

УДК 342.721

*МАРУЩАК Анатолій Іванович  
МЕЛЬНИК Костянтин Сергійович*

## **ОСОБЛИВОСТІ ОБРОБКИ ТА ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ У МЕРЕЖІ ІНТЕРНЕТ: ЄВРОПЕЙСЬКИЙ ДОСВІД ТА ЗАКОНОДАВСТВО УКРАЇНИ**

**Постановка проблеми.** Захист права на недоторканість приватного життя людини в контексті обробки її персональних даних (далі – ПД) є необхідним елементом людського життя і гуманного функціонування демократичного суспільства та фундаментальним правом людини, яке накладає на державу зобов'язання створити належну правову базу. У разі його порушення під загрозою опиняються людська гідність, свобода і безпека особи.

Такий захист важливий із погляду на значну кількість ПД, що обробляються володільцями ПД за допомогою управляючих елементів веб-ресурсів у мережі Інтернет. Найчастіше персональні дані із використанням веб-ресурсів обробляються у межах таких процесів, як: заповнення відвідувачами веб-ресурсів анкет; реєстрація та отримання логіна та пароля; реєстрація 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 з використанням платіжних карт, логіни та паролі, записи у соціальній мережі, номери телефонів, електронні адреси тощо.

Прагнучи відповідати європейським тенденціям захисту недоторканості приватного життя людини, Україна у 2010 році ратифі-

кувала базові європейські стандарти у сфері захисту персональних даних – Конвенцію Ради Європи про захист осіб у зв'язку з автоматизованою обробкою персональних даних та Додатковий протокол до неї щодо органів нагляду та транскордонних потоків даних [1-2]. У тому ж році прийнято Закон України № 2297-VI “Про захист персональних даних” [3], який спрямований на імплементацію згаданих вище стандартів та який втілює базові принципи захисту персональних даних в Європейському Союзі на основі Директиви Європейського Парламенту і Ради Європи № 95/46/ЄС про захист фізичних осіб при обробці персональних даних і про вільне переміщення таких даних [4]. Закон України “Про захист персональних даних” регулює правові відносини, пов'язані з захистом персональних даних при їх обробці, і спрямований на захист основоположних прав і свобод людини і громадянина, зокрема права на невтручання в особисте життя людини у зв'язку з обробкою персональних даних. Закон поширюється на діяльність із оброблення персональних даних, яке здійснюється повністю або частково із застосуванням автоматизованих засобів.

Діяльність особи в мережі Інтернет в контексті захисту персональних даних повинна розглядатись крізь призму двох складових: з одного боку, в розрізі дотримання прав суб'єктів, персональні дані яких обробляються у мережі Інтернет, з іншого – у розрізі виконання володільцями персональних даних вимог законодавства у сфері захисту персональних даних.

Необхідність комплексного дослідження питання особливостей обробки та захисту персональних даних у мережі Інтернет, визначення оптимальних шляхів його подальшого законодавчого врегулювання на основі європейського досвіду зумовлюють актуальність цього дослідження.

**Аналіз останніх досліджень і публікацій.** Наукові пошуки з питань оброблення та захисту персональних даних у мережі Інтернет знаходяться на початковій стадії свого розвитку. У вітчизняній юридичній літературі дослідженню окремих питань цієї проблематики у різні часи приділяли увагу такі фахівці, як О.Баранов, В.Брижко, А.Пазюк, А.Чернобай, А.Тунік, В.Цимбалюк, М.Швець та інші. Дослідження цього питання здійснюється і зарубіжними вченими Ф.Агре, Д.Беркін, Л.Брейдейс, С.Воррен, І.Вельдер, Р.Валеев, І.Гостев. Незважаючи на те, що порушеною проблематикою займалися багато науковців, деякі її аспекти сьогодні залишаються малодослідженими та дискусійними, особливо в контексті постійного становлення законодавства у сфері захисту персональних даних, захисту інформації в інформаційно-телекомунікаційних системах, телекомунікації тощо.

**Метою статті** є дослідження проблемних питань оброблення та захисту персональних даних у мережі Інтернет. Завдання статті: проаналізувати європейський та вітчизняний досвід регулювання питання обробки та захисту персональних даних у мережі Інтернет; визначити проблемні питання та шляхи подальшого розвитку законодавства України із цього питання на основі європейського досвіду.

**Виклад основного матеріалу.** Нормативно-правове визначення терміна “інтернет”, та інші пов’язані з ним терміни, містяться у Законі України “Про телекомунікації” від 18 листопада 2003 р. № 1280-IV (далі – Закон № 1280-IV). Цей Закон встановлює правову основу діяльності у сфері телекомунікацій. Він визначає повноваження держави щодо управління та регулювання цієї діяльності, а також права, обов’язки та засади відповіда-

льності фізичних і юридичних осіб, які беруть участь у такій діяльності або користуються телекомунікаційними послугами. Відповідно до статті 1 Закону № 1280-IV інтернет – всесвітня інформаційна система загального доступу, яка логічно пов’язана глобальним адресним простором та базується на інтернет-протоколі, визначеному міжнародними стандартами. У свою чергу, інформаційна система загального доступу визначається як сукупність телекомунікаційних мереж та засобів для накопичення, оброблення, зберігання та передавання даних [5].

Домен-частина ієрархічного адресного простору мережі Інтернет, яка має унікальну назву, що її ідентифікує, обслуговується групою серверів доменних імен та централізовано адмініструється. Веб-сайт – це сукупність веб-сторінок, доступних в інтернеті, які об’єднані як за змістом, так і навігаційно. Фізично веб-сайт може розміщуватися як на одному, так і на кількох серверах. Веб-сайтом також називають вузол мережі Інтернет, комп’ютер, за яким закріплена унікальна IP-адреса, і взагалі – будь-який об’єкт в інтернеті, за яким закріплена адреса, що ідентифікує його у мережі (FTP-site, WWW-site тощо). Веб-ресурс можна визначити як сукупність веб-сторінок в інтернеті, яка може бути ідентифікована, адресована і супроводжувана в мережевій інформаційній системі.

Загальні принципи оброблення персональних даних містяться у Конвенції Ради Європи про захист осіб у зв’язку з автоматизованою обробкою персональних даних та Законі України “Про захист персональних даних” від 1 червня 2010 р. № 2297-VI (далі – Закон № 2297-VI).

Так, на підприємства, установи й організації усіх форм власності, органи державної влади чи органи місцевого самоврядування, фізичних осіб – підприємців (володільців персональних даних), що обробляють персональні дані, з використанням веб-ресурсів у мережі Інтернет, поширюються такі положення законодавства, зокрема статті 6 Закону № 2297-VI:

1. Обробка персональних даних здійснюється відкрито і прозоро. Обробка персона-

льних даних здійснюється для конкретних і законних цілей, визначених за згодою суб'єкта персональних даних, або у випадках, передбачених законами України, у порядку встановленому законодавством.

2. Мета обробки персональних даних має бути сформульована у документах, які регулюють діяльність володільця персональних даних, та відповідати законодавству про захист персональних даних.

3. Склад та зміст персональних даних мають бути відповідними, адекватними та ненадмірними стосовно визначеної мети їх оброблення.

4. Персональні дані мають бути точними, достовірними та оновлюватися у міру потреби, визначеної метою їх оброблення. Обробка персональних даних здійснюється із застосуванням засобів та у спосіб, що відповідають цілям такої обробки. У разі, якщо нова мета обробки персональних даних є несумісною з попередньою, суб'єктом персональних даних має бути надана згода на обробку його персональних даних відповідно до зміненої мети.

5. Персональні дані повинні оброблятися у строк, не більший ніж це необхідно відповідно до їх законного призначення.

Відповідно до статті 8 Закону № 2297-VI суб'єкт персональних даних має такі права:

- знати назву, місцезнаходження та/або місце проживання (перебування) володільця персональних даних;
- отримувати інформацію про третіх осіб, яким передаються його персональні дані;
- знати механізм автоматичної обробки персональних даних;
- висувати вмотивовану вимогу щодо зміни або знищення своїх персональних даних будь-яким володільцем та розпорядником персональних даних, якщо ці дані обробляються незаконно чи є недостовірними;
- відкликати згоду на обробку своїх персональних даних.

У момент збирання персональних даних суб'єкт персональних даних *повідомляється про володільця персональних даних, склад та зміст зібраних персональних даних, права*

*такого суб'єкта, визначені цим Законом, мету збирання персональних даних та осіб, яким передаються його персональні дані* (стаття 12 Закону № 2297-VI).

*Забезпечення захисту персональних даних у базах персональних даних покладається на володільця персональних даних.* Суб'єкти відносин, пов'язаних із персональними даними, зобов'язані забезпечити захист цих даних від незаконної обробки, зокрема від втрати, незаконного або випадкового знищення, а також від незаконного доступу до них (стаття 24 Закону № 2297-VI).

З огляду на питання захисту персональних даних у мережі Інтернет важливо врахувати керівні принципи викладені в Рекомендації № (99) Комітету Міністрів Ради Європи щодо захисту недоторканості приватного життя в інтернеті, які мають рекомендаційний характер, проте можуть враховуватись при визначенні загальних процедур обробки персональних даних у мережі Інтернет державами-членами Ради Європи (зокрема Україною) [6].

Такі керівні принципи містять рекомендації користувачам щодо правил поведінки у мережі Інтернет та постачальникам послуг інтернету. Так, серед рекомендацій користувачам слід виокремити такі:

– необхідно 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;

– будь-яка транзакція, будь-яке відвідування сайту залишає в інтернеті так звані “сліди”. Подібні “електронні сліди” можуть бути використані без відома суб'єкта персональних даних для створення профілю про нього і його інтересів. Варто використовувати новітні технічні досягнення, що дозволяють проінформувати суб'єкта персональних даних про будь-який випадок можливості залишення відповідних “слідів”, і дають йому змогу відмовитися від подальших дій;

– найкращий спосіб забезпечення недоторканості приватного життя – це анонім-

ний доступ і анонімне використання послуг, анонімні засоби здійснення платежів. По можливості слід з'ясувати наявність технічних засобів для забезпечення анонімності. Повна анонімність не завжди можлива через певні законодавчі обмеження. У такому випадку, якщо це дозволено законодавством, варто використовувати псевдонім, що дозволить знати персональні дані суб'єкта тільки постачальникові послуг інтернету;

– необхідно повідомляти постачальникові послуг інтернету чи будь-кому іншому тільки ті дані, які необхідні для виконання певних дій, про які суб'єкт заздалегідь поінформований. Особлива обережність необхідна при використанні кредитних карток і номерів рахунків, які в інтернеті можуть легко стати об'єктом зловживань;

– необхідно з обережністю ставитись до сайтів, де просять інформацію особистого характеру більшу, ніж це потрібно для доступу чи здійснення трансакції, чи не пишуть для чого така інформація необхідна взагалі.

Для постачальників послуг інтернету рекомендації полягають у тому, що:

– необхідність використання процедур і доступних технологій, переважно сертифікованих, для забезпечення недоторканності 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;

– необхідність попереднього інформування користувачів при їхній підписці на послуги чи початком обслуговування про ризики недоторканності приватного життя при використанні інтернету;

– необхідність інформування користувача про технічні засоби, що він/вона можуть використовувати на законній підставі для зниження ризику порушення безпеки персональних даних і їхньої передачі, наприклад, про дозволені засоби шифрування і цифрового підпису;

– вжиття заходів із метою недопущення будь-якого зовнішнього втручання у зміст

переданих даних, якщо тільки це не передбачено законом і не здійснюється державними органами;

– збирання, оброблення і зберігання персональних даних користувачів дозволяється тільки тоді, коли це необхідно для зрозумілих, точно визначених і законних цілей;

– передача персональних даних можлива лише за наявних, законодавчо визначених підстав, або згоди суб'єкта персональних даних;

– зберігання персональних даних повинно відбуватися не довше, ніж це необхідно для цілей їх оброблення;

– не повинні використовуватися персональні дані для власної рекламної чи маркетингової діяльності, якщо поінформований про наміри такого використання користувач заперечує проти цього, або якщо, у випадку обробки переданих чи спеціальних категорій даних, він/вона не дав чіткої згоди;

– перед передачею персональних даних в іншу країну необхідно подати запит до, наприклад, компетентних органів власної країни щодо законності такої передачі. Слід наголосити приймаючій стороні щодо вжиття усіх необхідних заходів для захисту персональних даних.

Вимоги Закону України “Про захист персональних даних” та застосування його положень при обробці персональних даних із використанням веб-ресурсів у мережі Інтернет загалом кореспондуються із зазначеними рекомендаціями Комітету Міністрів Ради Європи, а також рекомендаціями Робочої групи, що функціонує відповідно до статті 29 Директиви 95/46/ЄС (далі – РГ 29) [7], та рекомендаціями Міжнародної робочої групи з питань захисту персональних даних в телекомунікаційній сфері (Берлінська група) [8].

Рекомендації РГ 29 є важливими в контексті детального дослідження питань *відстежування поведінки відвідувачів веб-ресурсів (web-tracking) та захисту приватного життя людини*.

Так, згідно з аналізом проведеного європейськими експертами для відстежування особливостей поведінки відвідувачів веб-ресурсів використовуються такі технології, як:

– надсилання до пристрою користувача файлів “cookies” першої та “cookies” третьої сторони;

– збирання в базах веб-ресурсів детальної інформації протягом тривалого часу про відвідані сторінки, вибрані режими, натиснуті клавіші тощо, та її подальше оброблення;

– збирання у базах веб-ресурсів інформації про апаратні та програмні засоби, які встановлено у користувача, тощо.

У рекомендаціях РГ 29 наводиться підтверджуючий приклад. Файл “cookie” зберігається на жорсткому диску користувача і містить інформацію про фізичну особу. Цю інформацію може прочитати веб-сайт, який розмістив файл, або будь-хто інший, хто має уявлення про формат даних цього веб-сайту. Файл “cookie” може містити будь-яку інформацію, яку веб-сайт бажає включити в нього: переглянуті сторінки, натиснуті рекламні оголошення, ідентифікаційний номер користувача тощо. У деяких випадках вони можуть бути корисними для надання послуги в інтернеті або для полегшення перегляду сторінок інтернет-користувачем. Наприклад, деякі веб-сайти використовують cookie, щоб ідентифікувати користувачів кожного разу, коли вони знову відвідують сайт, щоб користувачам не доводилося вводити своє ім'я кожного разу, коли вони перевіряють свої новини.

Поєднавши дані браузера і так звані “невидимі” гіперпосилання, наприклад, маркетингова компанія може за замовчуванням знати про всі ключові слова, введені конкретним інтернет-користувачем у пошукових системах, в яких така компанія розміщує рекламу, а також все про його комп'ютер, операційну систему, тип браузера, IP-адресу інтернет-користувача, час та тривалість HTTP-сесій. Ці вихідні дані дають змогу у поєднанні з іншими даними, наявними у компанії, 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.

Файли “cookie” дають змогу здійснювати систематичну відправку постійних та унікальних ідентифікаторів при кожному інформаційному запиті, оскільки IP-адреса залишається відносно слабким ідентифікатором, адже може бути прихована за допомогою проксі-серверів, і є ненадійною через свій динамічний характер у випадку з користувачами, які виходять в інтернет через модем. Так маркетингова компанія може проводити непомітне складання профілів.

Питання відстежування поведінки відвідувачів веб-ресурсів (web-tracking) та захисту приватного життя людини потребує детального аналізу в Україні з подальшими рекомендаціями щодо їх законодавчого та практичного вирішення. З огляду на це дуже корисними можуть бути ініціативи громадських організацій та проведені ними ґрунтовні дослідження, подібні до досліджень європейських експертів.

Слід зазначити, що перші кроки щодо залучення громадськості до дослідження питання захисту персональних даних у мережі Інтернет вже зроблені. У лютому 2013 року Всеукраїнська громадська організація “Українська асоціація захисту персональних даних” провела громадський моніторинг із тематики: “Забезпечення прозорості та відкритості обробки персональних даних на веб-ресурсах” [9]. А в жовтні 2012 року за ініціативи цієї громадської організації було прийнято Декларацію “За недоторканість приватного життя в Інтернеті”, до якої приєдналась низка провідних національних телекомунікаційних компаній [10].

Важливим також є питання удосконалення законодавства у частині обробки та захисту персональних даних у мережі Інтернет. Загальні питання оброблення та захисту персональних даних, зокрема у мережі Інтернет, урегульовані рамковим Законом

№ 2297-VI. На законодавчому рівні врегульовані окремі питання надання телекомунікаційних послуг із дотриманням вимог законодавства про захист персональних даних. Так, частиною другою статті 32 Закону № 1280-IV передбачається, що абонент, який отримує телекомунікаційні послуги без укладення договору в письмовій формі, може зареєструватися в оператора, надавши йому персональні дані відповідно до закону, у порядку, встановленому національною комісією, що здійснює державне регулювання у сфері зв'язку та інформатизації. У статті 34 Закону № 1280-IV регламентовані питання захисту інформації про споживача. Статтею 54 цього Закону регулюється питання адміністрування адресного простору українського сегмента мережі Інтернет.

Отже, питання обробки та захисту персональних даних у мережі Інтернет у контексті визначення чіткого механізму дотримання прав суб'єктів персональних даних та визначення обов'язків володільців персональних даних потребує подальшого правового врегулювання. На думку авторів, доцільно опрацювати це питання в органах державної влади, а також провести широке громадське обговорення із залученням провідних наукових фахівців у цій галузі, зокрема щодо внесення необхідних змін до законів України “Про інформацію” та “Про захист інформації в інформаційно-телекомунікаційних системах”, інших галузевих законів, що прямо чи опосередковано регулюють питання обробки та захисту персональних даних у мережі Інтернет.

### **Список використаних джерел**

1. Конвенція про захист осіб у зв'язку з автоматизованою обробкою персональних даних // Офіційний вісник України. – 2011. – № 1. – С. 701.
2. Додатковий протокол до Конвенції про захист осіб у зв'язку з автоматизованою обробкою персональних даних щодо органів нагляду та трансграничних потоків даних // Офіційний вісник України. – 2011. – № 1. – С. 708.
3. Закон України від 1 червня 2010 р. № 2297-VI “Про захист персональних даних” // Офіційний вісник України. – 2010. – № 49. – С. 199.

**Висновки.** З огляду на викладене доходимо таких висновків. Рамковий Закон України “Про захист персональних даних” визнає загальні вимоги до обробки та захисту персональних даних, зокрема у мережі Інтернет. Подальше внесення змін до законодавства у сфері інформаційної безпеки має відбуватися із урахуванням результатів комплексного дослідження цього питання в органах державної влади, а також проведення активного громадського обговорення із залученням провідних наукових фахівців у цій галузі.

Разом із цим, існує необхідність проведення широкої інформаційної кампанії з боку уповноваженого державного органу з питань захисту персональних даних (на сьогодні – Державної служби України з питань захисту персональних даних) щодо інформування як володільців персональних даних, так і суб'єктів персональних даних про їх права та обов'язки під час обробки персональних даних у мережі Інтернет, а також про механізми автоматизованого збору відомостей про поведінку відвідувачів у мережі Інтернет, про законні підстави для обробки персональних даних про відвідування веб-ресурсів, про необхідність повідомлення відвідувачів веб-ресурсів про механізми автоматизованої обробки персональних даних та про їх права. Важливим також вважаємо розроблення рекомендацій із боку уповноваженого державного органу з питань захисту персональних даних із питань обробки та захисту персональних даних у мережі Інтернет на основі рекомендацій європейських інституцій.

4. Директива Європейського Парламенту і Ради № 95/46/ЄС про захист фізичних осіб при обробці персональних даних і про вільне переміщення таких даних [Електронний ресурс]. – Режим доступу : [http://zakon.rada.gov.ua/laws/show/994\\_242](http://zakon.rada.gov.ua/laws/show/994_242).

5. Закон України від 18 листопада 2003 р. № 1280-IV “Про телекомунікації” // Відомості Верховної Ради України. – 2004. – № 12. – Ст. 155.

6. Рекомендації № R (99) 5 Комітету Міністрів державам-членам Ради Європи по захисту недоторканності приватного життя в Інтернеті

[Електронний ресурс]. – Режим доступу : [http://www.medialaw.kiev.ua/laws/laws\\_international/105/](http://www.medialaw.kiev.ua/laws/laws_international/105/).

7. ARTICLE 29 – DATA PROTECTION WORKING PARTY. WP 37. Working Document. Privacy on the Internet – An integrated EU Approach to On-line Data Protection, adopted on 21st November 2000 [Електронний ресурс]. – Режим доступу : <http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2000/wp37en.pdf>.

8. International Working Group on Data Protection in Telecommunications. Report and Guidance on Data Protection and Privacy on the Internet “Budapest – Berlin Memorandum” [Елект-

ронний ресурс]. – Режим доступу : [http://www.datenschutz-berlin.de/attachments/138/bbmem\\_en.pdf?1200577389](http://www.datenschutz-berlin.de/attachments/138/bbmem_en.pdf?1200577389).

9. ВГО “УАЗПД”. Звіт за результатами громадського моніторингу “Забезпечення прозорості та відкритості обробки персональних даних на веб-ресурсах” [Електронний ресурс]. – Режим доступу : <http://uapdp.org/images/news/doslidzhennya/Research-results-v.2.2.pdf>.

10. ВГО “УАЗПД”. Декларація “За недоторканість приватного життя в Інтернеті” [Електронний ресурс]. – Режим доступу : <http://uapdp.org/images/1016%202012%20.pdf>.

---

**Анотація:** В статтю проаналізовано український та європейський досвід врегулювання питання обробки та захисту персональних даних в мережі Інтернет, визначено проблемні питання та шляхи подальшого розвитку законодавства України на основі європейського досвіду.

**Ключові слова:** обробка та захист персональних даних, вдосконалення законодавства, іноземний та український досвід, інтернет.

**Abstract:** The domestic and European experience on processing and protection of personal data in Internet is analyzed in the article. The optimal ways of its development in Ukraine on European experience are suggested.

**Key words:** processing and protection of personal data, improvement of legislation, foreign and domestic experience, Internet.

УДК 35.746.1

*СОЛОДКА Олена Маркіянівна*

## **СУЧАСНІ ТЕНДЕНЦІЇ МІЖНАРОДНОЇ ПОЛІТИКИ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ**

**Постановка проблеми.** Глобальні інтеграційні процеси в умовах інформаційної революції впливають на формування нової системи міжнародних відносин, що характеризуються розмитістю державного суверенітету, збільшенням політичної та економічної взаємозалежності суб'єктів міжнародного співробітництва, необхідністю реалізації міжнародних стратегій цивілізаційного розвитку на різних рівнях взаємодії. Процеси глобалізації мають неоднозначні наслідки. З од-

ного боку, вони забезпечують взаємозв'язки у межах світу, сприяють демократизації глобального управління, відкривають нові можливості для збалансованого розвитку регіонів і держав; з іншого – технологічні зміни формують нові типи поляризації у сучасному світі, що призводить до асиметрії міжнародного розвитку.

Становлення інформаційного суспільства дає змогу не лише будувати більш ефективно та розвинене громадянське суспільство, але