УДК 340.11:330.341.1
DOI https://doi.org/10.32782/chern.v5.2023.19

М. О. Мельник
кандидатка юридичних наук,
старша викладачка кафедри загальнотеоретичного правознавства
та публічного права
Національного університету «Києво-Могилянська академія»
orcid.org/0009-0003-5932-021X

ГЛОБАЛЬНА ДІДЖИТАЛІЗАЦІЯ І ЗБЕРЕЖЕННЯ ОСОБИСТИХ КОРДОНІВ ЛЮДИНИ: ФОРМАЛІЗМ ПРОТИ РЕАЛІЗМУ

Стаття присвячена аналізу важливих питань сьогодення – впливу глобальної діджиталізації на особисті кордони та конфіденційну інформацію людини. У сучасному світі, насиченому технологіями, зростає збір та опрацювання даних, що порушує питання щодо захисту особистості та її персональних даних.

Стаття розглядає ключові аспекти глобальної діджиталізації, включаючи розширення електронних послуг та торгівлі, безпеку даних та прозорість використання персональної інформації. Окрім того, в статті досліджується розуміння змісту права на приватність у розрізі міжнародно-правових актів. Аналізується визначення елементів, що можуть бути кваліфікуючими при розумінні заподіяної шкоди приватності.

Окрема увага приділена маніпуляціям цифрового ринку за рахунок використання отриманих цифровими гігантами персональних даних на прикладі аналізу політики про конфіденційність. Досліджуючи ці питання, стаття пропонує розглянути виклики, що постають перед юриспруденцією для запровадження дієвих механізмів захисту особистих кордонів людини у цифрову еру та визначає шляхи досягнення балансу між технологічними інноваціями та забезпеченням приватності та безпеки персональних даних. У статті досліджуються регуляторні акти Європейського Союзу та Сполучених Штатів Америки, зокрема Регламент ЄС 2016/679 від 27 квітня 2016 року про захист фізичних осіб у зв'язку з опрацюванням персональних даних і про вільний рух таких даних, та про скасування Директиви 95/46/ЄС (Загальний регламент про захист даних, General Data Protection Regulation), Регламент ЄС 2022/2065 від 19 жовтня 2022 року про єдиний ринок цифрових послуг і внесення змін до Директиви 2000/31/ЕС (Акт про цифрові послуги, Digital Service Act) та Закон штату Каліфорнія про захист персональних даних споживачів (California Consumer Privacy Act, CCPA) від 2018 року, що були прийняті для захисту персональних кордонів людини в той час, коли швидкість розвитку цифрових інновацій є надзвичайно високою, але потреба у захисті загальнолюдських цінностей, які формувалися тисячоліттями, лишається.

У статті запропоновані механізми, що сприяють посиленню захисту персональних даних в еру розвитку технологічного світу, в розрізі формування юридичної практики через усвідомлене розуміння, насамперед, суспільством особистих кордонів, які не можуть порушувати гравці цифрового простору.

Ключові слова: цифрові технології, приватність, юридичне регулювання, захист персональних даних, юридична практика.

Melnyk. M. O. **GLOBAL DIGITALIZATION AND PRESERVATION OF PERSONAL BOUNDARIES: FORMALISM VERSUS REALISM**

The article is dedicated to analyzing a crucial challenge of our time – the impact of global digitalization on personal boundaries and the confidentiality of individual information. In a contemporary world saturated with technology, the escalating collection and processing of data raise questions about the protection of personal identity.

The article delves into key aspects of global digitalization, including the expansion of electronic services and commerce, data security, and transparency in the use of personal information. Additionally, it explores the interpretation of the right to privacy within the context of international legal acts. The analysis scrutinizes the definition of elements that may qualify as indicators when understanding the inflicted harm to privacy.

Particular attention is devoted to manipulations of the digital market through the utilization of personal data acquired by digital giants, illustrated by an analysis of privacy policies. In addressing these issues, the article offers insights into the challenges faced by jurisprudence in implementing effective mechanisms to safeguard individual boundaries in the digital era, outlining paths to strike a balance between technological innovations and ensuring the privacy and security of personal data. The article investigates international regulatory acts, notably the Regulation (EU) 2016/679 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 (General Data Protection Regulation), the Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act), and the California Consumer Privacy Act (CCPA) of 2018. These acts were enacted to protect personal boundaries at a time when the pace of digital innovation is exceptionally high, emphasizing the need to safeguard enduring human values that have evolved over millennia.

The article proposes mechanisms that can contribute to strengthening the protection of personal data in the era of technological advancement. It emphasizes the formation of legal practices through society's conscious understanding of personal boundaries that digital players cannot transgress.

Key words: digital technologies, privacy, legal regulation, personal data protection, legal practice.

© М. О. Мельник, 2023

Постановка проблеми. В сучасних реаліях розвитку людства технологічний прогрес посідає надзвичайно важливе місце. Розвиток цифрового простору став частиною щоденного життя значної частини людства: миттєвий доступ до будь-якої інформації в мережі Інтернет, доступність здійснення розрахунків завдяки цифровим технологіям, створення контенту за допомогою штучного інтелекту. Ця частина людського життя зазнала вкрай швидкого розвитку. З одного боку, цифрові інновації привносять великі можливості для розвитку, ефективності та комунікації, а з іншого – породжують низку серйозних юридичних викликів, пов'язаних з захистом права на приватність [1, с. 11–12], безпекою та іншими аспектами.

Нині захист персональних даних – одна з ключових тем сучасного суспільства. У світі, де технології розвиваються стрімко, приватність перетворюється у важливий аспект для багатьох.

Актуальність питання полягає в тому, чи встигає право, як основний регулятор суспільних відносин, встановлювати межі захисту приватних кордонів людського життя. У розрізі аналізу цієї статті автор проаналізує стандарти Європейського Союзу та Сполучених Штатів Америки, які спрямовані на захист персональних даних людини, а саме – правові акти у сфері захисту персональних даних: Регламент ЄС 2016/679 про захист фізичних осіб у зв'язку з опрацюванням персональних даних і про вільний рух таких даних, та скасування Директиви 95/46/ЄС, Закон штату Каліфорнія про захист персональних даних споживачів від 2018. Окрім того, буде проаналізовано Регламент ЄС 2022/2065 від 19 жовтня 2022 року про єдиний ринок цифрових послуг і внесення змін до Директиви 2000/31/ЕС від 19 жовтня 2022 року щодо визначення механізмів, спрямованих на захист персональних даних людини.

Збереження персональних даних в умовах стрімко зростаючої цифровізації стає завданням не лише для правників, але й для самого суспільства, яке шукає раціональний баланс між технологічними досягненнями та особистою свободою.

Аналіз останніх досліджень і публікацій. Оскільки визначена проблематика – нова для суспільства в цілому, наукова думка і юридична практика, як вітчизняна так і міжнародна, знаходяться на межі власного формування. Дослідженню питання розвитку цифрових технологій та кореляції їх з персональними даними людини присвячені публікації таких західних та європейських вчених, як: С. Вахтер (S. Wachter), Е. Голдман (E. Goldman), Д. Джонсон (D. Johnson), Л. Детерманн (L. Determann), Т.З. Зарський (T.Z. Zarsky), Р. Кало (R. Calo), Б. Міттельштадт (B. Mittelstadt) та Д. Пост (D. Post).

Окремим аспектам правового регулювання цифрових технологій власні дослідження присвятили наступні вітчизняні науковці: О.М. Вінник, О.А. Теличко, Є. Мічурін, В.А. Рекун. Міжнародні стандарти захисту персональної інформації особистості аналізували у своїх дослідженнях науковці: К. Врублевська-Місюна, О.В. Гронь, І.О. Кульчій, А.К. Погореленко, І.М. Сопілко, В. Тичина.

Метою дослідження є аналіз сучасних надбань юридичної науки і практики у створенні механізмів захисту особистих кордонів людини у час глобальної діджиталізації процесів, які супроводжують різноманітні сфери людського буття.

Виклад основного матеріалу. Свого часу, коли комунікація людей за допомогою комп'ютерних технологій лише зароджувалася, науковці з певною обережністю зазначали, що нові технології перетинають територіальні кордони, формуючи нову сферу людської діяльності, відокремлюючи віртуальний світ від «реального світу атомів». Ще тоді, аналізуючи витоки розвитку, науковці вбачали різницю між реальним емпіричним світом, який можливо пізнавати за допомогою органів чуття, та цифровим світом, вказуючи на необхідність створити законодавство, яке вирізнятиметься від того, що регулює фізично і географічно визначений простір [2, с. 1367].

Коли мережа Інтернет тільки набирала популярності, суспільство умовно розділилося на два табори. Одні наголошували на незалежності кіберпростору, а інші вимагали нових законів, які б його регулювали [3, с. 11].

Серед вітчизняних науковців зустрічається позиція, відповідно до якої цифровий світ потребує побудови відповідної моделі правового регулювання, яка б відповідала запитам нової технологічної реальності [4, с. 209].

В теорії юридичної думки існує концепція шкоди заподіяної приватності [5, с. 1027–1031]. Як часто користувач мережі Інтернет замислюється щодо перетину його приватних кордонів під час простого огляду онлайн-магазинів, бронювання житла чи авіаквитків за допомогою мережі? Насправді, це риторичне питання, оскільки використання мережі Інтернет сьогодні настільки невід'ємна частина життя людини, що багато дій здійснюється автоматично без належного осмислення, з метою збереження часу. Разом з тим, аби привернути увагу до важливості цього питання, у щоденному житті, розглянемо приклад, який свого часу навів у публікації американський правник Раян Кало.

Уявімо звичайні дії будь-якого користувача з пошуку товару для покупки на сайті Amazon. Користувач зацікавлений у здійсненні купівлі бажаного товару, він спостерігає за цінами протягом певного часу, повторно заходить на сторінку, переглядає інші товари і через деякий час вартість товару зростає, разом з тим користувач навіть не усвідомлює, що зростання вартості пов'язане

з його активністю з відвідування сторінки цифрового гіганта, оскільки сам факт відвідування сторінки користувачем зберігається на сервері [5, с. 1027–1028]. З метою легітимності таких дій торгівельного майданчика, варто було б проаналізувати політку конфіденційності, розміщену на сайті. В розділі «Яку особисту інформацію про клієнтів збирає Amazon?» можна ознайомитися з наступним: «ми автоматично збираємо та зберігаємо певні типи інформації про використання вами послуг Amazon, включаючи інформацію про вашу взаємодію з *продуктами, вмістом і послугами, доступними через сервіси Amazon*. Як і багато вебсайтів, ми використовуємо файли cookie та інші унікальні ідентифікатори, а також отримуємо певні типи інформації, коли ваш браузер або пристрій отримує доступ до сервісів Amazon та іншого вмісту, який надається Amazon або від імені майданчику на інших вебсайтах» [6].

У цьому розрізі цікаву думку висловлює американський правник щодо того, що у сфері цифрового ринку, коли маємо справу з маніпуляціями, споживач не завжди може знати, чи є ціна, яку йому пропонують, аналогічною тій, яку запропоновано іншій особі. Так само, як і використання іншого браузеру або покупка товару в інший день, може вплинути на зниження ціни товару чи послуги [5, с. 1029].

Питання збереження персональних даних комплексне і часом надзвичайно складно зрозуміти чи була дійсно порушена межа приватності. Здебільшого *порушення конфіденційності* призводить до негативних наслідків [5, с. 1028].

Інші західні науковці наголошують, що аналітика великих даних (big data) та штучний інтелект сприяють генерації висновків і прогнозів щодо поведінки, вподобань та приватного життя людей, які не мають своїм джерелом походження інтуїцію та внутрішню зацікавленість. Методи вивідної аналітики використовуються для визначення вподобань користувачів, думок (наприклад, політичних переконань) або для прогнозування поведінки (наприклад, для розміщення реклами). Ці методи можуть використовуватися для впливу на вибір, який робить людина [7, с. 497].

Право на повагу до приватного життя є фундаментальним правом людини, захист якого встановлений на рівні Європейської конвенції з прав людини [8].

Разом з тим, більшість конституцій і міжнародних угод про права людини прямо не визначають зміст права на приватне життя [3, с. 1].

Статтею 32 Конституції України передбачено, 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 [9].

Серед різних позицій науковців існує думка, що захист даних є лише одним із компонентів права на приватність, яке також включає право на ідентичність, репутацію, самоусвідомлення та незалежність [7, с. 615].

Разом з тим, вітчизняна наукова думка підтримує позицію про те, що невтручання в особисте життя є однією з головних цілей в процесі збору, зберігання та опрацювання персональних даних [10, с. 105].

27 квітня 2016 року Європейським Парламентом та Радою Європейського Союзу було прийнято Регламент ЄС 2016/679 про захист фізичних осіб у зв'язку з опрацюванням персональних даних і про вільний рух таких даних, та про скасування Директиви 95/46/ЄС (Загальний регламент щодо захисту даних, General Data Protection Regulation), загальновідомий за абревіатурою GDPR, що почав застосовуватися з 25 травня 2018 року [11].

GDPR став документом, який змусив всіх представників бізнесу в цифровому просторі щонайменше переглянути свою політику конфіденційності та перебудувати архітектуру вебресурсів, аби брати згоду користувачів на збір та опрацювання їх персональних даних, перелік якої має бути позначений в тій самій політиці.

Регламент побудований на повазі основоположного права людини, визнаного однією з найважливіших цінностей усім цивілізованим суспільством, а саме – захист приватного життя.

GDPR встановлює кілька основних принципів щодо опрацювання персональних даних. Ці принципи включають прозорість, законність, обмеження цілей та точність даних. Організації, які опрацьовують персональні дані, повинні відповідати цим принципам, щоб забезпечити адекватний рівень захисту [11].

З цієї точки зору цікаво проаналізувати, що ж в себе включає визначення персональних даних, яке охороняється регламентом. Під персональними даними регламент розуміє будь-яку інформацію щодо ідентифікованої (identified) або фізичної особи, яку можливо ідентифікувати (identifiable) («суб'єкта даних»); фізична особа, яку можливо ідентифікувати, – це особа, яку можна ідентифікувати прямо чи опосередковано, зокрема за ідентифікатором, таким як ім'я, ідентифікаційний номер, дані про місцезнаходження, онлайн-ідентифікатор або за одним чи кількома факторами, характерними для фізичної, фізіологічної, генетичної, розумової, економічної, культурної чи соціальної ідентичності цієї фізичної особи [11].

Цікаво проаналізувати нормативне регулювання захисту приватної інформації в Сполучених Штатах Америки, де в червня 2018 році був

прийняти Закон штату Каліфорнія про захист персональних даних споживачів (California Consumer Privacy Act, CCPA) – це законодавчий акт, прийнятий в штаті Каліфорнія, США, що регулює збір та опрацювання персональної інформації від споживачів [12].

Визначення персональних даних відповідно до CCPA (1798.140. v. 1) включає широкий спектр даних, які можуть ідентифікувати конкретну особу. Ось ключові аспекти того, що вважається персональними даними за CCPA: 1. ідентифікуючі інформаційні елементи (ім'я та прізвище: включає власне ім'я, прізвище, псевдонім споживача; адреса: фізична або електронна адреса, що ідентифікує особу; ідентифікуючі дані: включають соціальний страховий номер, номер водійського посвідчення, номер паспорту та інші ідентифікуючі дані); 2. комерційна інформація, включає записи про особисте майно, продукти чи послуги, придбані, отримані чи такі, що розглядалися для придбання, або іншу історію купівлі чи споживання чи зацікавленості; 3. фінансові дані: інформація про банківські рахунки, кредитні картки та інші фінансові деталі; 4. медична інформація: включає дані про стан здоров'я та медичні записи; 5. дані про локалізацію: інформація про місцезнаходження особи; 6. інші дані, які можуть ідентифікувати особу: біометричні дані; 7. *Інтернет-активність: історія перегляду та пошуку в Інтернеті, файли cookie, IP-адреса;* 8. професійні та освітні дані: інформація про роботу, освіту та інші профільні дані; 9. поведінкові дані та інша інформація: *інтереси та попередні замовлення, дані про власні інтереси, покупки та інші взаємодії з продуктами та послугами.* 10. інші особисті дані: які відображають ідентичність: включають зображення, відеозаписи та інші матеріали, які можуть ідентифікувати особу [12].

Ці категорії персональної інформації визначають широкий спектр даних, за якими організації повинні дотримуватися правил та обов'язків CCPA, забезпечуючи захист персональних даних споживачів [12].

Повертаючись до нормативного регулювання цифрового простору в Європейському Союзі, потрібно враховувати нові регуляторні документи, а саме: Акт про цифрові послуги (Digital Service Act, DSA) [13], прийнятий 19 жовтня 2022 року та Акт про цифрові ринки (Digital Markets Act, DMA) [14], прийнятий 14 вересня 2022 року.

У тексті DSA регулятор зазначає, що цифрова трансформація та збільшення використання цифрових послуг призвели до нових ризиків і викликів для окремих одержувачів відповідних послуг, компаній і суспільства в цілому. Зокрема в статті 46 DSA передбачена можливість створення Кодексу поведінки для онлайн реклами. Codes of Conduct (Кодекси поведінки) в контексті DSA це документи, які визначають стандарти та правила для онлайн-платформ та інших відповідних постачальників послуг, таких як постачальників посередницьких послуг у сфері онлайн-реклами, інших учасників ланцюжка створення вартості онлайн-реклами, в Європейському Союзі (ЄС). Ці Кодекси поведінки повинні сприяти ефективній передачі інформації, яка повністю поважає права та інтереси всіх залучених сторін, а також конкурентному, прозорому та справедливому середовищу в онлайн-рекламі, відповідно до законодавства Європейського Союзу та національного законодавства, зокрема про конкуренцію та *захист приватного життя і персональних даних* [13].

Резюмуючи наведений аналіз регуляторних актів у сфері захисту права на приватне життя та недоторканість приватної інформації, можна дійти висновку, що право, як основний регулятор суспільних відносин прагне до створення механізмів захисту наведених основоположних прав людини, але залишається питання щодо того чи встигає воно за розвитком технологічного процесу.

Розмірковуючи над цим запитанням, пригадується школа правового реалізму, яка виникла в двадцятому сторіччі на американському континенті, в пошуках механізмів і інструментів для подолання формалізм у процесі розгляді судових справ [15, с. 278–279]. Формалізм у регулюванні цифрового простору полягає в тому, що є юридичні акти, які надають формальну визначеність механізмам захисту приватного життя та персональних даних користувачів цифрових послуг, а реалізм проявляється в тому, що здебільшого політика конфіденційності Інтернет-ресурсів передбачає, що фактом використання відповідного вебсайту чи замовленням певної послуги, користувач приймає умови політики конфіденційності. До прикладу, у своєму Повідомлені про конфіденційність Amazon.com зазначає, що, користуючись послугами Amazon, інтернет-користувачі погоджується з положеннями, описаними в цьому Повідомленні про конфіденційність. Фактично користувач, відвідуючи сайт Amazon, надає згоду на те, аби останній мав змогу збирати персональну інформацію в момент, коли покупець шукає або купує продукти чи послуги в інтернет-магазині, додає або видаляє товар із кошика, розміщує замовлення або використовує службу Amazon; завантажує, транслює, переглядає або використовує вміст на пристрої або через службу чи програму на пристрої. Окрім того, в своїй політиці Amazon зазначає, що використовує персональну інформацію користувачів, щоб рекомендувати функції, продукти та послуги, які можуть його/її зацікавити, визначити вподобання та персоналізувати досвід роботи зі службами Amazon. У секторі реклами, цифровий гігант також наводить положення про те, що вико-

ристовує персональну інформацію користувачів, щоб показувати рекламу на основі інтересів останніх щодо функцій, продуктів і послуг, які можуть їх зацікавити [6].

Наукова юридична думка теж підкреслює, що рекламодавцям потрібна інформація відстеження для націлювання реклами відповідно до попередніх інтересів користувачів [3, с. 7].

Чи створює такий порядок використання цифрових технологій механізм задля формування і відповідним чином впливу на наступні інтереси користувачів, після того як була отримана персональна інформація, питання складне, яке вимагає від права розробки реальних механізмів захисту приватного життя та персональних даних, особливо у сфері діяльності цифрових гігантів.

Якщо ж говорити про шкоду, нанесену приватності, однією з її ознак можна визначити – використання отриманої інформації від користувача, аби вплинути на вибір особи, що ставить її у більш невигідне становище (приклад: удорожчання ціни, продаж товару чи послуги за рахунок постійної таргетної реклами) у порівнянні до можливих дій особи без вчинення впливу на неї в цифровому просторі з використанням зібраної персональної інформації [5, с. 1030].

Інший практичний аспект, який викликає чимало питань – це використання файлів cookies. Пунктом 30 преамбули GDPR передбачено, що фізичні особи можуть бути пов'язані з онлайн-ідентифікаторами, наданими їхніми пристроями, додатками, інструментами та протоколами, такими як адреси інтернет-протоколів, ідентифікатори файлів cookie або інші ідентифікатори, такі як радіочастотні ідентифікаційні мітки. Право бути проінформованим є базовим в розрізі регулювання збору та опрацювання персональних даних і закріплюється статтею 13 та 14 GDPR [11].

Своєю чергою, стаття 6 GDPR визначає підстави законності опрацювання даних, якщо це не підпадає під категорію необхідного опрацювання з підстав, визначених текстом регламенту, то вона може здійснюватися лише у випадках, *якщо суб'єкт даних надав згоду на опрацювання своїх персональних даних для однієї або декількох конкретних цілей*. Пунктом 32 преамбули GDPR визначається, *що згода повинна бути надана чітким підтверджуючим актом, який встановлює вільно надану, конкретно поінформовану та недвозначну вказівку на згоду суб'єкта даних на опрацювання персональних даних*, що стосуються його чи її, наприклад, письмовою заявою, у тому числі за допомогою електронних засобів або усної заяви. Це може включати проставлення відмітки під час відвідування вебсайту в Інтернеті, вибір технічних налаштувань для послуг інформаційного суспільства або іншу заяву чи поведінку, які чітко вказують у цьому контексті на згоду суб'єкта даних із запропонованим опрацюванням його чи її персональних даних. Таким чином, мовчання, автоматичне заповнення клітинок позначками або бездіяльність, відповідно, не становлять надання згоди. Згода має охоплювати всі дії з опрацювання даних, що здійснюються з тією самою метою або цілями. Пункт 39 преамбули визначає, що будь-яке опрацювання персональних даних має бути законним та правомірним. Фізичним особам має бути зрозуміло, що їхні персональні дані збираються, використовуються або опрацьовуються в інший спосіб, а також в якому обсязі ці дані опрацьовуються або будуть опрацьовуватися. Принцип прозорості вимагає, щоб будь-яка інформація та повідомлення, пов'язані з опрацюванням цих персональних даних, були легкодоступними та зрозумілими, а також щоб використовувалася чіткі та прості формулювання [11].

Перейдемо до практичного аспекту реалізації вищенаведених положень. Найімовірніше, що кожен читач цієї публікації має справу з переглядом різноманітних вебсторінок, в яких спливають віконця з запитом прийняти cookies. Часто архітектура сайту вибудована таким чином, що перейти до змісту сторінки неможливо без прийняття cookies. Ба більше, доволі часто трапляються віконця з запитом на прийняття файлів cookies, які не містять опцію прийняття лише необхідних cookies або кнопки прийняття вже налаштовані на надання згоди, де потрібно не надавати згоду, а фактично її забирати. Інший не менш цікавий аспект – це розмір і доступність для сприйняття тексту до ознайомлення, які містять політику збирання і опрацювання персональних даних та політику поводження з файлами cookies. Окрім того, в епоху швидкості, яка спричинена розвитком цифрових технологій, і практика пошукових навиків користувачів в мережі Інтернет, аби знайти інформацію, придбати товари, послуги, переказати кошти є настільки швидкою, що залишає питання, чи дійсно користувачі об'єктивно мають можливість ознайомлюватися з значним обсягом і змістом текстів, які розміщуються на вебресурсах і без погодження з якими жодна дія не буде можливою. Абсолютно справедливо буде у всіх вищенаведених випадках поставити під питання надання вільної згоди користувачами на опрацювання своїх персональних даних.

В цьому розрізі доречно пригадати глибинну думку професора Козюбри М.І. про те, що пізнання людьми своєї природи впливає на формування уявлення про права та межі їх захисту [16, с. 8]. Очевидно, суспільству потрібен ще час на дослідження природи своїх прав у сфері захисту приватного життя та особистих кордонів в кореляції із розвитком цифрових технологій.

Висновки. У світі, де цифрові технології стають неодмінною частиною повсякденного життя люди-

ни, важливо розглядати їхній вплив на збереження особистих кордонів. У праці простежується розвиток цифрового світу та його вплив на індивідуальну приватність. З розширенням обсягу збору та опрацювання персональних даних зростає загроза порушення особистих кордонів. Сучасні технології, такі як Інтернет-ресурси, штучний інтелект, розрахунки за допомогою цифрових технологій вимагають розвитку юридичної науки і практики у сфері захисту приватних кордонів особистості. Баланс між технологічними інноваціями та збереженням приватності є ключовим викликом сьогодення. На вагах, з одного боку, розвиток технологій, які сприяють розвитку суспільства, на іншому – перетин кордону приватного життя особистості шляхом отримання та використання персональних даних, що впливає на несвідомий вибір людини.

На рівні практичних інструментів потрібна розробка реальних механізмів політики збору та опрацювання персональних даних особи, яка повинна надаватися усвідомленою і зрозумілою для користувача згодою. Разом з тим, цифрова реальність вимагає не лише вдосконалення правових механізмів захисту персональних даних, але й активної участі суспільства в обговоренні та формуванні позиції щодо цих питань. Це може включати в себе проведення освітніх заходів, публічних обговорень та заохочення ініціатив, спрямованих на захист конфіденційності та особистих кордонів у цифрову еру.

Література

1. Булавіна С., Давидова Т. Право на приватність у системі поколінь прав людини. *Історико-правовий часопис*. 2018. № 1. С. 10–14.

2. Johnson D. R., Post D. Law and Borders – The Rise of Law in Cyberspace. *Stanford Law Review*. 1996. Vol. 48. P. 1367–1402.

3. Determann L. Social Media Privacy: A Dozen Myths and Facts. *Stanford Technology Law Review*. 2012. Vol. 7. P. 1–14. URL: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2298891

4. Теличко О. А., Рекун В.А. Розвиток правової системи у цифрову епоху. *Юридичний науковий електронний журнал*. № 1/2022. С. 209–212.

5. Calo R. Digital Market Manipulation. *The George Washington Law Review*. 2014. Vol. 82:995. P. 995–1051.

6. Amazon.com Privacy Notice. URL: https://www.amazon.com/gp/help/customer/display.html?nodeId=GX7NJQ4ZB8MHFRNJ

7. Wachter S., Mittelstadt B. A right to reasonable inferences: re-thinking data protection law in the age of Big Data and AI. *Columbia Business Law Review*. Vol. 2019 – Issue 2. P. 494–620.

8. Конвенція про захист прав людини і основоположних свобод (з протоколами) (Європейська конвенція з прав людини). URL: https://zakon.rada.gov.ua/laws/show/995_004#Text

9. Конституція України // Відомості Верховної Ради. 1996. No 30. 141 с. URL: https://zakon.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80#Text

10. Гронь О.В., Погореленко А.К. Проблеми захисту персональних даних у контексті сучасної комунікації. *Науковий вісник Ужгородського національного університету*. 2018. Випуск 19, частина 1. С. 102–108.

11. 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 (General Data Protect ion Regulation). URL: https://eur-lex.europa.eu/eli/reg/2016/679/oj

12. California Consumer Privacy Act (CCPA) of 2018. URL: https://cppa.ca.gov/regulations/pdf/cppa_act.pdf

13. Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act). URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex-%3A32022R2065

14. Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act) (Text with EEA relevance). URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32022R1925

15. Brown R. B., Kimball B. A. When Holmes Borrowed from Langdell: The 'Ultra Legal' Formalism and Public Policy of Northern Securities (1904). *The American Journal of Legal History*. 2001. Vol. 45, No. 3. P. 278–321.

16. Козюбра М. І. Право і людина: лінії взаємозв'язків та тенденції розвитку. *Наукові записки НаУКМА*. 2015. Т. 168, *Юридичні науки*. С. 3–9.