УДК 342.7
DOI: 10.31359/1993-0909-2023-30-1-15

Олег Сергійович Гиляка
Національна академія правових наук України
Харків, Україна

Кафедра міжнародного приватного права та порівняльного правознавства
Національний юридичний університет імені Ярослава Мудрого
Харків, Україна

ПРАВО НА ПРИВАТНІСТЬ ТА ЗАХИСТ ПЕРСОНАЛЬНИХ ДАНИХ В УМОВАХ ЦИФРОВІЗАЦІЇ

Анотація. *У статті досліджуються окремі аспекти права людини на приватність, а також особливості захисту персональних даних в умовах цифровізації. Мета дослідження полягає у здійсненні теоретико-правового аналізу права на приватність та визначення правових механізмів та сучасних тенденцій їх розвитку у сфері захисту персональних даних в умовах цифровізації. Для досягнення поставленої мети у роботі використовується система методів наукового пізнання, зокрема загальнонаукові, приватні, а також спеціально-юридичні. Зроблено висновок, однією з найбільш суттєвих проблем цифрової епохи стає захист персональних даних. Дані, збережені на цифрових платформах, стають потенційною мішенню шахраїв та злочинців, легко втрачаються, з ними досить складно оперувати пересічному користувачу. У сфері, пов'язаній з використанням персональних даних, відмічається зростання злочинів та правопорушень. Задля можливого усунення порушень у цій сфері та захисту персональних даних постійно оновлюється законодавство та правила, спрямовані на забезпечення безпечного зберігання цифрових даних. Законодавство, зокрема, встановлює механізми захисту від несанкціонованого доступу, використання та відновлення даних осіб. Основою для забезпечення безпеки персональних даних є належним чином законодавчо врегульовані процеси та технології, призначені для підтримки та спостереження за роботою цифрових систем та даних. Цифрові технології безпеки, такі як ідентифікація, авторизація користувачів, аутентифікація протоколів, шифрування і контроль доступу, дають фізичні засоби захисту даних. Але не менш важливим для забезпечення захисту персональних даних є дотримання правил та методик безпечного використання цифрових технологій. Процес встановлення компетентних та модернізованих механізмів захисту даних допоможе поліпшити безпеку цифрових ресурсів та захистити персональні дані всіх користувачів.*

Ключові слова: *права людини, право на приватність, персональні дані, захист персональних даних, цифровізація.*

Oleh S. Hyliaka
National Academy of Legal Sciences of Ukraine
Kharkiv, Ukraine

Department of Private International and Comparative Law
Yaroslav Mudryi National Law University
Kharkiv, Ukraine

RIGHT TO PRIVACY AND PROTECTION PERSONAL DATA IN DIGITALIZATION CONDITIONS

Abstract. *The article examines certain aspects of the human right to privacy, as well as the features of personal data protection in the conditions of digitalization. The purpose of the study is to carry out a theoretical and legal analysis of the right to privacy and to determine the legal mechanisms and modern trends in their development in the field of personal data protection in the conditions of digitalization. To achieve the set goal, the work uses a system of methods of scientific knowledge, in particular, general scientific, private, as well as special legal methods. It was concluded that one of the most significant problems of the digital age is the protection of personal data. Data stored on digital platforms become a potential target of fraudsters and criminals, are easily lost, and are quite difficult for the average user to operate with. In the area related to the use of personal data, there is an increase in crimes and offenses. In order to possibly eliminate violations in this area and protect personal data, legislation and regulations aimed at ensuring the safe storage of digital data are constantly being updated. The legislation, in particular, establishes mechanisms for protection against unauthorized access, use and recovery of personal data. The basis for ensuring the security of personal data is properly regulated processes and technologies designed to support and monitor the operation of digital systems and data. Digital security technologies such as identification, user authorization, protocol authentication, encryption and access control provide physical means of data protection. But no less important to ensure the protection of personal data is compliance with the rules and methods of safe use of digital technologies. The process of establishing competent and modernized data protection mechanisms will help improve the security of digital resources and protect the personal data of all users.*

Key words: *human rights, right to privacy, personal data, protection of personal data, digitization.*

ВСТУП

Пандемія COVID-19 спричинила суттєві зміни в економічному та соціальному житті більшості країн світу. Однією з таких характерних змін стало прискорене впровадження цифрових технологій у різних сферах. Повномасштабна військова агресія російської федерації проти України викликала ще більшу потребу в використанні цифрових технологій, виходячи першочергово із безпекової ситуації. В умовах обмежень на пересування, неможливості організувати нормальний навчальний та трудовий процес, заборони проведення різного роду

масових заходів, які були введені на території України, почали активно використовуватись цифрові рішення для продовження діяльності у віддаленому форматі.

Цифровізація сприяє переходу в онлайн-середовище більшості сфер, зокрема таких як медицина та освіта, дозволяє здійснювати онлайн-покупки, отримувати більше інформації та здійснювати її обмін. Розвиток передових технологій неминуче вимагає повноцінного законодавчого врегулювання їх використання, створення відповідної правової бази, яка б забезпечила стандарти та правила широкого використання цифрових технологій. При цьому варто наголосити, що ефективна національна правова база має вирішальне значення для забезпечення захисту від незаконного чи свавільного втручання, адже національне законодавство в більшій мірі не пристосоване до розвитку комунікаційних технологій та заходів спостереження, що здійснюють нові технології. Крім того, відсутній такий важливий запобіжник від зловживань, як належний нагляд за заходами стеження та їх повноцінна перевірка.

Не викликає жодного сумніву, що технологічний прогрес істотно покращив спілкування та обмін інформацією, зокрема в режимі онлайн. Завдяки йому спростилися процеси обміну, зберігання, отримання інформації, можливість проведення різного роду дистанційних переговорів тощо. Але разом з цим виникають й певні складнощі, адже нові пристрої та технології нерідко здійснюють електронне стеження та перехоплення інформації. Причому інколи розробники цифрових рішень використовують їх відверто для безпосереднього шпигунства.

Захист прав людини в мережі Інтернет невпинно стає надважливим завданням для всіх країн. Ті самі права, які люди мають офлайн, повинні бути ефективно захищені онлайн, зокрема мова йде про свободу вираження поглядів та право на приватність. Права людини в цифровій сфері необхідно захищати та заохочувати так само, як і права людини у фізичному світі.

Проблеми, пов'язані з захистом права на приватне життя та персональних даних в епоху цифрових технологій неодноразово ставали предметом обговорень на засіданнях Організації Об'єднаних Націй. Зокрема, наголошувалось на тому, що технологічний розвиток розширив можливості держав і комерційних суб'єктів для стеження, дешифрування та масового збору даних, що може серйозно порушити право людей на приватність, назріла потреба знайти відповідний баланс між законними інтересами національної безпеки та індивідуальними свободами. Відзначено, що хоча сучасні комунікаційні технології є потужним інструментом для демократії, вони також сприяли стиранню меж між публічною та приватною сферами, тому виникають занепокоєння щодо широкого спектру режимів стеження за безпекою та потенційних вторгнень, яким сприяють сучасні технології [1].

Окремі аспекти права на приватність та захисту персональних даних стали предметом дослідження таких учених, як О. Баранов [2], В. Брижко [3], О. Рогова [4] та ін. Розгляд цього питання здійснювали й зарубіжні вчені – Х. Ніссенбаум

[5], Д. Солове [6], М. Фрумкін [7] та ін. Незважаючи на те, що порушеною проблематикою займалася значна кількість науковців, багато її аспектів нині залишаються малодослідженими чи дискусійними, особливо в контексті постійної зміни відносин у цій сфері та відповідно необхідності оновлення законодавства. Слід також враховувати, що тенденції розвитку правового регулювання захисту персональних даних в Європейському Союзі є досить динамічними.

Мета дослідження полягає у здійсненні теоретико-правового аналізу права на приватність та визначення правових механізмів та сучасних тенденцій їх розвитку у сфері захисту персональних даних в умовах цифровізації.

1. МАТЕРІАЛИ ТА МЕТОДИ

Для здійснення дослідження було застосовано систему методів наукового пізнання, зокрема загальнонауковий метод аналізу, приватні методи наукового пізнання (порівняльний, кількісного й якісного аналізу), а також спеціально-юридичні (формально-юридичний, порівняльно-правовий). Загальнофілософський (універсальний) метод пізнання використовувався на всіх етапах пізнавального процесу.

За допомогою методу аналізу розкриті характерні ознаки та вивчені окремі особливості права на приватність та захист персональних даних в умовах цифровізації. Він надав змогу встановити, що вперше нормативне закріплення норм з правового регулювання захисту персональних даних відбулося в тих положеннях міжнародних договорів з прав людини, які гарантували право на приватність та визначити правові механізми та сучасні тенденції їх розвитку у сфері захисту персональних даних в умовах цифровізації. За допомогою методу узагальнення сформовано основні особливості та підходи, закріпелені в міжнародних нормативних актах щодо захисту персональних даних.

Метод дедукції надав можливість на основі загального терміну «право на приватність» зробити висновок, що відповідно до європейського підходу, захист персональних даних випливає із права на захист приватного життя. Відповідні питання займають важливе місце у діяльності Європейського Союзу та таких організацій, як Організація Об'єднаних Націй та Рада Європи. На міжнародному та наднаціональному рівнях розрізняється захист персональних даних загалом та захист даних при автоматизованій обробці. Саме останньому все частіше присвячується найбільш детальна правова регламентація. Індуктивний метод пізнання надав можливість одержати загальний висновок щодо характерних ознак захисту персональних даних особи в умовах цифрової трансформації.

Порівняльний метод пізнання надав можливість виявити різні підходи до захисту персональних даних в країнах світу, встановити країни з найвищий рівнем такого захисту.

У статті застосовувались 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

та розкритті особливостей правових підстав для обмеження використання персональних даних.

Нормативна база для цього дослідження включає міжнародні акти та нормативно-правові акти України, зокрема: Закон України «Про інформацію» від 2 жовтня 1992 р. №2657-XII [8], Закон України «Про доступ до публічної інформації» від 13 січня 2011 р. №2939-VI [9] та Закон України «Про захист персональних даних» від 1 червня 2010 р. №2297-VI [10].

2. РЕЗУЛЬТАТИ ТА ОБГОВОРЕННЯ

Цифрова трансформація стала новим етапом розвитку цивілізації, процесом суспільно-економічної, гуманітарної та інформаційної модернізації. В умовах цієї трансформації здійснюється глобальна електронізація даних, а значні обсяги персональних даних зберігаються у формі, доступній для передачі, поширення чи обміну на різних рівнях, в тому числі транснаціональному. Проте, такі процеси можуть бути ризикованим з погляду захисту персональних даних.

Захист персональних даних – досить актуальна тема, й з кожним днем її актуальність зростає. Захист персональних даних полягає у забезпеченні їх конфіденційності, безпечного поширення та захисту від несанкціонованого використання. З цього погляду, цифрова трансформація створює ряд викликів щодо захисту даних та забезпечення їх достовірності, належного зберігання та використання. Основні засоби та методи захисту персональних даних в умовах цифрової трансформації включають шифрування даних у доступній формі, використання анонімізації даних, визначення правил та процедур для безпечного управління даними, щоб визначити те, як доступ до них буде організовано, і забезпечити їх мінімальне затребування з метою вирішення різних питань.

Як відзначила Хелен Ніссенбаум, професор кафедри інформаційних технологій Корнельського університету, недоторканність приватного життя – це не право на секретність чи контроль, а право на належний потік особистої інформації. Це означає, що залежно від ситуації та контексту, людина може оцінити та вирішити, чим поділитися з іншими у цифровому середовищі. Іншими словами, людина має право знати, як і для яких цілей використовуються її дані, хто і як довго їх зберігає, а також кому доступна така інформація. Особа повинна мати можливість звернутись про видалення особистих даних або їх виправлення [5].

У більшості країн право на захист персональних даних розглядається як фундаментальне. Так, відповідно до європейського підходу, захист персональних даних випливає із права на захист приватного життя. Відповідні питання займають важливе місце у діяльності Європейського Союзу та таких організацій, як Організація Об'єднаних Націй та Рада Європи. На міжнародному та наднаціональному рівнях розрізняється захист персональних даних загалом та захист даних при автоматизованій обробці. Саме останньому все частіше присвячується найбільш детальна правова регламентація.

Зростання штучного інтелекту значною мірою впливає на суспільство, і в цьому контексті забезпечення права на приватність стає гострою соціальною проблемою, яка заслуговує на особливу увагу. Велика кількість особистої інформації, особливо конфіденційного характеру, збирається з багатьох джерел, проходить через певні операції, а потім акумулюється. Це становить велику загрозу безпеці права громадян на конфіденційність.

Вперше нормативне закріплення норми з правового регулювання захисту персональних даних відбулося в тих положеннях міжнародних договорів з прав людини, які гарантували право на приватність. Зокрема, у ст. 12 Загальної декларації прав людини встановлено, що ніхто не може зазнавати безпідставного втручання в його особисте і сімейне життя, безпідставного посягання на недоторканність його житла, таємницю його кореспонденції або на його честь і репутацію. Кожна людина має право на захист закону від такого втручання або таких посягань [11].

Згідно зі статтею 8 Конвенції про захист прав людини і основоположних свобод [12] право на захист щодо обробки персональних даних є частиною права на повагу до приватного та сімейного життя, до житла та кореспонденції. Конвенція Ради Європи від 28 січня 1981 року № 108 «Про захист осіб у зв'язку з автоматизованою обробкою персональних даних» [13] – перший міжнародний юридично зобов'язальний документ, який стосується виключно питань захисту персональних даних. Конвенція пройшла процес оновлення, який було завершено прийняттям Протоколу про внесення змін до Конвенції CETS № 223 [14].

У праві Європейського Союзу право на захист персональних даних визнано як основоположне право. Це було підтверджено у Договорі про функціонування Європейського Союзу, а також у Хартії основних прав Європейського Союзу. Директива про захист персональних даних 1995 року [15] була першим документом, який регулював захист персональних даних у праві Європейського Союзу. Враховуючи швидкі технологічні зміни, з метою адаптування правил захисту персональних даних до ери цифрових технологій Європейський Союз у 2016 році прийняв нове законодавство. Загальний регламент захисту персональних даних набув чинності у 2018 році, а Директива про захист персональних даних втратила чинність.

Так, Регламентом 2016/679 Європейського Парламенту та Ради від 27 квітня 2016 року про захист фізичних осіб стосовно обробки персональних даних та про вільне переміщення таких даних, а також про скасування Директиви 95/46/ЄС (Загальний регламент про захист даних) [16] передбачаються відповідні повноваження для моніторингу та забезпечення дотримання правил захисту персональних даних та санкції за їх порушення в державах-членах. Документом зазначається, що обробка персональних даних є законною тільки в тому разі і в тій мірі, в якій виконується щонайменше одна з таких умов:

– суб'єкт персональних даних дав згоду на обробку своїх персональних даних для однієї чи кількох конкретних цілей;

– обробка персональних даних є необхідною для виконання договору, в якому суб'єкт даних є стороною або з метою вжиття заходів на прохання суб'єкта даних для укладення договору;

– обробка персональних даних є необхідною для відповідності юридичним зобов'язанням, покладеним на контролера;

– обробка персональних даних є необхідною для захисту важливих інтересів суб'єкта, його даних або іншої фізичної особи;

– обробка персональних даних є необхідною для виконання поставленого завдання, що проводиться в інтересах суспільства або під час виконання службових обов'язків, покладених на контролерів;

– обробка персональних даних є необхідною для цілей захисту законних інтересів, які переслідує контролер або третя сторона, за винятком випадків, коли такі інтереси перекриваються інтересами основоположних прав і свобод суб'єкта даних, який потребує захисту персональних даних, зокрема, коли суб'єктом даних є дитина.

У національному законодавстві відправною точкою в сфері захисту права на приватність та персональних даних є положення Конституції України [17]. Так, ст. 32 Конституції України проголошує, що ніхто не може зазнавати втручання в його особисте і сімейне життя, крім випадків, передбачених Конституцією України. Не допускається збирання, зберігання, використання та поширення конфіденційної інформації про особу без її згоди, крім випадків, визначених законом, і лише в інтересах національної безпеки, економічного добробуту та прав людини. Саме ці норми Конституції становлять основу для побудови та розвитку національного законодавства щодо захисту персональних даних.

В Україні діють три основних закони, що регулюють питання доступу до інформації та захисту персональних даних: Закон України «Про інформацію» [8], Закон України «Про доступ до публічної інформації» [9] та Закон України «Про захист персональних даних» [10]. Їх положення передбачають режим доступу до публічної інформації, захист персональних даних та юридичні механізми, які застосовуються для пошуку балансу між правом знати та правом на приватність. Так, частина 2 статті 6 Закону України «Про доступ до публічної інформації» [9] містить юридичний механізм, який є обов'язковим до застосування у переважній більшості випадків обмеження доступу до інформації. Винятки становлять лише ті категорії інформації, які, у відповідності до норм чинного законодавства, не можуть бути обмежені в доступі.

Проте, стрімкий розвиток відносин та ускладнення технологій зумовлюють необхідність подальшого удосконалення правової регламентації в цій сфері. Зокрема, важливим питанням на сьогодні є можливість видалення персональних даних, які надавались особою раніше. Закон України «Про захист персональних даних» [10] передбачає таку можливість, але не допускає можливості це зробити особою самостійно за власним зверненням. Підставами для видалення персональ-

них даних можуть бути лише рішення суду або припис Уповноваженого Верховної Ради України з прав людини. Враховуючи складність таких звернень та відповідних розглядів, завантаженість цих органів, процес видалення персональних даних може затягуватись на невизначений термін.

У щоденному житті користувачі продовжують залишати чимало особистих даних в мережі Інтернет, навіть не здогадуючись про можливість використання їх третіми особами. Тому важливим постає питання щодо контролю за дотриманням правил збору, зберігання та захисту персональних даних. Врегулювання спорів щодо захисту персональних даних та доступу до інформації може відбуватися через оскарження до суду, який повноважний приймати рішення по суті справи чи оскарження до Уповноваженого Верховної Ради України з прав людини, представники якого проводять перевірки та складають протоколи про факти порушення права на захист персональних даних та права на доступ до інформації, і на основі таких протоколів суд може накласти адміністративне стягнення. Однак, на сьогодні в Україні діє здебільшого модель парламентського контролю за дотриманням приписів законодавства України про захист персональних даних та про доступ до публічної інформації (через Уповноваженого Верховної Ради України з прав людини).

Відповідно до Додаткового протоколу до Конвенції про захист осіб у зв'язку з автоматизованою обробкою персональних даних щодо органів нагляду та транскордонних потоків даних [14], який Україна ратифікувала у 2010 році, кожна сторона має створити контролюючий орган, який би здійснював контроль за дотриманням права на захист персональних даних. Для виконання цих функцій такий орган повинен бути незалежним від інших органів влади. У 2018 році як у праві Ради Європи, так і в праві Європейського Союзу відбулись реформи та модернізація правил захисту права на захист персональних даних. З цього часу незалежний нагляд за дотриманням права на захист персональних даних є суттєвим елементом європейського права із захисту персональних даних.

У зв'язку з цим в Україні точаться дискусії, який саме орган буде здійснювати відповідний контроль. Задля того, аби привести законодавство України у відповідність до міжнародних стандартів у сфері захисту персональних даних, зокрема щодо створення окремого незалежного контролюючого органу у сфері захисту персональних даних, у 2021 році було внесено проект Закону України «Про Національну комісію з питань захисту персональних даних та доступу до публічної інформації» [18]. Наразі законопроект перебуває на розгляді профільного комітету. Варто зазначити, що експерти у сфері захисту персональних даних вже висловили певні зауваження до законопроекту, та відмітили, що він потребує доопрацювання, адже окремі його положення не відповідають вимогам правової визначеності та передбачуваності, потребують запровадження більш чітких критеріїв необхідності втручання [19].

Варто відмітити, що досить багатою є практика Європейського Суду з прав людини у цій сфері. ЄСПЛ розглядав велику кількість справ, де йшлося про захист

персональних даних, включно з перехопленням інформації, різними формами спостереження з боку як державного, так і приватного сектору та захист від зберігання персональних даних державними органами. Право на повагу до приватного життя не є абсолютним правом, оскільки його реалізація може становити втручання в інші права, наприклад право на свободу вираження поглядів та доступ до інформації і, навпаки, реалізація цих прав може обмежувати право на приватність. Отже, ЄСПЛ намагається знайти баланс між різними правами. Суд роз'яснював, що стаття 8 ЄКПЛ не тільки зобов'язує держави утримуватися від будь-яких дій, які могли б порушити гарантоване Конвенцією право, але й за певних обставин передбачає позитивні зобов'язання держав активно забезпечувати ефективне дотримання права на приватне і сімейне життя.

Так, Європейський Суд у справі S. and Marper v. The United Kindgom вказав, що захист даних особистого характеру має найважливіше значення для можливості особи здійснювати право на недоторканність приватного і сімейного життя. Однією з гарантій дотримання таких прав є зобов'язання органів державної влади і приватних компаній дотримуватися певних правил і процедур при обробці персональних даних. Так, персональні дані повинні оброблятися тільки у випадках, встановлених законом або у випадках, коли особи самі дали на це згоду. В цілому громадяни повинні мати змогу здійснювати контроль над власними персональними даними (перевіряти їх точність, виправляти, видаляти або робити запити, щоб вони не зберігалися довше необхідного терміну) [20].

Одним із найбільш значущих прецедентних рішень ЄСПЛ, присвячених питанням анонімності в мережі Інтернет, стало рішення у справі Делфі А. проти Естонії (Delfi AS v. Estonia, no. 64569/09, 10 October 2013). Вказавши в рішенні у даній справі на важливість онлайн-анонімності для вільного вираження ідей і думок, суд тим не менше зазначив специфіку мережі Інтернет як безпрецедентного за доступністю, швидкістю і охопленням засобом поширення інформації, здатного довгий час зберігати дані після їх розкриття, що значно погіршує наслідки незаконних висловлювань порівняно з традиційними ЗМІ. Більш того, суд допустив і охарактеризував різні ступені онлайн-анонімності, вказавши, що користувач Інтернету може бути анонімним для широкого загалу, але при цьому ідентифікуватися постачальником послуг через обліковий запис або контактні дані. Надання (розкриття) цих даних, як правило, вимагає припису слідчого або судового органу і підлягатиме обмежувальним умовам. Проте в деяких випадках це може знадобитися для виявлення і переслідування винних [20].

Досить цікавою є судова практика щодо захисту персональних даних в контексті так званої нейтральності мережі Інтернет. Нейтральність мережі Інтернет – один із основних її принципів, який розуміється як забезпечення рівної швидкості доступу до будь-яких веб-ресурсів незалежно від їхнього контенту, без будь-яких пріоритетів чи привілеїв. Найбільш очевидно конфлікт між питанням захисту персональних даних та нейтральності мережі проявляється у зв'язку з поширен-

ням так званих фейкових новин, а також застарілої інформації, що зазвичай має наслідком втручання в персональні дані.

Такий конфлікт знайшов відображення у практиці Європейського Суду у справі Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González [21]. Заявник просив представників пошукової системи видалити посилання на публікацію 1998 року, де йшлося про розпродаж його майна за борги, аргументуючи тим, що проблема боргів давно врегульована і відповідна інформація застаріла. Представники пошукової системи Google зазначали, що керуються принципом нейтральності мережі Інтернет та відкритості інформації, що не передбачає контролю контенту. Однак Суд вказав, що діяльність пошукової системи з пошуку, зберігання та надання інформації через мережу Інтернету є обробкою даних в контексті Директиви 95/46/ЕС про захист персональних даних, а компанія, що використовує пошукову систему, відповідальна за таку обробку та зобов'язана контролювати процес обробки даних та забезпечувати суб'єктам персональних даних реалізацію всіх передбачених Директивою прав, зокрема і права на забуття. Суд дійшов висновку, що у цій справі захист персональних даних важливіший, ніж мережева нейтральність, та зобов'язав Google видалити відповідну інформацію.

Починаючи з 2013 року ООН прийняла дві резолюції з питань приватного життя під назвою «право на приватність у цифрову еру». Ці резолюції були ухвалені у відповідь на розвиток нових технологій та оприлюднення фактів масового спостереження в певних державах. У резолюціях засуджується масове спостереження і наголошується на його можливому впливі на такі засадничі права, як приватне життя та свобода вираження поглядів, а також на функціонування динамічного демократичного суспільства. Хоча резолюції не є юридично обов'язковими, вони дали поштовх важливій міжнародній дискусії високого рівня щодо приватності, нових технологій та спостереження. Вони також привели до запровадження посади Спеціального доповідача щодо права на приватне життя з повноваженнями щодо популяризації та захисту цього права. Його конкретним завданням є збір інформації про підходи та досвід різних країн у питаннях приватності та про виклики, пов'язані з новими технологіями, обмін та популяризація найкращим досвідом, а також визначення потенційних перешкод.

Як зазначає дослідник Солове Д., окрему проблему становлять сучасні агресивні стратегії збору персональної інформації. Основною умовою доступу до продуктів та сервісів з використанням програмного забезпечення є згода із запропонованими правилами користування, яка досить часто є засобом отримання персональних даних користувача. Безкоштовне користування певними послугами та цифровими продуктами фактично надається в обмін на доступ до персональних даних. Можлива загроза конфіденційності користувача та негативні наслідки, які можуть виникнути в зв'язку з цим у майбутньому, розробники програмного забезпечення намагаються компенсувати перевагами свого продукту, такими як до-

ступ до важливої інформації, активну соціальну взаємодію, новими прогресивними технологіями тощо [6, с. 44].

Оцінка загроз недоторканості приватного життя стає ще складнішим завданням у світлі розвитку алгоритмів штучного інтелекту та машинного навчання. Інформація використовується все більш несподіваними способами, абсолютно всупереч очікуванням осіб, які її надають. Вже очевидно, що навіть обмежений обсяг персональних даних, що вводиться в алгоритми штучного інтелекту, розкриває іншу інформацію про особу, поширювати яку вона не мала жодного наміру. Передбачити обсяг інформації, яка може бути розкрита таким чином, не можуть навіть фахівці.

М. Фрумкін запропонував термін «міопія розуміння конфіденційності» (privacy myopia) для позначення системної нездатності людини коректно оцінити загрози збереження своїх персональних даних. Для звичайної людини неможливо залишатися обізнаною про зростаючі можливості використання інформації, яка на перший погляд не викликає занепокоєння. Навіть якщо уявити, що довгострокові наслідки розкриття інформації пізнаються, занадто дорого розігрувати всі можливі сценарії того, як дані можуть бути використані в майбутньому [7, с. 1465].

У науці широкого розповсюдження набуває підхід, згідно якого персональні дані набувають економічної оцінки. Так, В. Багнолі виступає за введення у науковий обіг поняття «релевантний ринок великих даних». На думку автора, персональні дані стають джерелом нематеріальних благ з метою створення об'єктів, які мають вартісне вираження на рівні з авторськими правами, патентами, діловою репутацією тощо. Таким чином, організації, які збирають персональну інформацію, можуть претендувати на захист авторських прав щодо форм даних баз даних. У свою чергу, споживачі електронних сервісів зберігають авторські права на оригінальні публікації, фотографії та відео, які розміщують на онлайн-сервісах [22, с. 80–82].

Однак варто зазначити, що такий підхід має певні застороги, адже встановити механізм формування вартісного вираження персональних даних надзвичайно складно. Більш того, при такому підході наслідком може стати повна декларативність права на недоторканність приватного життя, яке стане виключно предметом торгу. Конфіденційність має соціальний вимір, тому її не можна використовувати як об'єкт ринкових відносин.

В цьому аспекті Д. Солове вказує на ряд найважливіших, на його думку, причин соціальної цінності права на приватність: обмеження втручання влади, повага до особистості, встановлення соціальних бар'єрів, свобода думки та вираження поглядів, свобода соціальної та політичної активності. Право на приватність та недоторканність приватного життя має надзвичайно велике значення як конститутивний елемент вільного демократичного суспільства. Конфігурація відносин конфіденційності має важливе інструментальне значення у досягненні і суспільних, і індивідуальних цілей. Правове регулювання не може будуватись на тому, наскільки охоче люди «торгують» своїми персональними даними [6, с. 35].

Підсумовуючи, варто відзначити, що захист конфіденційності в цифрову епоху стає дедалі складнішим. Люди щодня публікують персональні дані (власні та своїх друзів і знайомих) через соціальні мережі та інтернет-сервіси. Методи збору та обробки даних швидко змінюються. Швидкий технологічний розвиток істотно збільшив обсяг і масштаб збору та обміну персональними даними. Це призвело до необхідності змінити спосіб захисту даних, оскільки старі методи не відповідають новим реаліям.

Оскільки більшість дій людей залишає за собою певний слід цифрових даних, контролювати поведінку таких осіб стало дедалі простіше. Часто люди не розуміють, як легко використовувати їх особисті дані в злочинних чи комерційних цілях. Про таку можливість використання персональних даних не говориться на момент їх збирання. Економічна цінність персональних даних постійно зростає, що робить персональні дані наріжним каменем для різних бізнес-моделей як онлайн, так і офлайн.

Крім того, міждержавні потоки даних значно зросли, і для забезпечення стабільного функціонування Європейського Союзу було визнано необхідним на законодавчому рівні врегулювати співпрацю між державами щодо обміну персональними даними з метою її уніфікації, адже до цього існували значні відмінності в правилах щодо захисту персональних даних у різних державах-членах Європейського Союзу.

ВИСНОВКИ

Можливості для захисту персональних даних змінились з приходом цифрової епохи. Умови цифрової епохи прискорили розповсюдження інформації в глобальній системі та додали до цієї системи більш широкі рівні можливостей. Завдяки поступовій еволюції цифрових мереж і сервісів з кожним роком збільшується кількість цифрової інформації і даних, яка зберігається на цифрових платформах.

Однією з найбільш суттєвих проблем цифрової епохи стає захист персональних даних. Дані, збережені на цифрових платформах, стають потенційною мішенню шахраїв та злочинців, легко втрачаються, з ними досить складно оперувати пересічному користувачу. У сфері, пов'язаній з використанням персональних даних, відмічається зростання злочинів та правопорушень. Задля можливого усунення порушень у цій сфері та захисту персональних даних постійно оновлюється законодавство та правила, спрямовані на забезпечення безпечного зберігання цифрових даних. Законодавство, зокрема, встановлює механізми захисту від несанкціонованого доступу, використання та відновлення даних осіб.

Основою для забезпечення безпеки персональних даних є належним чином законодавчо врегульовані процеси та технології, призначені для підтримки та спостереження за роботою цифрових систем та даних. Цифрові технології безпеки, такі як ідентифікація, авторизація користувачів, аутентифікація протоколів, шиф-

рування і контроль доступу, дають фізичні засоби захисту даних. Але не менш важливим для забезпечення захисту персональних даних є дотримання правил та методик безпечного використання цифрових технологій. Процес встановлення компетентних та модернізованих механізмів захисту даних допоможе поліпшити безпеку цифрових ресурсів та захистити персональні дані всіх користувачів.

Оскільки поняття приватного цифрового життя людини поступово розширюється, це стало справжнім викликом для людства, адже, з одного боку, таке право зазнає порушень та неправомірних втручань, а з іншого – важко піддається технологічному та юридичному контролю. Таким чином, методи контролю та захисту ускладнюються відповідно, адже відсутність адекватних законодавчих положень щодо захисту від втручання у приватне життя ставить під загрозу майбутнє приватного електронного життя особи, не дозволяє належним чином реагувати на порушення у цій сфері та притягувати до відповідальності порушників.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

[1] The right to privacy in the digital age: report of the United Nations High Commissioner for Human Rights (A/HRC/39/29) 3 August 2018. URL: https:// https://documents-dds-ny.un.org/doc/UNDOC/GEN/G18/239/58/PDF/G1823958.pdf?OpenElement (дата звернення: 06.12.2022)

[2] Баранов О. А. Правове забезпечення інформаційної сфери: теорія, методологія і практика : монографія. Київ : Едельвейс, 2014. 434 с.

[3] Брижко В. М. Захист персональних даних: реалії та практика сучасності. *Інформація і право*. 2013. № 3(9). С. 31–48.

[4] Рогова О. Г. Захист персональних даних у законодавстві Європейського Союзу та України. *Теорія та практика державного управління* : зб. наук. праць. Харків : Вид-во ХарРІ НАДУ «Магістр», 2011. Вип. 3 (34). 512 с.

[5] Nissenbaum H. Protecting Privacy in an Information Age: The Problem of Privacy in Public. *Law and Philosophy*. URL: https://nissenbaum.tech.cornell.edu/papers/privacy.pdf (дата звернення: 06.01.2023)

[6] Solove D. The Myth of the Privacy Paradox. *The George Washington law review*. Washington. 2021. Vol. 89. N. 1. 51 p.

[7] Froomkin M. The Death of Privacy? *Stanford Law Review*. 2000. Vol. 52. № 5. P. 1461–1543.

[8] Про інформацію : Закон України від 02.10.1992 № 2657-XII. URL: https://zakon.rada.gov.ua/laws/show/2657–12#Text (дата звернення: 22.01.2023)

[9] Про доступ до публічної інформації : Закон України від 13.01.2011 № 2939-VI. URL: https://zakon.rada.gov.ua/laws/show/2939–17#Text (дата звернення: 23.01.2023)

[10] Про захист персональних даних : Закон України від 01.06.2010 № 2297-VI. URL: https://zakon.rada.gov.ua/laws/show/2297–17#Text (дата звернення: 22.01.2023)

[11] Загальна декларація прав людини ООН від 10.12.1948. URL: http://zakon1.rada.gov.ua/cgi-bin/laws/main.cgi?nreg=995_015 (дата звернення: 15.01.2023)

[12] Конвенція про захист прав людини і основоположних свобод. URL: http://zakon4.rada.gov.ua/laws/show/995_004 (дата звернення: 18.01.2023)

[13] Конвенція про захист осіб у зв'язку з автоматизованою обробкою персональних даних від 28.01.1981. URL: http://zakon4.rada.gov.ua/laws/show/994_326 (дата звернення: 18.01.2023)
[14] Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (CETS № 223). URL: https://rm.coe.int/16808ac918 (дата звернення: 19.01.2023)
[15] Директива 95/46/ЄС Європейського парламенту і Ради про захист осіб у зв'язку з обробкою персональних даних і вільним обігом цих даних від 24.10.1995. URL: https://zakon.rada.gov.ua/laws/show/994_242 (дата звернення: 20.01.2023)
[16] Регламент Ради ЄС 2016/679 про захист фізичних осіб щодо обробки персональних даних та про вільний рух таких даних, а також про скасування Директиви 95/46/ЕС (Загальний регламент захисту даних) від 27.04.2016. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN (дата звернення: 23.01.2023)
[17] Конституція України : Закон України від 28.06.1996 № 254к/96-ВР. *Відомості Верховної Ради України.* 1996. № 30. Ст. 141.
[18] Проект Закону України № 6177 від 18 жовтня 2021 року «Про Національну комісію з питань захисту персональних даних та доступу до публічної інформації». URL: http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=72992 (дата звернення: 23.01.2023)
[19] Аналіз проєкту Закону України «Про Національну комісію з питань захисту персональних даних та доступу до публічної інформації» № 6177. Українська Гельсінська спілка з прав людини. URL: https://www.helsinki.org.ua/articles/analiz-proiektu-zakonu-ukrainy-pro-natsionalnu-komisiiu-z-pytan-zakhystu-personalnykh-danykh-ta-dostupu-do-publichnoi-informatsii-6177/ (дата звернення: 18.01.2023)
[20] Як ЄСПЛ захищає «цифрові» права людини в Інтернеті. Практика ЄСПЛ. Український аспект. URL: https://www.echr.com.ua/yak-yespl-zaxishhaye-cifrovi-prava-lyudini-v-interneti/ (дата звернення: 15.12.2022)
[21] Google Spain SL, Google Inc.v. Agencia Española de Protección de Datos (AEPD), Mario Costeja González. Judgment of the Court (Grand Chamber) of 13 May 2014. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:62012CJ0131&from=EN (дата звернення: 15.12.2022)
[22] Bagnoli V. The big data relevant market. *Concorrenza e mercato*. Rome, 2016. P. 73–94.

REFERENCES

[1] The right to privacy in the digital age : report of the United Nations High Commissioner for Human Rights (A/HRC/39/29). (2018, August). Retrieved from: https://documents-dds-ny.un.org/doc/UNDOC/GEN/G18/239/58/PDF/G1823958.pdf?OpenElement.
[2] Baranov, O. A. (2014). *Legal support of the information sphere: theory, methodology and practice: monograph*. Kiev: Edelweiss.
[3] Bryzhko, V. M. (2013). Protection of personal data: realities and modern practice. *Information and law*, 3(9), 31–48.
[4] Rogova, O. G. (2011). Protection of personal data in the legislation of the European Union and Ukraine. *Theory and practice of public administration*, 3(34). 512.

[5] Nissenbaum, H. Protecting Privacy in an Information Age: The Problem of Privacy in Public (2000, September). Retrieved from: https://nissenbaum.tech.cornell.edu/papers/privacy.pdf.
[6] Solove, D. (2021). The Myth of the Privacy Paradox. *The George Washington law review,* 89, 1, 51.
[7] Froomkin, M. (2000). The Death of Privacy? *Stanford Law Review*. 52, 5. 1461–1543
[8] On Information: Law of Ukraine. (1992, October). Retrieved from https://zakon.rada.gov.ua/laws/show/2657–12#Text
[9] On Access to Public Information: Law of Ukraine. (2011, January). Retrieved from https://zakon.rada.gov.ua/laws/show/2939–17#Text
[10] On Protection of Personal Data: Law of Ukraine. (2010, June). Retrieved from https://zakon.rada.gov.ua/laws/show/2297–17#Text
[11] UN Universal Declaration of Human Rights. (1948, December). Retrieved from http://zakon1.rada.gov.ua/cgi-bin/laws/main.cgi?nreg=995_015
[12] Convention on the Protection of Human Rights and Fundamental Freedoms. (1950, November). Retrieved from http://zakon4.rada.gov.ua/laws/show/995_004.
[13] Convention on the Protection of Individuals in Connection with Automated Processing of Personal Data. (1981, January). Retrieved from http://zakon4.rada.gov.ua/laws/show/994_326
[14] Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (CETS No. 223). (2018, October). Retrieved from https://rm.coe.int/16808ac918
[15] On the protection of individuals in connection with the processing of personal data and the free circulation of this data. Directive 95/46/EC of the European Parliament and the Council. (1995, October). Retrieved from https://zakon.rada.gov.ua/laws/show/994_242
[16] EU Council Regulation 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, as well as on the repeal of Directive 95/46/EC (General Data Protection Regulation). (2016, April). Retrieved from: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN
[17] Constitution of Ukraine: Law of Ukraine. (1996, June). *Information of the Verkhovna Rada of Ukraine*. 1996. №. 30. Art. 141.
[18] On the National Commission for the Protection of Personal Data and Access to Public Information: Draft Law of Ukraine (2021, October). Retrieved from http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=72992
[19] Analysis of the draft Law of Ukraine «On the National Commission on Personal Data Protection and Access to Public Information» No. 6177. Ukrainian Helsinki Human Rights Union. (2021, November). Retrieved from https://www.helsinki.org.ua/articles/analiz-proiektu-zakonu-ukrainy-pro-natsionalnu-komisiiu-z-pytan-zakhystu-personalnykh-danykh-ta-dostupu-do-publichnoi-informatsii-6177/
[20] How the ECtHR protects «digital» human rights on the Internet. Practice of the ECtHR. Ukrainian aspect. (2021, May). Retrieved from https://www.echr.com.ua/yak-yespl-zaxishhaye-cifrovi-prava-lyudini-v-interneti/
[21] Google Spain SL, Google Inc. v. Agencia Española de Protección de Datos (AEPD), Mario Costeja González. (2014, May). Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:62012CJ0131&from=EN
[22] Bagnoli, V. (2016). The big data relevant market. *Concorrenza e mercato*, 23, 73–94.

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 міжнародного приватного права і порівняльного правознавства
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 Private International and Comparative Law
Yaroslav Mudryi National Law University
61024, 77 Pushkinska Str., Kharkiv, Ukraine

Рекомендоване цитування: Гиляка О. С. Право на приватність та захист персональних даних в умовах цифровізації. *Вісник Національної академії правових наук України*. 2023. Т. 30. № 1. С. 15–30.

Suggested Citation: Hyliaka, O. S. (2023). Right to privacy and protection personal data in digitalization conditions. *Journal of the National Academy of Legal Sciences of Ukraine,* 30(1), 15–30.

Стаття надійшла / Submitted: 10/02/2023
Доопрацьовано / Revised: 10/03/2023
Схвалено до друку / Accepted: 24/03/2023