УДК 341.231.145
DOI: 10.31359/1993-0909-2023-31-1-40

Олег Сергійович Гиляка
Національна академія правових наук України
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

ПРАВОВЕ РЕГУЛЮВАННЯ ТА ПРАКТИКА ЄВРОПЕЙСЬКОГО СУДУ З ПРАВ ЛЮДИНИ І ЄВРОПЕЙСЬКОГО СУДУ СПРАВЕДЛИВОСТІ ЩОДО ПРАВ ЛЮДИНИ У СФЕРІ ВИКОРИСТАННЯ ЦИФРОВИХ ТЕХНОЛОГІЙ

Анотація. *У статті наголошується на тому, що правове регулювання захисту прав людини у сфері використання цифрових технологій здійснюється розгалуженою системою міжнародних правових документів. Зокрема у статті розглядаються: Рекомендації щодо захисту конфіденційності та транскордонних потоків персональних даних; Керівні принципи щодо використання даних особи; Конвенція про захист осіб щодо автоматизованої обробки персональних даних; Додатковий протокол до Конвенції про захист осіб щодо автоматизованої обробки персональних даних щодо органів нагляду та транскордонних потоків даних; Протокол про внесення змін до Конвенції про захист осіб щодо автоматизованої обробки персональних даних протокол; Директива 95/46/ЕС про захист прав осіб під час обробки персональних даних і їх вільного переміщення; Директива про телекомунікації; Директива про конфіденційність електронної пошти; Директива Європейського парламенту та Ради 97/13/ЕС; Директива 2002/58/ЕС щодо електронної конфіденційності; Директива Європейського Парламенту та Ради 2002/58/ЕС щодо обробки персональних даних і захисту конфіденційності в секторі електронних комунікацій; Директив Європейського парламенту та Ради 2006/24/ЕС про збереження даних, створених або оброблених у зв'язку з наданням загальнодоступних електронних комунікаційних послуг або громадських комунікаційних мереж; Хартія основних прав Європейського союзу; Загальний регламент захисту даних (GDPR); Регламент Європейського Парламенту та Ради 2016/679 про захист фізичних осіб щодо обробки персональних даних і про вільний рух таких даних. У рамках статті ставиться ціль вивчити судову практику Європейського суду з прав людини і Європейського суду справедливості щодо*

реалізації та забезпечення права на приватність і конфіденційність в сучасних умовах, захисту персональних даних у цифровому суспільстві. Зазначено, що сьогодні спостерігається різке зростання кількості прецедентів, пов'язаних із захистом прав людини в Інтернеті у практиці Європейського суду з прав людини (ЄСПЛ), так і Європейського суду справедливості (ЄС). 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). За результатом дослідження зроблено висновок, що головне завдання правого регулювання прав людини в умовах використання цифрових технологій – це захист фундаментальних прав та створення правового порядку. Поряд з системою правових норм захист основних прав передбачає й інші заходи, розроблені як в рамках національних правових систем, так і ті, що передбачені у ЄКПЛ. Кожен із цих механізмів захисту, безсумнівно, переслідує конкретні цілі, і механізми, безперечно, побудовані на основі правових інструментів. Одним із таких механізмів є можливість захисту порушеного права у суді.

Ключові слова: *права людини, цифрові технології, Європейський суд з прав людини, Європейський суд справедливості.*

Oleh S. Hyliaka
National Academy of Legal Sciences of Ukraine
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

LEGAL REGULATION AND PRACTICE EUROPEAN COURT OF HUMAN RIGHTS AND THE EUROPEAN COURT OF JUSTICE CONCERNING HUMAN RIGHTS IN THE SPHERE OF USE OF DIGITAL TECHNOLOGIES

Abstract. *The article emphasizes that the legal regulation of the protection of human rights in the field of the use of digital technologies is carried out by an extensive system of international legal documents. In particular, the article examines: Recommendations for the protection of privacy and cross-border flows of personal data; Guidelines for the use of personal data; Convention on the Protection of Individuals with regard to Automated Processing of Personal Data; Additional Protocol to the Convention on the Protection of Individuals Regarding Automated Processing of Personal Data Regarding Supervisory Authorities and Cross-Border Data*

Flows; Protocol on Amendments to the Convention on the Protection of Individuals Regarding Automated Processing of Personal Data Protocol; Directive 95/46/EC on the protection of the rights of individuals during the processing of personal data and their free movement; Telecommunications Directive; Email Privacy Policy; European Parliament and Council Directive 97/13/EC; Directive 2002/58/EC on electronic privacy; Directive 2002/58/EC of the European Parliament and of the Council on the processing of personal data and the protection of privacy in the electronic communications sector; Directive 2006/24/EC of the European Parliament and of the Council on the retention of data created or processed in connection with the provision of publicly available electronic communications services or public communications networks; Charter of Fundamental Rights of the European Union; General Data Protection Regulation (GDPR); Regulation of the European Parliament and the Council 2016/679 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. The article aims to study the judicial practice of the European Court of Human Rights and the European Court of Justice regarding the implementation and provision of the right to privacy and confidentiality in modern conditions, protection of personal data in the digital society. It is noted that today there is a sharp increase in the number of precedents related to the protection of human rights on the Internet in the practice of the European Court of Human Rights (ECHR) and the European Court of Justice (EC). To achieve the goal, the work uses a system of methods of scientific knowledge, including general scientific (analysis, synthesis), private (comparative, quantitative and qualitative analysis, approximation), as well as special legal (formal-legal, comparative-legal) methods. Based on the results of the research, it was concluded that the main task of the legal regulation of human rights in the conditions of the use of digital technologies is the protection of fundamental rights and the creation of a legal order. Along with the system of legal norms, the protection of fundamental rights includes other measures developed both within the framework of national legal systems and those provided for in the ECHR. Each of these protection mechanisms undoubtedly pursues specific goals, and the mechanisms are certainly built on legal instruments. One of these mechanisms is the possibility of defending the violated right in court.

Keywords*: human rights, digital technologies, European Court of Human Rights, European Court of Justice.*

ВСТУП

З початку 2000-х років як Європейський суд з прав людини (ЄСПЛ), так і Європейський суд справедливості (ЄС) спостерігали різке зростання кількості прецедентів, пов'язаних з захистом прав людини в Інтернеті. Уже на ранніх стадіях розвитку Інтернету наднаціональні організації розглядали вплив всесвітньої павутини та розробляли вказівки щодо того, як забезпечити захист основних прав.

У 1980 році Організація економічного співробітництва та розвитку (ОЕСР) видала Рекомендації щодо захисту конфіденційності та транскордонних потоків персональних даних. У них контролер даних визначається як сторона, яка компетентна приймати рішення щодо змісту та використання персональних даних незалежно від того збираються, зберігаються, обробляються чи поширюються ці дані цією стороною або агентом від її імені. Персональні дані визначався як будь-яка інформація, що стосується ідентифікованої особи.

Як Додаток до зазначених Рекомендацій від 23 вересня 1980 року групою експертів, призначених OECD для перегляду законодавства в державах-членах, були складені Керівні принципи щодо використання даних особи. Викладалися сім основних принципів щодо збору та використання даних: має бути згода суб'єкта даних; дані мають відповідати меті, для якої вони використовуються; причину збору необхідно вказати під час збору; дані не можуть бути передані третім особам без згоди; дані мають бути захищені; особа повинна мати можливість запитувати, чи має контролер дані, що стосуються її; особа повинна мати право змінювати свої дані.

У 1981 році Рада Європи відкрила для підписання Конвенцію про захист осіб щодо автоматизованої обробки персональних даних від 1 жовтня 1985 року. У цьому документі «контролером даних» було визначено, як фізичну або юридичну особу, державний орган, агентство або будь-який інший орган, який відповідно до національного законодавства уповноважений вирішувати, якою має бути мета збережених даних, які категорії персональних даних повинні зберігатися та які операції з ними здійснювати.

Конвенція також передбачала, що дані, які дозволяють ідентифікувати суб'єкта, слід зберігати лише до тих пір, поки це необхідно для обробки даних. Суб'єкт даних повинен мати право визначати, чи зберігаються персональні дані, а також право вимагати виправлення або видалення збережених даних, якщо обробку було завершено. Конвенція дозволяє безперебійний і безпечний транскордонний обмін даними з іншими країнами, які є сторонами Конвенції. Для моніторингу дотримання положень Конвенції було створено консультативний комітет з повноваженнями вносити пропозиції щодо сприяння або покращення застосування Конвенції, внесення необхідних змін до документу.

У 2004 році був відкритий для підписання Додатковий протокол до Конвенції про захист осіб щодо автоматизованої обробки персональних даних щодо органів нагляду та транскордонних потоків даних з метою посилення захисту персональних даних суб'єктів даних шляхом створення національних наглядових органів і встановлення обмежень на транскордонні потоки даних до третіх країн. Передача персональних даних до третіх країн має бути дозволено лише тоді, коли третя країна забезпечує «належний рівень захисту для передбачуваної передачі даних».

У 2018 році відкрито для підписання наступний Протокол про внесення змін до Конвенції про захист осіб щодо автоматизованої обробки персональних даних протокол. Цей Протокол передбачав зміни до статті 5 Конвенції та додав положення, які зміцнюють гарантії забезпечення прав суб'єкта даних. Внесені зміни передбачали, що обробка даних має бути пропорційною переслідуваній законній меті та відображати на всіх етапах обробки справедливий баланс між зацікавленими інтересами держави та приватними правами та свободами людини. Протокол роз'яснив, за яких обставин третій країні може бути присвоєно «відповідний рівень захисту» та які повноваження повинні мати національні органи нагляду.

Зокрема, належний рівень захисту може бути забезпечений: законодавством цієї держави або міжнародної організації, включаючи відповідні міжнародні договори чи угоди; або спеціально схваленими стандартизованими гарантіями, що мають юридичну силу, прийнятими та впровадженими особами, залученими до передачі та обробки інформації.

Органи влади мають повноваження щодо розслідування та втручання; виконують функції, пов'язані з передачею даних, зокрема щодо затвердження стандартизованих гарантій; мають повноваження виносити рішення щодо порушень положень Конвенції та накладати адміністративні санкції; мають право брати участь у судовому розгляді або доводити до відома компетентних судових органів про порушення положень цієї Конвенції.

1. ОГЛЯД ЛІТЕРАТУРИ

Окремі аспекти правового регулювання та судової практики прав людини у сфері використання цифрових тегнологій стали предметом наукового розгляду О. Гиляки [1, с. 16], В. Серьогіна [2, с. 7], Р. Пожоджука [3, с. 97], М. Абдули [4, с. 16], Ж. Штуйк [5, с. 367], А. Пазюка [6], Р. Кабальського [7, с. 148] та ін.

Р. Пожоджук у своїй статті наголошує, що стрімкий розвиток електронної комерції та повсюдна діджиталізація є безумовно прогресивним моментом еволюції людства. Водночас це спричиняє не тільки позитивні зміни в глобальній економіці, а й створює окремі загрози та виклики, які потребують оперативного реагування та вирішення [3, с. 98].

М. Абдула зазначає, що розвиток у методах виробництва і дистрибуції, а також щодо різних видів договорів щодо товарів і послуг може призвести до загального браку інформації з боку споживача, що впливає на прийняття ним зважених рішень щодо покупки [4, с. 16].

Ж. Штуйк звертає увагу на те, що сучасне інформаційне суспільство у своєму розвитку докорінно змінює взаємодію споживача та постачальника товарів, робіт чи послуг. Споживче право в цілому розглядається як інструмент покращення захисту прав споживачів. Це зумовлює фундаментальне питання, чи інтереси споживача найкраще забезпечуються захисними заходами [5, с. 367].

А. Пазюк, досліджуючи інститут захисту недоторканості приватного життя, зазначає, що у західній правовій доктрині для його позначення використовується термін «прайвесі» (англ. privacy). Найбільш вдалим його перекладом українською мовою є слово приватність, яке співвідноситься зі словом приватний, що характеризує належність до приватної сфери життя людини. Термін приватність за останні роки здобув визнання і закріпився в лексиконі українських правників, завдячуючи лаконічності відображення сутності цього правового феномену [6].

Р. Кабальський у своїй роботі досліджує основні аспекти використання даних електронного листування для доказування в цивільному судочинстві та акцентує увагу на тому, що сьогодні складно знайти людину, яка б не користувалась елек-

тронною поштою, електронним переказом коштів, не мала б електронну сторінку в мережі Інтернет, не приймала б повідомлення в месенджерах, не створював електронні файли. Поряд з позитивними результатами цього явища можна констатувати й негативні наслідки. Наприклад, часте укладання цивільно-правових правочинів безпосередньо в месенджерах, соціальних мережах, наприклад купівля в інтернет-магазині, що не зареєстрований як суб'єкт підприємницької діяльності, а існує лише наприклад як сторінка в мережі Instagram [7, с. 148].

2. МАТЕРІАЛИ ТА МЕТОДИ

Для здійснення дослідження було застосовано систему методів наукового пізнання, зокрема загальнонаукові, приватні методи наукового пізнання, а також спеціально-юридичні. Загальнофілософський (універсальний) метод пізнання автори використовували на всіх етапах пізнавального процесу.

За допомогою методу аналізу розкриті характерні ознаки та вивчені окремі особливості правового регулювання прав людини в умовах використання сучасних цифрових технологій. Порівняльний аналіз надав можливість виявити різні підходи до захисту прав людини в умовах сучасності у практиці Європейського суду з прав людини і Європейського суду справедливості. Наприклад, Європейський суд з прав людини у рішенні «Big Brother Watch та інші проти Сполученого Королівства» не слідує висновкам, зробленим Європейським судом справедливості, і покладається на власну історію прецедентного права, вирішуючи, чи мало місце порушення права на конфіденційність.

За допомогою методу узагальнення виділено спільні риси доктрин Європейського суду з прав людини і Європейського суду справедливості, які дозволяють подолати сучасні виклики забезпечення права на приватність. Так, незважаючи на подекуди різні погляди судів на питання виправданості масового стеження, останній розвиток законодавства Європейського Союзу і Ради Європи демонструє ознаки зближення доктрин суду.

Метод дедукції надав можливість на основі практики Європейського суду з прав людини і Європейського суду справедливості вивести загальний висновок щодо уніфікації підходів до захисту даних в умовах сучасної цифровізації у рішеннях Страсбурзького та Люксембурзького судів. Одним із факторів, що вказує на активний діалог між Судом спарведливості та ЄСПЛ, є перехресне посилання на судові рішення.

Індуктивний метод пізнання норм чинного законодаства щодо реалізації права на приватність та конфіденційність в умовах розвитку сучасних цифрових технологій надав можливість одержати загальний висновок щодо характерних ознак порушення персональних даних особи.

Історичний метод пізнання посприяв розкриттю питання правового регулювання прав людини у сфері використання цифрових технологій шляхом детального аналізу підстав прийняття нормативних актів у хронологічному порядку.

Нормативна база для цього дослідження включає: Конвенція про захист осіб щодо автоматизованої обробки персональних даних [8]; Додатковий протокол до Конвенції про захист осіб щодо автоматизованої обробки персональних даних щодо органів нагляду та транскордонних потоків даних [9]; Директива 95/46/ЕС про захист прав осіб під час обробки персональних даних і їх вільного переміщення [10]; Директива про телекомунікації [11]; Директива Європейського парламенту та Ради 97/13/ЕС [12]; Директива про запровадження Європейського кодексу електронних комунікацій [13]; Хартія основних прав Європейського союзу [14]; Загальний регламент захисту даних (GDPR) [15]; Регламент Європейського Парламенту та Ради 2016/679 про захист фізичних осіб щодо обробки персональних даних і про вільний рух таких даних [16].

Окрім цього, у роботі використовуються доктринальні джерела, що розкривають зміст прав людини у сфері використання цифрових технологій**.**

3. РЕЗУЛЬТАТИ ТА ОБГОВОРЕННЯ

3.1. Правове регулювання прав людини в умовах використання цифрових технологій

У 1995 році Європейське співтовариство прийняло Директиву 95/46/ЕС про захист прав осіб під час обробки персональних даних і їх вільного переміщення. Стаття 12 Директиви надає суб'єктам даних право отримувати інформацію контролера даних, якщо відбувається обробка його даних, і право на виправлення, видалення або блокування даних, якщо вони є неповними або неточними.

Подібно до Конвенції, Директива 1995 року надає чіткі вказівки щодо того, як можна збирати дані. Повинна бути згода суб'єкта даних або обробка повинна бути необхідною на підставі юридичного зобов'язання контролера чи захисту життєво важливих інтересів суб'єкта даних. Суб'єкту даних було надано право отримати інформацію щодо контролера, цілей обробки його даних і переліку одержувачів даних.

Директива про телекомунікації 1997 року та Директива про конфіденційність електронної пошти 2002 року окреслили, як принципи Директиви 1995 року будуть реалізовані у сферах телекомунікацій та онлайн. Директива Європейського парламенту та Ради 97/13/ЕС від 10 квітня 1997 року встановила загальні правила отримання дозволів та індивідуальних ліцензій у сфері телекомунікаційних послуг. Директива 2002/58/ЕС щодо електронної конфіденційності стосується юридичних осіб та не поширюється на зовнішню політику та політику безпеки, поліцейську та судову співпрацю у кримінальних справах. Ця директива засуджує будь-які форми шпигунського програмного забезпечення, яке розглядається як серйозне втручання в конфіденційність. Файли cookie у цьому документі розглядаються як законний інструмент для отримання відповідної інформації. Користувачам має бути надано чітку та стислу інформацію про використання файлів cookie.

Директива Європейського Парламенту та Ради 2002/58/ЕС від 12 липня 2002 року щодо обробки персональних даних і захисту конфіденційності в секторі електронних комунікацій (Директива про конфіденційність та електронні комунікації) допускає обмеження з міркувань національної безпеки щодо конфіденційності передачі, даних трафіку та даних про місцезнаходження. Дозволено зберігати дані протягом обмеженого періоду часу.

Після сплеску терористичних атак на початку 2000-х років у 2006 році було видано Директиву про збереження даних, яка змінила Директиву 2002 року та зобов'язала телекомунікаційні мережі зберігати певні категорії трафіку протягом щонайменше шести місяців. Доступ до даних можна отримати лише з дозволу національного суду відповідно до процедур країни. Зазначене положення було передбачено у Директиві Європейського парламенту та Ради 2006/24/ЕС від 15 березня 2006 року про збереження даних, створених або оброблених у зв'язку з наданням загальнодоступних електронних комунікаційних послуг або громадських комунікаційних мереж, та про внесення змін до Директиви 2002/58/ЕС.

Хартія основних прав Європейського союзу набула чинності разом із Лісабонським договором 1 грудня 2009 року. Хартія відображає принципи Європейської конвенції з прав людини, Європейської соціальної хартії та практики Суду ЄС. Вона включає право на повагу до приватного та сімейного життя, право на захист персональних даних і свободу вираження поглядів та інформації.

У 2016 році було прийнято Загальний регламент захисту даних (GDPR), який набув чинності в травні 2018 року. Регламент замінив Директиву 1995 року. Деякі з ключових удосконалень включають захист даних особи, зміни в праві на видалення та суворі санкції за недотримання регламенту. Тепер захист даних має бути присутній у розробці бізнес-процесів для продуктів і послуг. Контролер повинен вжити заходів для забезпечення того, щоб персональні дані оброблялися лише в обсязі, необхідному для конкретної мети. Параметри конфіденційності за замовчуванням мають бути встановлені на високому рівні.

Регламент (ЄС) 2016/679 Європейського Парламенту та Ради від 27 квітня 2016 року про захист фізичних осіб щодо обробки персональних даних і про вільний рух таких даних, а також про скасування Директиви 95/46/ЕС передбачив реалізацію захисту даних за замовчуванням, право на видалення, яке дозволяє суб'єкту даних вимагати видалення персональних даних на певних підставах, у тому числі якщо дані більше не актуальні для цілей обробки або якщо суб'єкт даних відкликає згоду.

Право на доступ, закріплене у Директиві 1995 року, було розширено. У той час як Директива 1995 року надавала суб'єкту даних право на виправлення, видалення або блокування обробки даних у разі неповного або неточного характеру даних, GDPR, крім того, надало право на видалення, коли персональні дані більше не є необхідні для цілей, для яких вони були зібрані, або якщо користувач

скасовує свою згоду на обробку даних. Це право не є абсолютним – його слід порівнювати зі свободою слова та інформації. Крім того, якщо обробка потрібна для виконання юридичних зобов'язань, в інтересах громадського здоров'я, для цілей архівування в суспільних інтересах або для встановлення, здійснення чи захисту юридичних претензій, запит на видалення також може бути відхилено.

Головне завдання правового регулювання прав людини в умовах використання цифрових технологій – це захист фундаментальних прав та створення правового порядку. Поряд з системою правових норм захист основних прав передбачає й інші заходи, розроблені як в рамках національних правових систем, так і ті, що передбачені у ЄКПЛ. Кожен із цих механізмів захисту переслідує конкретні цілі і механізми, які, безперечно, побудовані на основі правових інструментів. Одним із таких механізмів є можливість захисту порушеного права у суді, про що піде мова у наступному розділі.

3.2. Аналіз справ Європейського суду з прав людини та Суду справедливості Європейського союзу з питань реалізації прав людини в Інтернеті

З початку 2000-х років як Європейський суд з прав людини (ЄСПЛ), так і Суду справедливості Європейського союзу (ЄС) спостерігали різке зростання кількості прецедентного права, пов'язаного з Інтернетом.

Вибрані справи будуть зосереджені на двох аспектах прецедентного права, пов'язаного з Інтернетом, – індивідуальному праві на конфіденційність і захист даних, що здійснюється шляхом виправлення, стирання чи видалення даних, і законності механізмів масового спостереження, особливо якщо вони дозволяють передачу даних до третіх країн.

У справі Google Іспанія [17] розглядалось питання розширення сфери застосування Директиви 1995 року 95/46/ЕС про захист осіб у зв'язку з обробкою персональних даних і вільного переміщення таких даних. Громадянин Іспанії попросив Google видалити особисті дані, які були збережені з аукціону продажу його будинку. В якості правової основи заявник, пан Костеха, посилався на Директиву про захист даних 1995 року. До суду було направлено три питання: чи Директива ЄС про захист даних 1995 року застосовується до пошукових систем, таких як Google; чи застосовується законодавство ЄС до Google Spain, враховуючи, що сервер обробки даних компанії був у Сполучених Штатах; чи має право особа вимагати видалення її особистих даних із доступу через пошукову систему (право бути забутим)?

Суд постановив, що Google можна вважати контролером даних у розумінні Директиви, що особи мають право вимагати видалення персональних даних із загального доступу. Ця справа відіграла важливу роль у складанні проекту Загального регламенту захисту даних (GDPR).

Наступну справу було подано в рамках провадження між паном Шремсом і Уповноваженим із захисту даних щодо відмови останнього розслідувати скаргу

пана Шремса щодо того, що «Facebook Ірландія» передає особисті дані своїх користувачів до Сполучених Штатів Америки та зберігає їх на серверах, розташованих у цій країні.

Для забезпечення належного стандарту захисту персональних даних у Сполучених Штатах були розроблені принципи «безпечної гавані». У США погодилися дотримуватися семи принципів, перелічених у Директиві про захист даних 1995 року: особи повинні бути проінформовані про те, що їх дані збираються та як вони будуть використовуватися; повинна бути можливість відмовитися від збору та передачі даних третім особам; загалом передача може відбуватися лише третім особам, які дотримуються відповідних принципів захисту даних; контролери даних повинні докласти розумних зусиль, щоб запобігти втраті зібраної інформації; зібрані дані мають бути відповідними та надійними для мети, для якої вони були зібрані; особи мають право на доступ до інформації про себе та право змінити або видалити її, якщо вона є недостовірною; Сполучені Штати забезпечать наявність ефективних способів забезпечення виконання правил.

Після викриття певних даних Шремса, ним було подано заяву до ірландського органу з нагляду за захистом даних, щоб перевірити, чи передача даних від Facebook Ireland на сервери, які розташовані в США, відповідала Директиві 1995 року. Орган із захисту даних відмовився розслідувати цю справу, і вона була передана до національних судів Ірландії, де її було передано для попереднього розгляду до Суду справедливості Європейського Союзу. Суду було запропоновано відповісти на запитання: чи наглядовий орган зобов'язаний перевіряти, що Сполучені Штати забезпечують необхідний рівень захисту; або, як альтернатива, посадова особа може та/або повинна провести власне розслідування справи у світлі фактичних подій?

Суд установив, що принципи «безпечної гавані» виходять за рамки повноважень, наданих національним органам із захисту даних Директивою 1995 року. Це конкретне положення надає владі повноваження призупиняти потоки даних, якщо відповідний державний орган у Сполучених Штатах виявляє, що організація не дотримується принципів «безпечної гавані», або якщо існує значна ймовірність того, що принципи порушуються. Оскільки, у рішенні конкретно не зазначено, що Сполучені Штати фактично «забезпечують» необхідний рівень захисту, Суд дійшов висновку, що рішення щодо «безпечної гавані» було недійсним.

У справі «Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein v. Wirtschaftsakademie Schleswig-Holstein» [18] Суд ухвалив рішення щодо питань, які стосуються аспектів усіх попередніх справ. Відповідач створив фан-сторінку у Facebook. Ця фан-сторінка збирала анонімні файли cookie, які зберігалися у Facebook протягом двох років і могли використовуватися для отримання статистики про те, хто переглядав фан-сторінку. Ні Facebook, ні Wirtschaftsakademie не повідомили користувача про збір цих файлів cookie. Управління захисту даних землі Шлезвіг-Гольштейн наказало Wirtschaftsakademie закрити фан-сторінку, або

їй буде загрожувати штраф. Wirtschaftsakademie стверджувала, що вона не є контролером даних відповідно до Директиви 1995 року. Суд підтвердив позицію уряду Німеччини, що втручання держави в зазначеній справі у процес використання особистих даних осіб були необхідними в демократичному суспільстві і не порушує права журналістів на свободу слова. Суд зазначив, що при здійсненні заходів стеження та обробки отриманих даних мають існувати гарантії проти зловживань.

У справі «Big Brother Watch проти Великобританії» [19] Суд ухвалив рішення, яке вплинуло на масове стеження за громадянами Європи. Справа стосувалася характеру перехоплення електронних комунікацій Сполученим Королівством. Після викриття агента Штаб урядового зв'язку був звинувачений у проведенні операції Tempora, яка дозволяла йому підключатися до носіїв та отримувати дані з них. На основі так званих простих селекторів (тобто адреси електронної пошти) дані осіб збиралися та зберігалися. Інші дані автоматично відкидалися. Після процесу сортування система визначала, які дані насправді відкриті. Правовою основою для збору даних були Закони про розвідувальні служби та Закони про служби безпеки.

Big Brother Watch та інші британські некомерційні організації звернулися до уряду з проханням визнати ці операції неприйнятними з точки зору практики Європейського суду з прав людини. Однак судове провадження у національних судах Великобританії завершилося ухваленням рішень не на користь заявників.

ЄСПЛ ухвалив рішення на користь заявників, але наголосив на тому, що масове перехоплення даних є цінним засобом для досягнення законних цілей, особливо з огляду на поточний рівень загрози як від глобального тероризму, так і від інших серйозних злочинів. Зі своєї прецедентної практики Суд дійшов висновку, що держави мають велику свободу розсуду, коли вживають заходів для запобігання проявів тероризму, тому перевіряючи на трирівневий тест, Суд підтримав точку зору, що втручання було необхідним у демократичному суспільстві.

Європейські суди, незважаючи на історичне небажання визнавати шкоду конфіденційності та жахливі наслідки в певних контекстах, продемонстрували більшу готовність приймати такі позови в ряді недавніх резонансних справ. Серед них – трансформаційне рішення Суду справедливості ЄС у справі Google Іспанія про визнання обмеженого права бути забутим у 2014 році; рішення Європейського суду з прав людини про скасування принципів безпечної гавані у 2015 році; та рішення Європейського суду з прав людини, яке продемонструвало практику масового онлайн-спостереження Штаб-квартири урядового зв'язку Сполученого Королівства, британського агентства сигнальної розвідки, яка порушувала конфіденційність і не передбачала достатніх гарантій захисту від стеження. Суди США не виявляли такого ж ставлення до справ щодо захисту прав людини на приватність в умовах цифрових технологій, але і там з'являються ознаки того, що американські суди також можуть бути більш відкритими до претензій щодо конфі-

денційності та стеження, оскільки четвертий окружний апеляційний суд нещодавно дозволив продовжити позов, поданий Американською асоціацією громадянських свобод проти уряду США щодо шкоди конфіденційності через належне спостереження, скасовуючи ухвалу суду нижчої інстанції про її повну відмову.

ВИСНОВКИ

Розгляд прецедентного права Суду справедливості Європейського союзу та Європейського суду з прав людини дозволяє зробити оцінку того, чи відображають рішення Страсбурзького та Люксембурзького судів уніфікований чи розрізнений підхід до захисту даних в умовах сучасної цифровізації.

Одним із факторів, що вказує на активний діалог між Судом справедливості ЄС та ЄСПЛ, є перехресне посилання на судові рішення. Наприклад, такі посилання присутні в тексті рішення по справі «Digital Rights Ireland Ltd проти Міністра зв'язку, морських і природних ресурсів та інших». В ньому, при розгляді пропорційності втручання в основні права Ірландського органу із захисту даних, цитується рішення по справі «Марпер проти Сполученого Королівства», у виборі не розслідувати справу, а також встановлюючи, що законодавство ЄС, яке розглядається, повинно встановлювати чіткі та точні правила, що регулюють сферу застосування заходів щодо особистих даних особи, а також запроваджувати мінімальні гарантії, щоб особи, чиї дані були збережені, мали достатні гарантії для ефективного захисту своїх особистих даних.

Європейський суд з прав людини, в свою чергу, у своєму рішенні «Big Brother Watch та інші проти Сполученого Королівства», присвятив цілий розділ свого рішення прецедентному праву Суду справедливості Європейського Союзу. У своєму рішенні Суд не визнав, що масове стеження порушує права, надані Європейською конвенцією. Як наголошується в окремій думці суддів Пардалоса та Ейке, Суд вирішив не слідувати висновкам, зробленим Європейським судом, і замість цього покладатися на власну історію прецедентного права, вирішуючи, чи мало місце порушення права на конфіденційність. Судді у своїй думці висловлюють припущення, що прецедентне право Суду справедливості ЄС відображає, що обсяг захисту, наданий Хартією основних прав, є ширшим, ніж обсяг Конвенції про захист прав і основоположних свобод.

Відмову від ширшого обсягу захисту прав також можна побачити в рішенні ЄСПЛ по справі «M. L. та W. W. проти Німеччини». Суд встановив, що розміщення статті на веб-сайті в Інтернеті не є порушенням права на конфіденційність, її видалення може мати негативний вплив на свободу слова. Однак слід зазначити, що на відміну від аргументації у справі «Google Spain», у цій справі видаленню підлягала сама стаття, а не згадування її у пошуковій системі.

Нарешті, незважаючи на подекуди різні погляди Суду справедливості Європейського Союзу та Європейського суду з прав людини на питання виправданос-

ті масового стеження, останній розвиток законодавства ЄС і Ради Європи демонструє ознаки зближення доктрин суду. Хартія основних прав ЄС базується на Європейській конвенції з прав людини. Тепер одна з цілей розвитку законодавства ЄС полягає в тому, щоб стандарти захисту даних держав-підписантів відповідали належному рівню захисту, передбаченому у Загальному регламенті захисту даних.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

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

[2] Серьогін В. О. Прайвесі як право «бути залишеним у спокої». *Право і Безпека*. 2010. № 3. С. 6–9.

[3] Походжук Р. Захист права на недоторканність приватного життя споживача послуг у мережі інтернет. *Приватне право і підприємництво*. 2019. Вип. 19. С. 97–106.

[4] Al-Ghafri Abdulla M. A. The Inadequacy of Consumer Protection in the UAE: The Need for Reform. Thesis submitted to the department of law, Brunal University, UK for the degree of doctor of philosophy in law in 2013, 280 p. URL: https://bura.brunel.ac.uk/bitstream/2438/7691/1/FulltexThesis.pdf (дата звернення: 04.12.2023).

[5] Jules Stuyck. European Consumer Law After the Treaty of Amsterdam: Consumer Policy In or Beyond the Internal Market? (2000) 37, Common Market Law Review, Issue 2, pp. 367–400. URL: http://www.asf.com.pt/winlib/cgi/winlibimg.exe?key=&doc=9775&img=1189 (дата звернення: 04.12.2023).

[6] Пазюк А. В. Право на приватність в інформаційному суспільстві. URL: http://cyberpeace.org.ua/ files/pravo_na_privatnist__v_informaciinomu_suspil_stvi.pdf (дата звернення: 04.12.2023).

[7] Р. Кабальський. Окремі аспекти використання даних електронного листування для доказування в цивільному судочинстві. *Юридичний науковий електроний журнал.* 2022. 12. С. 148–150.

[8] Конвенція про захист осіб щодо автоматизованої обробки персональних даних від 28.01.1981. *Офіційний вісник України*. 2011. № 58. Ст. 701.

[9] Додатковий протокол до Конвенції про захист осіб щодо автоматизованої обробки персональних даних щодо органів нагляду та транскордонних потоків даних від 08.11.2001. *Офіційний вісник України*. 2011. № 1(58).

[10] Директива 95/46/ЕС про захист прав осіб під час обробки персональних даних і їх вільного переміщення від 24.10.1995. URL: https://zakon.rada.gov.ua/laws/show/994_242#Text. (дата звернення: 04.12.2023).

[11] Директива 2002/21/ЄС від 07.03.2002 про спільні правові рамки для електронних комунікаційних мереж та послуг. URL: https://zakon.rada.gov.ua/laws/show/984_003-02#Text. (дата звернення: 04.12.2023).

[12] Директива Європейського парламенту та Ради 97/13/ЕС «Про спільну базу для загальних дозволів та індивідуальних ліцензій в сфері телекомунікаційних послуг» від 10.04.1997. URL: https://zakon.rada.gov.ua/laws/show/994_096#Text. (дата звернення: 04.12.2023).

[13] Директива ЄС 2018/1972 від 11.12.2018 про запровадження Європейського кодексу електронних комунікацій**.** URL: https://zakon.rada.gov.ua/laws/show/984_013-18#Text. (дата звернення: 04.12.2023).

[14] Хартія основних прав Європейського союзу від 07.12.2000. URL: https://zakon.rada.gov.ua/laws/show/994_524#Text (дата звернення: 04.12.2023).
[15] Загальний регламент захисту даних (GDPR). URL: https://gdpr-text.com/uk/. (дата звернення: 04.12.2023).
[16] Регламент Європейського Парламенту та Ради 2016/679 про захист фізичних осіб щодо обробки персональних даних і про вільний рух таких даних від 27.04.2016. URL: https://zakon.rada.gov.ua/laws/show/984_008-16#Text (дата звернення 04.12.2023).
[17] Рішення Суду Справедливості Європейського союзу у справі «Google Spain SL, Google Inc. v Agencia Española de Protección de Datos, Mario Costeja González» від 13.05.2014. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62012CJ0131 (дата звернення: 04.12.2023).
[18] Рішення Європейського суду з прав людині у справі «Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein v. Wirtschaftsakademie Schleswig-Holstein» від 05.06.2018. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62016CJ0210 (дата звернення: 04.12.2023).
[19] Рішення Європейського суду з прав людині у справі «Big Brother Watch проти Великобританії» від 25.05.2021. URL: https://www.echr.com.ua/translation/sprava-big-brother-watch-ta-inshi-proti-spoluchenogo-korolivstva-pres-reliz/ (дата звернення: 04.12.2023).

REFERENCES

[1] Hyliaka, O. (2023). Human rights in the digital age: Challenges, threats and prospects. *Scientific legal journal,* 28 (1), 16.
[2] Seryogin, V. (2010). Privacy as the right «to be left alone.» *Law and Security*, 3, 6–9.
[3] Pokhozhuk, R. (2019). Protection of the right to inviolability of private life of the user of services on the Internet. *Private law and entrepreneurship*, 19, 97–106.
[4] Al-Ghafri, Abdulla M. A. (2013). *The Inadequacy of Consumer Protection in the UAE: The Need for Reform. Thesis submitted to the department of law, Brunal University, UK for the degree of doctor of philosophy in law*. Retrieved from https://bura.brunel.ac.uk/bitstream/2438/7691/1/FulltexThesis.pdf.
[5] Stuyck, J. (2000). European Consumer Law After the Treaty of Amsterdam: Consumer Policy In or Beyond the Internal Market? *Common Market Law Review*, 37(2), 367–400. Retrieved from http://www.asf.com.pt/winlib/cgi/winlibimg.exe?key=&doc=9775&img=1189.
[6] Pazyuk, A. (2023). The right to privacy in the information society. Retrieved from http://cyberpeace.org.ua/files/pravo_na_privatnist__v_informaciinomu_suspil_stvi.pdf.
[7] Kabalskyi, R. (2022). Certain aspects of using e-mail data for evidence in civil proceedings. *Legal scientific electronic journal*, 12, 148–150.
[8] Convention on the Protection of Individuals with regard to Automated Processing of Personal Data (1981, January). *Official Gazette of Ukraine*, 58, 701.
[9] Additional Protocol to the Convention on the Protection of Individuals with regard to the Automated Processing of Personal Data Regarding Supervisory Authorities and Cross-Border Data Flows (2001, November). *Official Gazette of Ukraine*, 1(58).
[10] Directive 95/46/EC on the protection of the rights of individuals during the processing of personal data and their free movement (1995, October). Retrieved from https://zakon.rada.gov.ua/laws/show/994_242#Text.

[11] Directive 2002/21/EC on a common legal framework for electronic communications networks and services (2002, March). Retrieved from https://zakon.rada.gov.ua/laws/show/984_003-02#Text.
[12] Directive 97/13/EC of the European Parliament and the Council «On a common basis for general authorizations and individual licenses in the field of telecommunications services» (1997, April). Retrieved from https://zakon.rada.gov.ua/laws/show/994_096#Text.
[13] EU Directive 2018/1972 on the introduction of the European Electronic Communications Code. (2018, December). Retrieved from https://zakon.rada.gov.ua/laws/show/984_013-18#Text.
[14] Charter of Fundamental Rights of the European Union dated (2000, December). Retrieved from https://zakon. rada.gov.ua/laws/show/994_524#Text.
[15] General Data Protection Regulation (GDPR) Retrieved from https://gdpr-text.com/uk/.
[16] Regulation of the European Parliament and the Council 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (2016, April). Retrieved from https://zakon.rada.gov.ua/laws/show/984_008-16#Text.
[17] Decision of the Court of Justice of the European Union in the case «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.
[18] The decision of the European Court of Human Rights in the case «Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein v. Wirtschaftsakademie Schleswig-Holstein» (2018, June). Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62016CJ0210.
[19] Decision of the European Court of Human Rights in the case «Big Brother Watch v. Great Britain» (2021, May). Retrieved from https://www.echr.com.ua/translation/sprava-big-brother-watch-ta-inshi-proti-spoluchenogo-korolivstva-pres-reliz/.

Олег Сергійович Гиляка
Кандидат юридичних наук, старший дослідник
Заступник головного ученого секретаря –
начальник управління стратегічного розвитку
Національної академії правових наук України
61024, вул. Пушкінська, 70, Харків, Україна

Доцент кафедри прав людини та юридичної методології
Національного юридичного університету імені Ярослава Мудрого
61024, вул. Пушкінська, 77, Харків, Україна

Oleh S. Hyliaka
Candidate of Law, Senior Researcher
Deputy chief academic secretary –
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

Анастасія Муслімівна Мерник
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
Національного юридичного університету 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
61024,77 PushkinskaStr., Kharkiv, Ukraine

Рекомендоване цитування: Гиляка О. С., Мерник А. М. Правове регулювання та практика Європейського Суду з прав людини і Європейського Суду справедливості щодо прав людини у сфері використання цифрових технологій. *Вісник Національної академії правових наук України*. 2024. Том 31. № 1. С. 40–55.

Suggested Citation: Hyliaka, O. S., & Mernyk, A. M. (2024). Legal Regulation and Practice European Court of Human Rights and the European Court of Justice Concerning Human Rights in the Sphere of use of Digital Technologies. *Journal of the National Academy of Legal Sciences of Ukraine*, 31(1), 40–55.

Стаття надійшла / Submitted: 09/01/2024
Доопрацьовано / Revised: 08/02/2024
Схвалено до друку / Accepted: 28/03/2024