській традиції конфіденційності визначили право на приватність як право на самотність і право на те, щоб інформація та плітки щодо приватних осіб не поширювалися та не оприлюднювалися. Якщо ми визначаємо приватність як певний обсяг

інформації, яку особа має право тримати в повній таємниці, то, звичайно, ця форма конфіденційності є недосяжною через існування новітніх технологічних реалій, які генеруються та зберігають інформацію про нас і нашу діяльність.

Джеррі Канг ділить конфіденційність на три види: фізична або просторова; конфіденційність прийняття рішень; інформаційна [21, с. 284]. Річардс визначає конфіденційність як категорію, яку слід розуміти як сукупність чотирьох елементів: вторгнення в захищені простори, відносини або рішення, збір інформації, використання інформації та розкриття інформації [22]. Тут слід погодитися з Джудітом Томасом, який зазначив, що ми не маємо чіткого уявлення про те, що таке конфіденційність [23, с. 272]. І це є другим викликом праву на приватність, відсутність теоретичного розуміння зазначеної категорії. Ми не можемо захищати право, зміст якого не розуміємо.

Третім викликом праву на приватність та конфіденційність можна вважати проблеми з вимірюванням, доказуванням та обґрунтуванням шкоди та збитків від порушення цього права. На практиці важко визначити таку шкоду, кількісно її визначити, виміряти та задокументувати. І через ці проблеми та унікальну природу шкоди конфіденційності суди та вчені-юристи виявляють скептицизм щодо права на приватність. Це призводить до того, що суди неохоче визнають судові позови, засновані на завданні шкоди праву на приватність. Часто відхиляють такі позови як «суб'єктивні», «спекулятивні» або «гіпотетичні».

Однак не слід бачити в цьому питанні лише проблематику, існують фактори, які дозволяють подолати сучасні виклики праву на приватність. Серед них: нові емпіричні ідеї щодо наслідків і шкоди від порушень прав на приватність; нова відкритість та практика судів як у США, так і Європі до позовів про порушення конфіденційності; зближення американських і європейських традицій конфіденційності, що призводить до нових інноваційних позитивних засобів захисту конфіденційності, репутації та захисту даних, таких як GDPR (Регламент у межах законодавства Європейського Союзу щодо захисту персональних даних усіх осіб у межах Європейського Союзу та Європейської економічної зони) [5].

3.2. Захист персональних даних у цифровому суспільстві

Права на повагу до приватного життя та захист особистих даних тісно пов'язані, оскільки обидва вони захищають подібні цінності. Проте в країнах Європи на додаток до права на конфіденційність поступово сформувалося незалежне фундаментальне право на захист даних. Після його окремого визнання в Хартії основних прав Європейського Союзу [13], право на захист даних зайняло своє місце в Загальному регламенті Європейського Союзу про захист даних (GDPR) [5]. Стаття 1(2) GDPR однозначно підтверджує, що вона захищає основні права, зокрема право на захист даних. Такий підхід відрізняється від норм чинного Директиву Європейського Союзу про захист даних [14], який захищає, зокрема, право на конфіденційність стосовно обробки персональних даних.

Багато компаній, державних установ щодня шукають відповіді на питання щодо захисту персональних даних особи: як довго мають зберігатися данні, хто може отримувати доступ до такої інформації, що робити у випадку порушення персональних даних? Спробуємо знайти відповіді на поставленні запитання.

Що стосується питання про те, як довго дані мають бути дійсними та зберігатися, потрібно визначити сталість даних, щоб установити період дії. Це необхідно, оскільки нова вимога GDPR щодо обмеження зберігання означає, що можна зберігати дані лише стільки часу, скільки це необхідно для мети, для якої вони були зібрані.

У відповідь на питання про те, хто може отримати доступ до даних, існує потреба обмежити коло осіб, хто може переглядати та використовувати дані осіб, лише людьми в організації, для яких цей доступ є критичним. Наприклад, ідентифікатори соціальних мереж можуть мати відношення лише до певних спеціалістів із маркетингу та продажів, тоді як фінансовому відділу не обов'язково мати до них доступ. У цьому процесі також необхідно визначити певні терміни, наприклад, що є контактними даними? Це, наприклад, лише електронна пошта, чи це ім'я, електронна адреса, адреса та номер телефону, чи це якийсь третій варіант?

Порушення персональних даних можна загалом визначити як інцидент безпеки, який вплинув на конфіденційність, цілісність та/або доступність персональних даних. Порушення персональних даних відбуватиметься щоразу, коли будь-які персональні дані буде втрачено, знищено, пошкоджено та/або розкрито; якщо хтось отримує доступ до даних або передає їх без належного дозволу, або якщо дані стають недоступними, наприклад, коли вони були зашифровані програмою-вимагачем, або випадково втрачені чи знищені. Коли відбувається інцидент безпеки, є необхідність швидко встановити, чи сталося порушення персональних даних, і, якщо так, негайно вжити необхідні заходи для можливого відвернення негативної шкоди.

Коли сталося порушення персональних даних, необхідно встановити ймовірність і серйозність ризику для прав людини. Оцінюючи ризик для прав, важливо зосередитися на потенційних негативних наслідках для залучених осіб. Порушення персональних даних, якщо його не усунути належним чином і своєчасно, може призвести до фізичних, матеріальних або нематеріальних збитків для фізичних осіб, таких як втрата контролю над їхніми персональними даними або обмеження їхніх прав, дискримінація, крадіжка особистих даних або шахрайство, фінансові збитки, несанкціоноване скасування псевдонімізації, шкода репутації, втрата конфіденційності персональних даних, захищених професійною таємницею, або будь-які інші значні економічні чи соціальні збитки для відповідної фізичної особи.

Це означає, що такі порушення можуть мати низку несприятливих наслідків для людей, які включають емоційний стрес, а також фізичну та матеріальну шкоду. Деякі порушення персональних даних не призведуть до ризиків, крім можли-

вих незручностей для тих, кому ці дані потрібні для виконання своєї роботи. Інші порушення можуть суттєво вплинути на осіб, чиї особисті дані були скомпрометовані, і це потрібно оцінювати в кожному конкретному випадку, розглядаючи всі відповідні фактори. Якщо порушення може призвести до високого ризику для прав людини, GDPR рекомендує повідомити зацікавлених осіб швидко та безпосередньо, особливо якщо є потреба зменшити безпосередній ризик їхнього збитку. Однією з головних причин для інформування осіб є допомогти їм вжити заходів, щоб захистити себе від наслідків порушення.

У разі порушення персональних даних організація та установа, що володіє персональними даними, повинна без затримки, не пізніше ніж через 72 години після того, як їй стало відомо про інцидент, повідомити про порушення персональних даних у наглядовий орган. Повідомлення повинно містити: характер порушення персональних даних, у тому числі, де це можливо, категорії та приблизну кількість відповідних суб'єктів даних, а також категорії та приблизну кількість відповідних записів персональних даних; ім'я та контактні дані вповноваженого із захисту даних; ймовірні наслідки порушення персональних даних; опис заходів, що зроблені для відвернення шкоди.

З іншого боку, якщо використовувати нові правила неправильно, це цілком може призвести до гальмування розвитку захисту персональних даних. Песимістичний варіант розвитку подій припускає, що суб'єкти даних будуть блокувати процеси щодо надання згоди на обробку інформації, працівники можуть використовувати для цього профспілки, індивідуальні особи – спеціалістів із захисту даних, у публічному просторі реалізацію своїх прав можна здійснювати за допомога неурядових організацій. Уявіть собі, компанія зіткнулася з тисячею запитів на видалення даних у поєднанні з відповідними запитами на перенесення, доступ і виправлення. У цьому випадку компанії доведеться вичерпати свої ресурси, щоб впоратися з цими запитами, побоюючись непропорційних штрафів та іншої відповідальності, нехтуючи при цьому своїм головним завданням – розвитком.

3.3. Право бути забутим

Право бути забутим, як визначено у статті 17 Загального регламенту ЄС про захист даних № 679 від 2016 року, не є новим юридичним правом [24, с. 17]. У Франції право на забуття визнається та забезпечується судами з середини 1960-х років. В Італії захист права бути забутим можна простежити з кінця 1970-х років. У США це право можна віднайти у судовій практиці. Наприклад, у судовій справі «Бріско проти Рідерс Дайджест Асоціації» від 1971 року потрібно було вирішити, чи може «ідентифікація особи в звітах про давно минулі злочини» служити інтересам суспільства чи це суспільна цікавість. Судді дійшли висновку, що особи не повинні задовольняти цікавість публіки за рахунок повторного привернення уваги суспільства таким способом [25, с. 382].

Право бути забутим розглядається в цих випадках як специфікація або складовий елемент права особи на приватне життя. Останнє закріплено як у статті 12 Загальної декларації прав людини 1948 року [15], так і в статті 8 Конвенції про захист прав людини і основоположних свобод 1950 року [16]. Будучи складовим елементом права людини на приватність та поваги до приватного життя, право бути забутим слід вважати відносним, а не абсолютним правом людини. Тому право бути забутим має бути збалансоване з іншими правами, які захищаються правовою системою. Серед цих прав – право на інформацію, свободу слова чи преси. Подібним чином у положеннях Європейської конвенції з прав людини 1950 року закріплено, що право на приватність, отже, і право бути забутим підлягає обмеженням відповідно до закону та якщо це є необхідним у демократичному суспільстві в інтересах національної безпеки, громадської безпеки тощо.

Цифрова революція безумовно вплинула на процес реалізації права бути забутим. З одного боку, використання інформаційно-комунікаційних технологій (ІКТ), таких як Інтернет, соціальні мережі та смартфони, зробило набагато легшим ідентифікацію актора з інформацією про минулі події. З іншого боку, правові питання дедалі більше перетворюються на питання доступу до інформації в цифровому середовищі, контролю та захисту інформації. Відповідно законодавці та політики доповнили систему захисту права людини на приватне життя новим правом – право на захист персональних даних (наприклад, стаття 8 Хартії основних прав ЄС від 2000 року мала на меті доповнити гарантії статті 7 про традиційну повагу до приватного життя, яка існувала в доцифрову епоху). Таким чином, право бути забутим розвивалося в епоху цифрових технологій. Як специфікація права особи на захист її особистих даних, право бути забутим сьогодні слід розуміти як право на видалення персональних даних, що стосуються цієї особи.

Рішення Суду Справедливості Європейського Союзу у справі «Google Spain SL, Google Inc. v Agencia Española de Protección de Datos, Mario Costeja González» [26] стало новим етапом у сфері захисту персональних даних особи.

По-перше, Постанова Суду Справедливості Європейського Союзу встановлює, що оператори пошукових систем (SEO) обробляють і контролюють персональні дані. SEO виступають контролерами даних у значенні статті 2 Директиву 95/46/ЕС та статті 2 Загального регламенту захисту даних (GDPR). Це означає, що обробка персональних даних, тобто індексування результатів пошуку, які здійснює SEO, слід відрізняти від обробки персональних даних, яку здійснюють видавці сторінок вебсайтів, і є додатковою до неї.

По-друге, відповідно до статей 7 і 8 Хартії основних прав ЄС від 2000 року суб'єкт даних має право бути забутим у вузькому сенсі, як право на вилучення зі списку, тобто право вимагати, щоб інформація більше не була доступною для широкого загалу через список результатів, отриманих у результаті пошуку, здійсненого за посиланням на ім'я суб'єкта. Важливо підкреслити, що суб'єкт даних немає необхідності доводити, що включення інформації до списку результатів

пошуку завдало йому шкоди. Крім того, спеціалісти з оптимізації не зобов'язані попереджати та повідомляти редакторів веб-сайтів про видалення певних посилань.

По-третє, Рішення щодо «Google Spain» не встановила права суб'єкта даних на видалення інформації з першоджерела. Видалення конкретного посилання не тягне за собою повного видалення посилання з індексів пошукового оператора або видалення інформації через ланцюжок контролерів, які обробляють інформацію. З одного боку, вихідну інформацію все ще можна отримати, посилаючись на інші пошукові запроси, або шляхом прямого доступу до веб-сторінки, де інформація була спочатку опублікована. З іншого боку, SEO як контролер даних, якому адресовано запит на видалення зі списку, може виконати або відхилити такий запит без обов'язкового залучення первинного видавця інформації до процесу прийняття рішення.

По-четверте, необхідним є встановлення справедливого балансу між фундаментальними правами суб'єкта даних та інтересами широкої громадськості щодо доступу до відповідної інформації. Цей баланс залежить від низки відповідних факторів, таких як характер і конфіденційність даних, що обробляються, своєчасність або актуальність інформації, роль суб'єкта даних у суспільному житті тощо. До інтересів суспільства можна відносити, наприклад, інтереси національної безпеки чи громадської безпеки. Таким чином, при захисті права забутим має враховувати захист прав інших людей на свободу вираження поглядів і доступ до інформації.

Ми все ще можемо задаватися питанням про природу «права бути забутим». Зрештою, позивачі у справі «Google Spain» не просили, щоб про них забули. Право на виключення зі списку не слід плутати з правом на видалення, тобто видаляти інформацію з Інтернету чи загальнодоступного архіву. Як нещодавно зазначив Королівський суд Великої Британії у справі «NT1 & NT2 проти Google LLC», задоволення запиту про видалення зі списку щодо певної URL-адреси не завадить Google повертати результати пошуку, що містять цю URL-адресу за іншими критеріями запиту; це лише означає, що URL-адреса не повинна повертатися у відповідь на пошук за ім'ям позивача. Таким чином, нове право, встановлене судом, дає позивачам можливість вилучати своє ім'я зі списку результатів пошуку, пов'язаних з однією чи кількома URL-адресами.

ВИСНОВКИ

У світі зростає визнання необхідності спільних зобов'язань щодо гарантування права на приватність та конфіденційність. Зіткнувшись із загальною проблемою, пов'язаною з конфіденційністю та захистом даних в Інтернеті та пов'язаних із ним цифровими технологіями, експерти та регулятори визнають необхідність радикального перегляду регулювання публічного поводження з конфіденційною інформацією. В Європі це набуло форми формулювання та введення в дію нового

Загального регламенту захисту даних, розробленого, щоб відповідати викликам цифрової ери. У США Федеральна торгова комісія зобов'язалася виконувати захист приватних даних, що раніше було не характерним для американської традиції конфіденційності. Нові інноваційні виклики праву на приватність мають призводити не до зневіри у можливості існування цього права, а до сприяння більш широкому захисту конфіденційності як в Інтернеті, так і поза ним.

Є надія, що новий режим правового регулювання, передбачений Загальним регламентом захисту даних (GDPR) стане прикладом для правового регулювання захисту персональних даних не лише в європейському просторі, позитивно вплине на зміну культури захисту персональних даних; компанії матимуть обізнаність щодо правил обробки даних, а суб'єкти даних будуть більш обережними щодо того, якою інформацією вони діляться, для яких цілей і в контексті якої правової основи; обробники даних більше не будуть перебувати в стані квазіімунітету і відповідатимуть за будь-який витік даних, який відбувається в межах їх відповідальності. Дотримання зазначених положень буде сприяти реальному захисту персональних даних.

Розглядаючи сучасний стан права бути забутим і способи, якими інформаційна революція вплинула на його доцифрову версію, слід зробити висновок, що зміст права бути забутим сьогодні включає й право вилучення ім'я людини зі списку результатів пошуку, пов'язаних з однією чи кількома URL-адресами. В будь-якому випадку, право бути забутим і його складовий елемент, що виник у цифрову еру – право на видалення, слід відносити до сучасних прав людини, яке має гарантуватися та забезпечуватися реальними правовими та технічними механізмами.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

[1] Warren Samuel D., Brandeis, Louis D. The right to privacy. *Harvard law review*. 1890. Vol 4. P. 193–220.

[2] Penney J. The cycles of global telecommunication censorship and surveillance. *University of Pennsylvania journal of international law*. 2015. Vol. 36. P 693–694.

[3] V. Boehme-Neßler. Privacy: A matter of democracy. Why democracy needs privacy and data protection. *International Data Privacy Law*. 2016. Vol. 6. P. 222.

[4] Kuner C. Transborder data flow regulation and data privacy law. *Oxford University Press*. 2013. P. 57.

[5] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC [2016] OJ L 119/1. URL: https://gdpr-text.com/uk/read/article-25/ (дата звернення: 12.06.2023)

[6] Hyliaka O. Human rights in the digital age: Challenges, threats and prospects. *Науковий юридичний журнал*. 2023. №28 (1). С. 16.

[7] Pasquale F., Cashwell G. Prediction, persuasion, and the jurisprudence of behaviourism. *University of Toronto Law Journal.* 2018. Vol. 68. P. 63.

[8] Elkin-Koren N., Gal M. The chilling effect of governance by data on data markets. *University of Chicago Law Review*. 2018. Vol. 68 (1). P. 4.

[9] Razmetaeva Y. The Right to Be Forgotten in the European Perspective. *Baltic Journal of European Studies*. 2022. Vol 10 (1). P. 58–76.
[10] Schaumburg-Müller S. Liability regimes for online human rights violations. *Human Rights, Digital Society and the Law.* 2019. P. 103–116.
[11] Vosoughi S., Roy and S. Aral D. The Spread of True and False News Online. *Science*. 2018. Vol. 359. P. 1146–1151.
[12] Donnelly J. The relative universality of human rights. *Human rights quarterly*. 2007. Vol. 29. P. 281–306.
[13] The Charter of Fundamental Rights of the European Union. 18.12.2000. URL: https://www.europarl.europa.eu/charter/pdf/text_en.pdf (дата звернення: 12.06.2023)
[14] Директива Європейського Парламенту і Ради № 95/46/ЄС про захист фізичних осіб при обробці персональних даних і про вільне переміщення таких даних від 24.10.1995. URL: https://zakon.rada.gov.ua/laws/show/994_242#Text (дата звернення: 12.06.2023)
[15] Загальна декларація прав людини від 10.12.1948 / Генеральна Асамблея ООН. URL: https://zakon.rada.gov.ua/laws/show/995_015#Text (дата звернення: 12.06.2023)
[16] Конвенція про захист прав людини та основоположних свобод від 04.11.1950. URL: https://zakon.rada.gov.ua/laws/show/995_004#Text (дата звернення: 12.06.2023)
[17] Рішення Європейського суду з прав людині у справі «Ганновер проти Німеччини» від 24.06.2004. URL: https://zakon.rada.gov.ua/laws/show/980_324#Text (дата звернення: 12.06.2023).
[18] Рішення Європейського суду з прав людині у справі «K. U. проти Фінляндії» від 02.12.2008. URL: https://rm.coe.int/168059920d (дата звернення: 12.06.2023).
[19] Rosenberg J. The death of privacy. New York : Random House, 1. 1969. P. 13.
[20] Regan P. Legislative privacy: technology, social values, and public policy. UNC. 1995. P. 16.
[21] Nicholas A., Peters J., Peters B. Why privacy keeps dying: the trouble with talk about the end of privacy. *Information, communication and society.* 2017. Vol. 20. No. 2. P. 284–287.
[22] Richards N. Four myths of privacy. A world without privacy: what the law can and should do. *Cambridge Press*. 2015. P. 38. URL: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2427808 (дата звернення: 12.06.2023)
[23] Thomas J. The right to privacy. Philosophical dimensions of privacy: an anthology. *Cambridge University Press*. 1984. P. 272.
[24] Pagallo U., Durante M. Legal memories and the right to be forgotten. *Protection of information and the right to privacy.* Dordrecht : Springer. 2014. P. 17–30.
[25] Pagallo U. Online security and the protection of civil rights: a legal overview. *Philosophy and technology*. 2013. Vol. 26. No. 4. P. 381–395.
[26] Judgment of the Court of Justice of the European Union**. «**Google Spain SL, Google Inc. v Agencia Española de Protección de Datos, Mario Costeja González**»** (13 May 2014)**.** URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62012CJ0131 (дата звернення: 12.06.2023).

REFERENCES

[1] Warren, Samuel D. & Brandeis, Louis D. (1890). The right to privacy. *Harvard law review*, 4, 193–220.
[2] Penney, J. (2015). The cycles of global telecommunication censorship and surveillance. *University of Pennsylvania journal of international law*, 36, 693–694.

[3] Boehme-Neßler, V. (2016). Privacy: A matter of democracy. Why democracy needs privacy and data protection. *International Data Privacy Law*, 6, 222.
[4] Kuner, C. (2013). Transborder data flow regulation and data privacy law. *Oxford University Press*, 57.
[5] Regulation (EU) 2016/679 of the European Parliament and of the Council on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC [2016] OJ L 119/1. (2016, April). Retrieved from https://gdpr-text.com/uk/read/article-25/
[6] Hyliaka, O. (2013). Human rights in the digital age: Challenges, threats and prospects. *Scientific legal journal*, 28 (1), 16.
[7] Pasquale, F., & Cashwell, G. (2018). Prediction, persuasion, and the jurisprudence of behaviourism. *University of Toronto Law Journal*, 68, 63.
[8] Elkin-Koren, N., Gal, M. (2018). The chilling effect of governance by data on data markets. *University of Chicago Law Review*, 68 (1), 4.
[9] Razmetaeva, Y. (2022). The Right to Be Forgotten in the European Perspective. *Baltic Journal of European Studies*, 10 (1), 58–76.
[10] Schaumburg-Müller, S. (2019). Liability regimes for online human rights violations. *Human Rights, Digital Society and the Law,* 103–116.
[11] Vosoughi, S., & Aral, D. (2018). The Spread of True and False News Online. *Science*, 359, 1146–1151.
[12] Donnelly, J. (2007). The relative universality of human rights. *Human rights quarterly*, 29, 281–306.
[13] The Charter of Fundamental Rights of the European Union. (2000, Desember). Retrieved from https://www.europarl.europa.eu/charter/pdf/text_en.pdf
[14] Directive of the European Parliament and the Council No. 95/46/EU on the protection of natural persons during the processing of personal data and on the free movement of such data (1995, October). Retrieved from https://zakon.rada.gov.ua/laws/show/994_242#Text
[15] Universal Declaration of Human Rights. (1948, Desember). Retrieved from https://zakon.rada.gov.ua/laws/show/995_015#Text
[16] Convention for the Protection of Human Rights and Fundamental Freedoms. (1950, November). Retrieved from https://zakon.rada.gov.ua/laws/show/995_004#Text
[17] Decision of the European Court of Human Rights in the case «Hannover v. Germany». (2004, June). Retrieved from https://zakon.rada.gov.ua/laws/show/980_324#Text
[18] The decision of the European Court of Human Rights in the case «K. U. against Finland» (2008, Desember). Retrieved from https://rm.coe.int/168059920d
[19] Rosenberg, J. (1969). *The death of privacy*. New York: Random House.
[20] Regan, P. (1995). Legislative privacy: technology, social values, and public policy. *UNC*, 16.
[21] Nicholas, A., Peters, J., & Peters, B. (2017). Why privacy keeps dying: the trouble with talk about the end of privacy. *Information, communication and society,* 20 (2), 284–287.
[22] Richards, N. (2015). Four myths of privacy. A world without privacy: what the law can and should do. *Cambridge Press*, 38. Retrieved from https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2427808
[23] Thomas, J. (1984). The right to privacy. Philosophical dimensions of privacy: an anthology. *Cambridge University Press*, 272.
[24] Pagallo, U., Durante, M. (2014). Legal memories and the right to be forgotten. *Protection of information and the right to privacy.* Dordrecht: Springer, 17–30.

[25] Pagallo, U. (2013). Online security and the protection of civil rights: a legal overview. Philosophy and technology, 26 (4), 381–395.
[26] Judgment of the Court of Justice of the European Union. «Google Spain SL, Google Inc. v Agencia Española de Protección de Datos, Mario Costeja González». (2014, May). Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62012CJ0131

Олег Сергійович Гиляка
Кандидат юридичних наук, старший дослідник
Начальник управління стратегічного розвитку
Національна академія правових наук України
61024, вул. Пушкінська, 70, Харків, Україна

Доцент кафедри прав людини та юридичної методології
Національний юридичний університет імені Ярослава Мудрого
61024, вул. Пушкінська, 77, Харків, Україна

Oleh S. Hyliaka
Candidate of Law, Senior Researcher
Head of the Strategic development department
of the National Academy of Legal Sciences of Ukraine
61024, 70 Pushkinska Str., Kharkiv, Ukraine

Associate professor of the Department of Human Rights and Legal Methodology
Yaroslav Mudryi National Law University
61024, 77 Pushkinska Str., Kharkiv, Ukraine

Мерник Анастасія Муслімівна
Кандидат юридичних наук, доцент
Провідний науковий співробітник сектору теоретико-методологічних
проблем організації державної влади
Науково-дослідного інституту державного будівництва та місцевого самоврядування
Національна академія правових наук України
61002, вул. Чернишевська, 80, Харків, Україна

Доцент кафедри теорії права
Національний юридичний університет імені Ярослава Мудрого
61024, вул. Пушкінська, 77, Харків, Україна

Anastasiia M. Mernyk
Candidate of Law, Associate Professor
Leading Researcher of the Sector Theoretical and Methodological

Problems of the Organization of State Power
Scientific Research Institute of State Building and Local Government
National Academy of Legal Sciences of Ukraine
61002, 80 Chernyshevska Str., Kharkiv, Ukraine

Associate Professor of the Department of Theory of Law
Yaroslav Mudryi National Law University
61000, 70 Pushkinska Str., Kharkiv, Ukraine

Рекомендоване цитування: Гиляка О. С., Мерник А. М. Деякі питання реалізації права на приватність та конфіденційність в умовах сучасних цифрових технологій. *Вісник Національної академії правових наук України*. 2023. Том 30. № 3. С.156–172.

Suggested Citation: Hyliaka, O.S., & Mernyk, A.M. (2023). Some issues of implementation of the right to privacy and confidentiality in the conditions of modern digital technologies. *Journal of the National Academy of Legal Sciences of Ukraine*, 30(3), 156–172.

Стаття надійшла / Submitted: 09/08/2023
Доопрацьовано / Revised: 08/09/2023
Схвалено до друку / Accepted: 27/09/2023