УДК 347.2/3

Гуйван П. Д.,
кандидат юридичних наук,
заслужений юрист України, докторант
Національного юридичного університету імені Ярослава Мудрого

ЮРИДИЧНЕ РЕГУЛЮВАННЯ ЕЛЕКТРОННОЇ ОБРОБКИ ПЕРСОНАЛЬНИХ ДАНИХ

LEGAL REGULATION OF ELECTRONIC PROCESSING OF PERSONAL DATA

Праця присвячена проблематиці правового регулювання обороту персональних даних під час їх автоматизованої обробки. Досліджено реальний стан взаємовідносин користувача веб-ресурсами та оператора, визначені категорії найпоширеніших порушень прав людини при цьому. Проаналізовано зміст та дієвість відповідних міжнародних та національних актів у цій сфері. Надані конкретні рекомендації щодо подальшого вдосконалення українського законодавства.
Ключові слова: *електронна обробка персональних даних, веб-ресурси.*

Работа посвящена проблематике правового регулирования оборота персональных данных при их автоматизированной обработке. Исследовано реальное состояние взаимоотношений пользователя веб-ресурсами и оператора, определены категории распространенных нарушений прав человека при этом. Проанализировано содержание и действенность соответствующих международных и национальных актов в этой сфере. Даны конкретные рекомендации по дальнейшему совершенствованию украинского законодательства.
Ключевые слова: *электронная обработка персональных данных, веб-ресурсы.*

The work is devoted to the problems of legal regulation of the turnover of personal data during their automated processing. The real state of the relationship between the user of web resources and the operator was investigated, and categories of widespread human rights violations were identified. The content and effectiveness of the relevant international and national acts in this sphere are analyzed. Specific recommendations for further improvement of Ukrainian legislation are given.
Key words: *electronic processing of personal data, web resources.*

У сучасних умовах розвитку суспільних відносин велике значення має зростання обсягу інформаційних відносин. У межах національного, міждержавного та світового обміну даними задіюються невичерпні ресурси, які зумовлені останніми досягненнями у сфері інформаційних та телекомунікаційних технологій. Це надає досить широкі можливості для продукування, споживання та поширення ресурсів у глобальному інформаційному просторі. З іншого боку, зростають загрози порушення конкретних прав особи, яка є суб'єктом конкретних відомостей, ризики неконтрольованого розміщення, незаконного ознайомлення та використання інформації. Особливо це стосується конфіденційних даних про особу, які в доктрині та законодавстві набули визначення як персональні дані.

Значно поширилися як можливості обробки, так і ризики правопорушень у цій царині внаслідок стрімкого розвитку комп'ютерних електронних систем, зокрема мережі Інтернет. У цьому контексті всі країни, що входять до демократичної спільноти і які активно використовують інформаційний мережевий ресурс, мусять ефективно вирішувати питання нормативного врегулювання інформаційних відносин, які постійно виникають на все новому технічному та організаційному рівні. Однією з головних проблем, що потребує досить серйозної уваги не лише науковців, а й законодавця, є серйозність загроз основоположним правам людини на приватність у площині збору, обробки, поширення особистої інформації за допомогою використання електронних систем. Ці питання залишаються актуальними як для локальних комп'ютерних мереж, так і для подібної діяльності у глобальних мережах. Вони часто мають досить резонансні прояви в публічному житті. Адже йдеться про втручання через мережу Інтернет у всьому світі як у приватне життя людей, так і в діяльність державних органів і організацій через систему несанкціонованого доступу до приватної інформації про особу. Так, наприклад, політики в США намагаються отримати від найбільшого пошукача Google додаткові гарантії того, що компанія робить максимально можливі кроки для захисту особистої інформації її користувачів та інших людей. Члени американського конгресу звернулися до Google із листом із проханням уточнити деякі питання, пов'язані із захистом персональних даних під час використання нової технології розумних окулярів Google Glass, оскільки використання останніх ускладнює і не дає гарантій захисту персональних даних [1, с. 71].

Дане питання викликає занепокоєність усіх структур, покликаних забезпечувати демократичність, чесність та гуманність обробки персональних даних. Так, у документі Європейського Парламенту та Ради – Регламенті (ЄС) 2016/679 від 27 квітня 2016 року про захист фізичних осіб стосовно обробки персональних даних та щодо вільного переміщення таких даних та скасування Директиви 95/46 / ЄС (Загальні положення про захист даних), вказується, що стрімкий технологічний розвиток і глобалізація призводять до виникнення нових труднощів для захисту персональних даних. Масштаби збирання та спільного використання персональних даних суттєво зросли. Технології дозволяють як приватним

компаніям, так і публічним органам користуватися персональними даними в безпрецедентних масштабах із метою реалізації своєї діяльності. Фізичні особи дедалі частіше надають доступ до персональної інформації для громадськості та в глобальному масштабі. Технології змінили як економіку, так і суспільне життя і повинні надалі стимулювати вільний рух персональних даних у межах Союзу та передавання їх до третіх країн і міжнародних організацій, забезпечуючи при цьому високий рівень захисту персональних даних. Такі зміни вимагають наявності міцних та більш узгоджених засад щодо захисту даних у Союзі із запровадженням належного механізму виконання, беручи до уваги важливість формування довіри, що дозволить розвиток цифрової економіки на рівні внутрішнього ринку. Фізичні особи повинні мати контроль щодо власних персональних даних. Необхідно зміцнити правову та практичну визначеність для фізичних осіб, суб'єктів господарювання й органів публічної влади [2, п. 6-7].

Запровадження подібних виважених підходів у правовому полі не лише держав-членів Європейського Союзу, а й інших, що прагнуть дотримуватися демократичних критеріїв (у тому числі України), безумовно, зможе допомогти створити механізми, що забезпечать захист особистих відомостей від випадкового чи незаконного доступу, витоку персональної інформації, її знищення, блокування зміни та поширення. Слід також усвідомлювати, що регулювання відокремленої групи розглянутих суспільних відносин досягається за допомогою цілого комплексу різних за юридичною силою правових норм. Крім цього, загальне законодавство має бути деталізоване та конкретизоване на рівні спеціальних актів, що охоплюють режими здійснення відносин у конкретному напрямку. Фактично повинен встановитися пріоритет спеціальних правових норм, закріплених нормативними правовими актами, які покликані забезпечити оборот окремих видів інформації обмеженого доступу перед загальними нормами [3, с. 232]. Відтак суспільні відносини, пов'язані з обігом персональних даних, як одна із груп інформаційних правовідносин мають отримати не тільки детальне правове опосередкування кожного етапу обробки з урахуванням особливостей предмету – інформації з обмеженим доступом, що призначена для ідентифікації фізичних осіб (персональні дані), але ще й бути врегульованими з урахуванням специфіки такої обробки засобами комп'ютерних технологій.

Проблематика стосовно викликів, які з'являються під час автоматизованої обробки персональних даних та правового врегулювання інформаційних відносин, розглядалася в юридичній літературі. Зокрема, можемо згадати праці таких науковців, як: В. Брижко, О. Солодка, А. Чернобай, В. Козак, С. Воррен, М. Рижков, В. Цимбалюк, І. Вельдер, Є. Макаренко Р. Валєєв, А. Пазюк, А. Тунік, Р. Гавісон, І. Гостєв. та ін. У той же час питання потребує додаткового дослідження. Це зумовлено тим, що невпинний розвиток комп'ютерних технологій вимагає повсякчасного адекватного реагування на новітні загрози приватності особи, передовсім у сфері несанкціонованого доступу та неправомірного використання її персональних даних. У цьому контексті має бути детальніше вивчений міжнародний нормотворчий та правозастосовний досвід, що дозволить конструювати національне законодавство у правильному напрямку. Отже, метою цієї статті є науковий аналіз та узагальнення змісту сучасних моделей гарантування інформаційної безпеки на українському національному та міжнародному рівнях. На цій основі та з урахуванням європейського досвіду будуть визначені проблемні питання щодо обробки даних в електронних системах, включаючи мережу Інтернет, та шляхи їхнього вирішення в українському правовому полі.

Відмінність сучасного етапу розвитку комунікаційної діяльності від попереднього полягає в тому, що за останні десятиріччя створено комунікаційний канал, який є принципово новим матеріально-технічним засобом її здійснення. Цей простір комп'ютерних комунікацій (кіберпростір, або віртуальна реальність) – це простір взаємодії, утворений глобальною мережею комп'ютерів, із яких складається Інтернет [4, с. 6–7]. Він передає повідомлення у фізичному просторі та астрономічному часі з небаченою швидкістю та легкістю, що дає змогу значно інтенсифікувати процес руху даних у суспільстві в національному та міжнародному масштабах. У цьому аспекті кіберпростір є засобом розширення можливостей інформаційного простору, ефективне використання якого стає сучасною парадигмою суспільного розвитку [5, с. 26].

З огляду на об'єктивне існування глобального інформаційного простору зусилля науковців, законодавців та правозастосовних інституцій мають бути спрямовані на забезпечення ефективного та правомірного доступу до інформаційних ресурсів. Такий доступ, будучи спрямований на задоволення особистих потреб шляхом організації інформаційної взаємодії суб'єктів, все ж мусить знаходитися в тих межах, які дозволяють захистити інформацію конфіденційного характеру про людину від небажаного втручання. Для цього розробляються та застосовуються правові акти, що регулюють механізми забезпечення прав людини на охорону своїх приватно-правових інтересів (зокрема, персональних даних) з урахуванням дотримання балансу між ними та публічними суспільними інтересами щодо вільного отримання, розповсюдження і використання інформації як однієї з визначальних умов демократичного розвитку. Саме такі виважені та збалансовані юридичні інструменти сприяють належному унормуванню взаємовідносин конкретної людини з публічною владою. У сенсі врегулювання взаємин стосовно обороту конфіденційної інформації Радою Європи була прийнята Конвенція про захист осіб у зв'язку з автоматизованою обробкою персональних даних 28 січня 1981 року (ратифікована Україною у 2010 році). Цей документ має на меті запровадити однакові та обов'язкові правила поведінки країн шляхом визначення основних вимог до

обробки та передачі особистих відомостей про людину у всесвітньому електронному просторі.

Конвенція про захист осіб у зв'язку з автоматичною обробкою персональних даних визначає перелік певних вимог, яким мають відповідати дані, аби їх можна було кваліфікувати як персональні. Це, передовсім, будь-яка інформація, що відноситься до особи, яка ідентифікована або може бути ідентифікованою на основі цих відомостей. Основна увага щодо визначеності критеріїв прямої або непрямої ідентифікації (тобто потенціалу інформації, яка дозволяє ідентифікувати особу) має приділятися їх здатності охопити велику кількість даних, які мають пряме чи непряме відношення до конкретної людини. Відтак дані можуть бути «особистими», навіть якщо вони дозволяють ідентифікувати особу лише в поєднанні з іншими (допоміжними) даними. Персональні дані повинні збиратися справедливо і законно, що означає наявність правових підстав для збору та сумлінність цієї діяльності. Відомості не мають використовуватися для цілей, не сумісних із тими, для яких були зібрані, вони повинні збиратися відповідно до легітимної мети, бути повними, але не надмірними з точки зору тих цілей, для яких вони накопичуються, і зберігатися не довше, ніж цього вимагає мета їх використання (ст. 5 Конвенції).

На практиці спостерігаємо: як значна кількість персональних даних обробляється володільцями з використанням управляючих елементів веб-ресурсів у мережі Інтернет у межах процесів заповнення відвідувачами анкет; реєстрацію та отримання логіна та пароля; реєстрацію з використанням облікового запису соціальної мережі; надання електронної адреси відвідувача для зворотного зв'язку. При цьому можуть оброблятися персональні дані надзвичайно широкого діапазону: від анкетних персональних даних, які одночасно є відомостями про особу, яка ідентифікована, до відомостей, які можуть стосуватися особи опосередковано або які можуть використовуватися у процесі ідентифікації особи: відомостей про оплату послуг із використанням платіжних карт, логіни та паролі, записи в соціальній мережі, номери телефонів, електронні адреси тощо [6, с. 79].

На збір інформації про користувача послугами Інтернету впливає і техніко-організаційний аспект. Наприклад, суб'єкт господарювання, що працює як Інтернет-магазин MD, може продати безліч товарів та послуг (наприклад, харчові продукти, квитки на проїзд та інше). Якщо в покупця є контакт із MD також стосовно цих та інших товарів і послуг, MD буде в кінцевому підсумку мати інформацію про особисті вподобання покупця чи веб-переглядача. Одночасно одноразові операції з продажу або «відвідування магазину», ймовірно, включатимуть реєстрацію дещо меншої кількості даних про покупця чи браузера, ніж у випадку із частими або регулярними операціями за певною формою підписки на послуги. Також слід ураховувати, що кількість даних браузера, зареєстрованих MD, залежить, зокрема, від того, в якій мірі сервер використовує механізми автоматичного реєстрації таких, скажімо, даних, як «cookie». Отримані в такий спосіб дані в поєднанні з іншими, наявними в компанії, дають змогу дійти висновку щодо інших даних, таких як: – країна, в якій мешкає Інтернет-користувач; – домен Інтернету, до якого він належить; – сфера діяльності компанії, в якій працює Інтернет-користувач; – обіг та розмір компанії-роботодавця; – функція та посада користувача в компанії; – постачальник доступу до Інтернету; – типологія веб-сайтів, що відвідуються сьогодні [7, с. 23]. Таким чином, на даний час взагалі неможливо відвідати Інтернет-сервер без автоматичного виявлення програмного забезпечення браузера через певні дані на сервері. Ці дані, як правило, є ідентифікацією мережі (ім'я вузла та IP адреса) машини браузера, URL-адреси останньої сторінки, яку відвідував браузер раніше, що надходять на поточний сервер, і будь-яких файлів cookie, які зберігаються в браузері комп'ютера.

Отже, як бачимо, реєстрація та / або подальша обробка даних покупця та браузера в електронних мережевих системах може зазіхати на безліч інтересів суб'єктів даних. Найбільший важливі з них – приватність, автономія та цілісність. Кожне із цих понять є неоднозначним і часто використовується в різних тлумаченнях. У сучасних цілях поняття конфіденційності означає стан обмеженої доступності, що складається з трьох елементів: секретність – «тією мірою, якою ми відомі іншим»; самотність – «тією мірою, якою інші мають фізичний доступ до нас»; і анонімність – «тією мірою, до якої ми ставимось до уваги інших [8, p. 428–436]. Приватність тут не обмежена, щоб застосовувати лише ті аспекти життя людей, які вважається чутливим або інтимним. Концепція автономії означає самовизначення; тобто здатність людини жити його / її життям відповідно до його / її власних побажань (включаючи, звичайно, можливість використання товарів як він / вона вважає за потрібне). Тож самовизначення людини на інформаційну лінію має головне значення. Багато вчених визначають конфіденційність у плані здатності людини контролювати потік інформації про себе іншим; у цьому звіті таке інформаційне самовизначення розглядається як передумова і результат конфіденційності (тобто обмежена доступність). Що стосується поняття цілісності, то воно використовується тут, щоб позначити «стан людини цілісним», це гармонійна функціональність, заснована на повазі інших осіб [9, с. 42].

У контексті використання електронних систем конфіденційність покупця та веб-переглядача буде зменшена. Автономія даних у випадку простої реєстрації також зменшується, оскільки реєстрація відбувається без згоди особи чи навіть знання про це, або у зв'язку з тим, що реєстрація змушує їх вести себе уздовж ліній, визначених, у першу чергу, електронною системою. Це часто має негативний вплив, оскільки реєстрація або подальше використання даних не відповідає очікуванням про те, що є розумним. Наприклад, багато людей, ймовірно, розглядають приховану обробку даних про них іншими як цілісність-зловживання [10, с. 8]. Отже, дизайн

та функціонування електронних систем можуть зачіпати закони захисту даних під час їх обробки. Тож коли людина отримає відомості про те, що певні відомості, які стосуються її, були зареєстрованими, вона повинна хоча б неявно із цим погодитися. Таким чином, якщо сервер MD працює автоматично за допомогою механізму створення та встановлення файлів cookie під час першого доступу до сервера та файли cookie містять особисті дані, механізм знаходитиметься поза межами закону. При цьому, коли процесор або контролер обробляє дані покупця за параметрами, що принципово відрізняються від параметрів, про які покупець був спершу сповіщений і на які погодився (неявним або явним чином), обробка буде незаконною, якщо згода не буде надана заново. Неправомірною вважатиметься і обробка без повідомлення суб'єктів персональних даних про механізми автоматизованого збору відомостей, відвідування сайтів та поведінку відвідувачів в Інтернет, про законні підстави для обробки персональних даних тощо [11, с. 67].

В українському законодавстві питанням правового забезпечення електронної обробки персональних даних присвячено окремі норми в загальних актах. Так, у ст. 34 Закону України «Про телекомунікації» регламентовані питання захисту інформації про споживача. Зокрема, вказується, що призначені для оприлюднення телефонні довідники, в тому числі електронні версії та бази даних інформаційно-довідкових служб, можуть містити інформацію про прізвище, ім'я, по батькові, найменування, адресу та номер телефону абонента в разі, якщо в договорі про надання телекомунікаційних послуг міститься згода споживача на опублікування такої інформації. Під час автоматизованої обробки інформації про абонентів оператор телекомунікацій забезпечує її захист відповідно до закону. Споживач має право на безоплатне вилучення відомостей про нього повністю або частково з електронних версій баз даних інформаційно-довідкових служб. Інформація про споживача та про телекомунікаційні послуги, що він отримав, може надаватись у випадках і в порядку, визначених законом. В інших випадках зазначена інформація може поширюватися лише за наявності письмової згоди споживача. Також чотири невеликі рядки стосуються даної тематики в Угоді про асоціацію між Україною та Європейським Союзом, де у ст. 15 («Захист персональних даних») сказано таке: «Сторони домовились співробітничати з метою забезпечення належного рівня захисту персональних даних відповідно до найвищих європейських та міжнародних стандартів, зокрема відповідних документів Ради Європи. Співробітництво у сфері захисту персональних даних може включати, inter alia, обмін інформацією та експертами» [12]. Навряд чи вказані норми навіть із великим ступенем припущення можна кваліфікувати як регулятивні документи стосовно обробки та захисту персональних даних в електронних системах та мережах.

Як бачимо, національне законодавство взагалі не переймається питаннями регулятивного та охоронно-правового опосередкування відносин у досліджуваній царині, покладаючись на Бога. Між тим усе частіше спостерігаються такі типові порушення законодавства з питань захисту персональних даних під час обробки персональних даних із використанням веб-ресурсів, як неповідомлення на час збору персональних даних суб'єкта персональних даних про володільця персональних даних (найменування юридичної особи-володільця та її адресу), склад та зміст зібраних персональних даних, права, мету збору персональних даних та осіб, яким передаються його персональні дані; очевидна надмірність змісту персональних даних по відношенню до визначеної мети їхньої обробки; процедури обробки персональних даних визначені на сайті, але не визначені розпорядчими документами володільця, як це передбачено законодавством. За результатами проведеного в Україні дослідження встановлено, що понад 75% веб-сайтів національного сегменту Інтернет, за явних ознак обробки персональних даних, не надають користувачам жодних відомостей про найменування володільця персональних даних. Це свідчить про те, що відвідувачі сайтів не мають можливостей на захист свої персональних даних [6, с. 79].

Позаяк ми змушені констатувати практичну бездіяльність національної правової системи з питання впорядкування діяльності володільців та розпорядників (операторів) персональних даних в електронних мережах. Вважаємо за доцільне звернути прискіпливу увагу до міжнародних актів у цій сфері. До прикладу, механізми обробки та захисту персональних даних у мережі Інтернет детально визначені в Рекомендаціях № (99) Комітету Міністрів Ради Європи щодо захисту недоторканності приватного життя в Інтернеті, які, хоча і мають рекомендаційний характер, проте можуть враховуватись під час визначення загальних процедур діяльності з персональними даними в мережі Інтернет державами-членами Ради Європи (зокрема Україною). Вказаний документ встановлює керівні принципи щодо правил поведінки в мережі Інтернет користувачів та постачальників послуг Інтернету. Вони були детально проаналізовані в одній із наших попередніх праць [13]. Нагадаємо лише, що серед рекомендацій користувачам слід виділити такі, як необхідність використовувати всі доступні засоби для захисту даних та ліній зв'язку, як, наприклад, легально доступні засоби шифрування для конфіденційності електронної пошти, коди доступу до власного персонального комп'ютера. Також необхідно повідомляти постачальникові послуг Інтернету тільки ті дані, які необхідні для виконання певних дій, про які суб'єкт заздалегідь поінформований. Особлива обережність необхідна під час використання кредитних карток і номерів рахунків, які в Інтернеті можуть легко стати об'єктом зловживань. Вказується, що анонімний доступ, хоча він і не може бути повним, в Інтернеті є найкращим захистом приватного життя. Для постачальників послуг Інтернету рекомендації передбачають необхідність використання конкретних процедур і доступних технологій, переважно сертифікованих, для забезпечення недо-

торканності приватного життя людини (навіть якщо вони не користувачі мережі Інтернет), особливо шляхом забезпечення цілісності і конфіденційності даних поряд із забезпеченням фізичної і логічної безпеки мережі і послуг, наданих у мережі.

Із проведеного дослідження можемо зробити окремі висновки. Важливою проблемою регулювання Інтернету в Україні є відсутність системного підходу держави до питання «цифрових прав» (визначення, комплексні механізми, процедури і правила). Питання доступу до мережі Інтернет, її використання, а тим паче обмеження (блокування і фільтрація) описуються уривками норм, що містяться в різних законодавчих актах. Існує очевидна потреба в напрацюванні механізмів обробки персональних даних із використанням веб-ресурсів. Це стосується, зокрема, встановлення процедури повідомлення відвідувачів сайтів про їх права, про склад та зміст персональних даних, що збираються, про мету збору персональних даних та про осіб, яким передаються їхні персональні дані.

Діяльність особи в мережі Інтернет у контексті захисту персональних даних повинна бути вдосконалена як у розрізі дотримання прав суб'єктів, персональні дані яких обробляються в мережі Інтернет, так і щодо виконання володільцями та розпорядниками вимог законодавства у сфері захисту персональних даних. Серйозним недоліком є те, що в українській правовій системі правила, які стосуються обробки персональних даних, у тому числі в електронному форматі, так і залишаються порожніми деклараціями, які не мають дієвого характеру. До прикладу, вимога закону про те, що забезпечення захисту персональних даних від незаконного доступу, обробки (втрати, випадкового знищення) в базах даних покладається на їх володільця, жодним чином не забезпечена нормативним інструментарієм її практичної реалізації, тож вона не наповнена реальним змістом. Також, попри чіткі вимоги закону з приводу того, що суб'єкт персональних даних має повідомлятися про володільця персональних даних, склад та зміст зібраних персональних даних, прав такого суб'єкта, мету збирання персональних даних та осіб, яким передаються його персональні дані, стандартними є ситуації, коли суб'єкти персональних даних, які обробляються з використанням веб-ресурсів, не знають, хто відвідав їхній ресурс. Під час комп'ютерної обробки даних важливо, щоб зберігання інформації про приватне життя особи відбувалося впродовж лише необхідного строку, особливий характер таких відомостей вимагає, щоб після вирішення завдань, у зв'язку з якими вона збиралася, ця інформація була знищена і не могла бути використана в інших цілях усупереч інтересам відповідної особи.

ЛІТЕРАТУРА:

1. Сопілко І.М. Міжнародно-правовий досвід захисту персональних даних: напрямки вдосконалення для України. Юридичний вісник. 2014. № 4(33). С. 70–75.

2. Положення (ЄС) 2016/679 Європейського Парламенту та Ради від 27 квітня 2016 року про захист фізичних осіб стосовно обробки персональних даних та щодо вільного переміщення таких даних та скасування Директиви 95/46 / ЄС (Загальні положення про захист даних). Офіційний вісник Європейського Союзу. 04.05.2016. L 119/1. 98 с.

3. Бугель Н.В., Никулин А.В. Защита персональный данных как объект организационно-правового регулирования. Вестник Санкт-Петербургского университета МВД России. № 2(54). 2012. С. 230–233.

4. Global trends 2025: The National Intelligence Council's. 2025 Project. CreateSpace Independent Publishing Platform; 1 edition (November 15, 2008). 118 p.

5. Солодка О.М. Сучасні тенденції міжнародної політики забезпечення інформаційної безпеки. Інформаційна безпека людини, суспільства, держави. 2013. № 3(13). С. 25–29.

6. Русак Д.М., Березовська І.Р. Вдосконалення правового регулювання захисту персональних даних в мережі Інтернет в контексті інтеграції України в світовий інформаційний простір // Актуальні проблеми міжнародних відносин. 2015. Випуск 124 (частина ІІ). С. 74–84.

7. Марущак А.І., Мельник К.С. Особливості обробки та захисту персональних даних у мережі Інтернет: європейський досвід та законодавство України. Інформаційна безпека людини, суспільства, держави. 2013. № 3(13). С. 19–25.

8. Gavison R. (1980). Privacy and the limits of law. Yale Law Journal, 1980. № 89. P. 421–471.

9. Bygrave L.A. Data Protection Law: Approaching its Rationale, Logic and Limits. London: Kluwer Law International, 2002. 426 p.

10. Privacy, Data Protection and Copyright: Their Interaction in the Context of Electronic Copyright Management Systems. Institute for Information Law. Amsterdam. 1998. 83 p.

11. Козак В. Захист персональних даних та правила приватності при дослідженнях в Інтернет. Маркетинг в Україні. 2013. № 3(77). С. 49–70.

12. Угода про асоціацію між Україною, з однієї сторони, та Європейським Союзом, Європейським співтовариством з атомної енергії і їхніми державами-членами, з іншої сторонни. Міжнародний документ від 27.06.2014 року. URL: http://zakon3.rada.gov.ua/laws/show/984_011/page.

13. Гуйван П.Д. Окремі аспекти законодавства про захист персональних даних у Європейському Союзі // Вчені записки Таврійського національного університету імені В.І. Вернадського. Серія: Юридичні науки. Том 29(68). 2018. № 4.