УДК 316.324.8

КАРЄВ І.Ю., аспірант ДНУ ІІБП НАПрН України.
ORCID: https://orcid.org/0000-0003-2503-4007.

ЗАХИСТ ПРИВАТНОСТІ ПРИ ВИКОРИСТАННІ ФАЙЛІВ “COOKIES”: АНАЛІЗ СТАНУ ПРАВОВОГО РЕГУЛЮВАННЯ ЗА КОРДОНОМ

Анотація. *У статті досліджується світовий досвід регуляторних політик у сфері захисту персональних даних при використанні файлів “cookies” та ризиках приватності, які вони несуть. Розвиток інформаційних технологій створив розквіт електронної комерції та розвиток цифрових комунікативних технологій, але разом з цим стали з’являтися ризики у сфері захисту персональних даних. Розглянуто регламенти та умови обробки персональних даних у глобальній комп’ютерній мережі Інтернет як у вітчизняному, так і міжнародному законодавствах. Крім того, розглянуто необхідність використання сучасних роз’яснень іноземних регуляторів та необхідність розуміння технічної частини при створенні модернізованого українського регламенту захисту персональних даних.*

Ключові слова: *GDPR, CCPA, захист персональних даних, файли “cookies”, приватність, Privacy Policy, Cookies Policy.*

Summary. *This article examines the world experience with the regulatory policy in the field of personal data protection when using “cookies” files. The development of information technology created rise of e-commerce and the development of digital communication technology, but along with this, risks in the field of personal data protection have been appeared. Regulations and conditions of personal data processing in global computer network Internet in foreign and domestic legislation are considered. Beside this, need to use modern explanation of foreign regulators and understanding technology field when creating part in creating modernized Ukrainian regulation on personal data protection is considered.*

Keywords: *GDPR, CCPA, personal data protection, “cookies” files, privacy, Privacy policy, Cookies Policy.*

Постановка проблеми. Сучасні інформаційні технології (далі – ІТ-технології), що змогли змінити звичний світ у економічному та соціальному планах, а саме розвиток веб-ресурсів та Інтернет-магазинів, спричинили появу такого явища як технології відслідковування персональних даних користувача, для певних цілей веб-ресурсу, а саме шляхом використання файлів “cookies”, що в загальному вигляді полягає у створенні текстових файлів з необхідною інформацією та передачі їх до веб-ресурсу.

З одного боку ці файли необхідні для покращення роботи веб-сайту, але існує ризик, що певна інформація буде передана до третіх осіб, тобто відбудеться процес передачі персональних даних до третіх осіб. Сучасне українське законодавство практично не регламентує дану дію, але існує європейський досвід, який дає змогу захистити приватність користувача та у той же час не допустити витоку інформації.

Метою статті є аналіз нормативно-правової бази, окреслення завдань для модернізації та імплементації світового досвіду до українського законодавства у сфері застосування файлів “cookies” і аналогічних технологій, які створюють ризики приватності, та вдосконалення чинного законодавства у сфері захисту персональних даних у період цифрових трансформаційних процесів.

Результати аналізу наукових публікацій. Захист прав та свобод людини вважається пріоритетним явищем у юриспруденції, але з появою та розвитком інформаційних

технологій з'явилися нові виклики у питанні забезпечення прав у сфері захисту персональних даних. Стрімкий розвиток ІТ-технологій змусив розвивати і законодавчу базу, адже інструменти "відслідковування користувачів" (далі – трекери) стали повсякденною нормою життя. Глобальність та необхідність дослідження питання перебуває у фокусі уваги як багатьох вчених, що працюють у різних сферах науки, так і практиків – юристів.

В Україні початок вирішення законодавчих проблем та формування системи захисту персональних даних здійснюється з 1995 р. та продовжується у наш час в контексті захисту та безпеки інформаційної і конфіденційної приватності персональних даних у комунікаціях [1].

Питанню юридичного застосування файлів "cookies" приділяли увагу А. Кобрін, І. Лясківський, А. Ніколаєв, Л. Олексюк. За межами країни до вивчення феномену файлів "cookies" залучалися вчені різних галузей – фахівці з кібербезпеки, психологи, соціологи, юристи М. Дегелінг, К. Утц, К. Ленцш, Т. Хольц, К. Метт, Х. Хоссейні, Ф. Шауб та інші. Аналіз та роз'яснення практики застосування файлів "cookies" та інших видів трекерів міститься у звітній документації різних національних спеціалізованих органів.

Водночас залишаються недослідженими окремі проблеми, що виникають при використанні файлів "cookies" та трекерів, що можуть порушити приватність користувача.

Виклад основного матеріалу. З технологічним розвитком глобальної комп'ютерної мережі Інтернет з'явилося багато ризиків для особи у сфері інформаційної безпеки, кібербезпеки та у напрямі захисту приватності особи. Основний ризик – це передача персональних даних особи, отриманих під час взаємодії між пристроєм користувача та веб-ресурсом за допомогою певних технологічних рішень, які являють собою один з основних принципів роботи у мережі Інтернет.

Проблематика українського законодавчого регулювання питань використання файлів "cookies" та інших подібних технологій має відношення до Закону України "Про захист персональних даних", а саме у визначенні терміну "персональні дані" як "відомості чи сукупність відомостей про фізичну особу, яка ідентифікована або може бути конкретно ідентифікована" [2]. Саме по собі визначення носить загальний характер, адже немає жодної згадки про класифікацію та ознаки зазначених даних. У той же час, Загальний Регламент про захист даних (ЄС) 2016/679 від 27.04.16 р. (далі – GDPR) дає інше визначення: "персональні дані означає будь-яку інформацію, що стосується фізичної особи, що ідентифікована або може бути ідентифікована ("суб'єкта даних"); фізична особа, що може бути ідентифікована – це особа, яка може бути ідентифікована, прямо чи опосередковано, зокрема за такими ідентифікаторами, як ім'я, ідентифікаційний номер, дані про місце розташування, он-лайн-ідентифікатор або на один чи декілька факторів, специфічних для фізичної, фізіологічної, генетичної, ментальної, економічної, культурної або соціальної ідентичності цієї фізичної особи" [3].

В питанні ідентифікації суб'єкта у Законі штату Каліфорнія про приватність споживачів (California Consumer Privacy Act – CCPA) наводяться чіткі ідентифікатори, завдяки яким можливо ідентифікувати особу. А саме: MAC-адреса пристрою, IP-адреса, файли "cookies", заводський номер, IMEI, унікальний псевдонім (nickname), телефонні номери, але список не завершений, адже будуть з'являтися нові можливості для ідентифікації особи [4]. Різниця у законодавстві України та GDPR з CCPA полягає у моменті згоди на обробку персональних даних. Проблемою практики правовідносин між громадянином та організацією є те, що мета та підстави обробки персональних даних

доводиться до громадян незрозумілою, формалізованою або навіть протокольною мовою, що створює труднощі для розуміння. Саме через це особа не має захищеності своїх прав. У той же час GDPR встановлює, що повідомлення "політики приватності" (Privacy Policy) мають бути роз'яснені простою, зрозумілою мовою та дає можливість застосування ІТ-технологій для отримання даної згоди. Правила щодо інформування суб'єктів персональних даних містяться у статтях 12, 13 та 14 GDPR. Але існують критерії що базуються саме на статті 12 GDPR [5].

Ці критерії є такими:

- стислий зміст – уникнення великого об'єму інформаційного потоку на людину. Ідея полягає у тому, щоб запобігти стану людини, коли через великі об'ємів інформації притупляється сприйняття та з'являється бажання пропустити цей етап як найшвидше;
- прості слова та легкість розуміння – текст має бути роз'яснено зрозумілою мовою для кінцевого споживача, тобто легко, просто без специфічних термінів, навіть для дитячої аудиторії за умови, що вони є споживачами сервісу;
- легкодоступна форма – користувач повинен отримувати вичерпну інформацію про обробку персональних даних у кілька кліків. Заборонено введення у оману та заплутування користувача, або запуск по колу вже виданої інформації – за таку дію призначено штраф;
- вчасність – користувач має бути проінформований саме у момент отримання від нього персональних даних. За умови, що інформація про особу збирається з інших джерел, користувач має бути проінформований у місячний період з моменту першої комунікації з користувачем чи під час першого розголошення даних. Якщо існують істотні зміни у практиці збору, обробки персональних даних, то така інформація повинна бути відображена у "політиці приватності". За запитом суб'єкта – можлива усна форма інформування – телефонний дзвінок або за допомогою будь-якої технології, що дозволяє комунікувати голосом;
- безоплатність – надання Privacy Policy має відбуватися лише на безоплатній основі [5].

Для роботи з клієнтами з Євросоюзу необхідно дотримуватися правил GDPR, а також створення Privacy Policy для веб-ресурсу. Існує можливість її створення у автоматичному режимі за допомогою онлайн-сервісів [6]. У тексті будуть використані шаблонні фрази саме для певного випадку, але слід зазначити що навіть у такому разі необхідно розуміння того, що має бути втілено у Privacy Policy для уникнення штрафних санкцій. Наприклад, А. Кобрін наголошує, що у Privacy Policy обов'язково мають бути вказані такі пункти:

- найменування та контактні дані контролера, у разі потреби – його представника;
- контактні дані інспектора, якщо така особа призначена;
- цілі для яких обробляють персональні дані, правова підстава для їх обробки;
- одержувачі або категорії одержувачів персональних даних, якщо такі є;
- намір контролера передати персональні дані у іншу державу або міжнародну організацію;
- строк зберігання персональних даних;
- право подання скарг у наглядовий орган (уповноважений державою орган контролю);
- наявність прав вимагати від контролера доступу до персональних даних;
- наявність процесу автоматизованого прийняття рішення, включаючи профілювання, відповідно до статті 22 GDPR [7].

На відміну від GDPR, спеціалізований вітчизняний законодавчий акт у сфері захисту персональних даних не зобов'язує до роз'яснення простою зрозумілою мовою та немає розділення щодо інформування для дорослих та дітей. Завдяки такому підходу збільшується вірогідність того, що користувач прийме імпульсивне рішення згоди на обробку персональних даних, не маючи розуміння щодо інформації про Privacy Policy, що може бути використаним для соціального маніпулювання особою.

За дослідженнями М. Ковентрі та інших щодо прийняття файлів "cookies" – що складнішим, не зрозумілішим та об'ємнішим є текст, то імпульсивніше людина його сприйме. З дослідження випливає, що користувачі, які спостерігали за своїми знайомими та родичами, як ті не вникали у суть Privacy Policy, виробили рефлекс не вникати у суть Privacy Policy та надавати згоду[8]. Тобто, якщо неможливо сформувати культуру взаємодії при застосуванні персональних даних, то створюються умови для їх витоку.

Постає питання, яким чином надається згода користувача пристроїв без екрану – такого типу як "розумна колонка" Amazon? З одного боку сам пристрій не має засобів для виведення інформації щодо Privacy Policy, але все ж таки певні дані він буде збирати за допомогою трекерів. У даному випадку процес отримання згоди стає задачею виробника товару. Спираючись на п. 1 ст. 7 GDPR, можливість отримати згоду надається через спеціалізований додаток для смартфону або персонального комп'ютера, у якому вже є можливість ознайомитися, погодитися та при необхідності передивитися або відкликати згоду.

Разом з Privacy Policy йде так зване Cookies Policy (політика використання файлів "cookies") – тобто критерії відповідності взаємодії файлів "cookies" та пристрою споживача. Такі критерії передбачають відповіді на наступні питання:

- тип встановлених файлів "cookies";
- які категорії персональних даних обробляються файлами "cookies";
- які цілі має файли "cookies" на веб-сайті;
- який період часу файли "cookies" залишаються на пристрої користувача;
- куди та кому надсилаються персональні дані користувачів та яким третім особам вони передаються;
- яким чином користувач може дозволити чи заборонити файлам "cookies" обробляти свої дані;
- яким чином користувач може змінити або перевірити стан своєї згоди на обробку персональних даних.

Слід зауважити, що Cookies Policy – це не заміна або аналог Privacy Policy, це опис технічних особливостей застосування файлів "cookies". Кожен з власників веб-ресурсу повинен розташувати її на сайті. Існують спеціалізовані інструкції Європейської ради із захисту даних (EDPB), які регламентують, що може становити згоду (технічний аспект питання), яким чином повинні поводити себе банери згоди та яким саме чином вони повинні працювати [9]. Тому, наприклад, завчасно проставлені, власником сайту, галочки згоди на банері – це вже порушення, адже такого роду згода може бути із-за неуважності, а не від бажання людини.

Українське законодавство має загальні юридичні положення щодо регуляції у сфері захисту персональних даних. Але воно не визначає регуляцію діяльності з файлами "cookies" у контексті техніко-технологічних регламентів (стандартів) щодо них. Також не маємо пояснень щодо застосування файлів "cookies" та створення Cookies Policy.

Статті 4 та 7 GDPR регламентують вимоги до згоди, а стаття 6 має визначення згоди [10]. Слід відзначити, що має бути відповідність до GDPR та CCPA (або інших регіональних законів щодо конфіденційності та файлів "cookies"), тобто з'являється зобов'язання ретельного контролю за діяльністю та типом файлів "cookies" для самого власника веб-ресурсу. Існує програмне забезпечення для автоматичного аналізу та визначення порушень у законодавстві при використання трекерів на веб-ресурсі. Таким чином, існує можливість захисту власника веб-сайту від ризиків настання юридичної відповідальності. До речі, І. Лясківський стверджує, що у CCPA існує свій підхід до правочинності обробки персональних даних, а саме відсутність переліку підстав, на основі яких можна законно здійснювати обробку персональних даних, таким чином встановлюючи, що збір і обробка персональних даних як такі є апріорі законними та можуть здійснюватися компаніями. Разом з тим, в інтересах захисту прав суб'єктів даних, CCPA встановлює право особи направити компанії вимоги щодо заборони продажу її персональних даних. У випадку отримання такої вимоги компанія не має права в подальшому продавати дані цієї особи [11]. Цікаво при цьому те, що питання продажу даних та інформації взагалі не унормовано законодавством України, хоча це у практиці звичайне явище.

Слід зауважити, що згідно п. 2 статті 4 GDPR обробка даних може бути автоматизованою, але навіть у такому варіанті вона теж має підпорядковуватися правилам обробки персональних даних, а користувач проінформований, яка саме інформація збирається та для якої мети [3]. Завдяки максимально широкому тлумаченню терміну "обробка персональних даних" для охоплення циклу життя чутливої інформації починаючи від збирання, використання, зберігання до моменту розголошення або знищення при роботі з персональними даними необхідно враховувати наступне:

- термін "обробка" стосується лише персональних даних, але у той же час усі ті ж самі дії, але з іншими даними, норми GDPR не регулюють;
- дані, які були зібрані , оброблені, проаналізовані, повинні бути захищені на всіх стадіях, а не лише на тих, які цікаві контролеру, оператору [3];
- обробка стосується як роботи у автоматизованому режимі з цифровими базами даних, а також і даними з аналогових баз (тобто ті, які фізично існують), але для цього остання повинна бути структурована у певному вигляді;
- знеособлення також являє собою взаємодію з персональними даними, тому робота з такими даними повинна відбуватися на законних підставах про обробку персональних даних.

Поява файлів "cookies" змусила удосконалити певні аспекти роботи у глобальній мережі Інтернет, а саме можливість створення інтерактивних мап, "кошику покупця" для Інтернет-магазинів та збереження вже заповнених форм. Файли "cookies" являють собою текстові файли що були отримані від веб-сайту та зберігаються у браузері користувача. Тобто це спосіб довгострокового зберігання даних на стороні користувача. При відвідуванні цього самого веб-сайту файли "cookies" будуть повторно направлені до веб-сайту для що створить певні зручності для користувача [12].

Однією з функцій файлів "cookies" є створення веб-сесій, тобто для визначення періоду коли користувач зайшов на сайт та припинив роботу. Така функція необхідна для можливості авторизації на сайті, але існує і інший функціонал:

- збереження персональних даних. У файлах "cookies" зберігаються налаштування користувача – мова, тема оформлення, геолокація, формат дати та часу, валюта, кількість

елементів на сторінці, розширення екрану, введений текст, тип операційної системи, кліки та переходи [13];

- робота з Інтернет-магазином без реєстрації. При зборі товару у "кошик користувача" весь асортимент буде збережено та при наступному вході на сайт буде показано;
- швидке завантаження сайтів. Технічні засоби та службові дані надають таку можливість;
- аналіз якості роботи веб-сайту;
- збір статистики про відвідування сайту;
- збір даних про користувача для формування таргетованої та ревалентної реклами [14].

Передача персональних даних, що знаходяться у файлах "cookies", піднімає питання порушення приватності користувача та можливість створення профілю для ідентифікації. Один з варіантів показу ревалентної, таргетованої реклами – створення профілю користувача на основі персональних даних отриманих за допомогою файлів "cookies". Google прямо вказує на ідентифікатори [10].

Самі файли "cookies" можуть бути кількох видів:

- *Session cookies* – видаляються у момент закриття Інтернет-ресурсу;
- *Persistent cookies* – зберігаються певний час на пристрої користувача. Для них завжди йде запит про застосування. Дані види файлів відносяться до First party cookies – вони передають інформацію тільки між клієнтом та Інтернет-ресурсом. Але існує варіант, коли даний тип файлів передає інформацію до третіх сторін за допомогою URL-запитів;.
- *Third party cookies* – використовуються третьою стороною, тобто не самим веб-сайтом, а його партнерами. Зазвичай ця інформація йде до рекламодавців та соціальних мереж. Ця технологія дає змогу стежити за користувачем, навіть коли він переходить з сайту на сайт, збирає інформацію про його дії, цікаві статті або товари. У подальшому дана інформація буде використана для таргетованої, ревалентної реклами. Питання про заборону технології Third party cookies не вирішить питання втручання у приватність користувачів цифрової комп'ютерної мережі, адже існують інші маркетингові технології:
- *Single Sign-On (SSO)* – суть технології являє собою підключення до великої та кількості Інтернет-ресурсів за допомогою одного спільного облікового запису, який являє собою рекламний профіль;
- *Fingerprint* – відслідковує технічні дані пристрою та браузеру користувача, поведінку на сайті. За допомогою цих даних є змога отримувати інформацію майже так само, як і за допомогою файлів "cookies".

Контролюючий орган Франції (CNIL) розробив інструкції та роз'яснення щодо використання технологій типу Third Party Cookies та подібних технологій [13]. Існуючі технології та майбутні розробки повинні виконувати усі принципи та вимоги GDPR і E-privacy Derective [15]. Незважаючи на тип технології, необхідно повідомляти про збір персональних даних користувача, а також надати змогу відмовитися від відслідковування. При цьому, інформація має зберігатися не більше 25 місяців та термін повинен бути переглянутий задля розуміння, чи повинна ця інформація зберігатися саме такий час.

За повідомленням журналу Official Journal of the Italian Republic існує інструкція, яка роз'яснює аспекти роботи з трекерами та іншими інструментами відслідковування [16]:

- заборона на показ інформації на сайті через відмову від "cookies" являє собою правопорушення (так званий принцип Cookie Wall);

- при кожній новій сесії користувача, що вже відмовився від використання “cookies”, потрібно знову демонструвати угоду про застосування “cookies” – а якщо ні, то це визначає “агресивний підхід”, що неприпустимо та не має жодних підстав для застосування (GDPR та E-Privacy не примушують до таких дій);

- сайт повинен надати користувачу інформацію, хто буде отримувачем їхніх персональних даних, з якою метою збирається та скільки буде зберігатися.

GDPR дає можливість обробки персональних даних за згодою суб’єкта [17]. Для компанії, яка збирає та обробляє дані, для цього має бути чітко визначений інтерес. При роботі з Інтернет-ресурсами – це захист від шахрайства шляхом збирання відомостей про IP-адреси, час відвідування, поведінку на сайті, інформацію про пристрій, MAC-адресу, або для певних маркетингових досліджень – з якого регіону або міста більша кількість відвідувачів та у який час. Але існує нюанс, що такий інтерес має відповідати законодавству, а контролер має захищати такі дані та нести відповідальність за їх виток. Такий законний інтерес, за роз’ясненням EDPB, не може становити підставу для обробки персональних даних у зв’язку з такими цілями як відстеження, профілювання та реклама [18; 19]. У будь-якому випадку, кожен користувач мережі Інтернет буде мати справу з трекерами або іншими технологіями, які будуть обробляти та відслідковувати користувача.

Постає питання, чи правомірним, для користувача, буде використання блокувальників реклами та анонімайзерів, або VPN для роботи у мережі Інтернет? Так як реклама показується за допомогою отриманих персональних даних, файлів “cookies” та інших трекерів, GDPR не має пунктів, що забороняють використання програмних продуктів, що дозволяють змінювати IP та MAC адреси, блокувати чи спотворювати інформацію, отриману завдяки файлам “cookies”.

З погляду GDPR ніякого порушення прав та свобод немає, а навіть навпаки, закон дає право на захист від зазіхання на приватність особи, як технологічні варіанти, завдяки яким можливо зберегти приватність. Є технології, які розроблені Агентством Європейського Союзу з питань мережевої та інформаційної безпеки (ENISA, European Union Agency for Cybersecurity) з метою захисту анонімності особи, а також зменшення факторів, що дають можливість ідентифікації особи. Побачити структуру набору даних можливо, але ідентифікувати особу, до якої вона відноситься – стає складніше [20].

До речі, Закон України “Про рекламу” жодним чином не регламентує обіг реклами у цифровій комп’ютерній мережі Інтернет [21]. Стосовно файлів “cookies” або інших трекерів також регламентування відсутнє.

Немає визначених правил щодо використання інструментів для застосування або збору маркетингових даних, так само як і не вказаний технологічний регламент стосовно принципів роботи у сфері Інтернет-маркетингу. Законодавством поки що не регулюється ринок персональних даних у сфері маркетингу та реклами. Не визначено правил та обов’язків для власників веб-ресурсів щодо збору та використання персональних даних українців. Державний контроль за подальшою долею приватних даних, зібраних за допомогою трекерів, не проводиться, так як в Україні немає контролюючого органу у сфері захисту персональних даних. В той же час, існує необхідність створення вітчизняних версій E-Privacy та Cookies Policy, що продиктовано сучасним станом розвитку IT-технологій. Й це має відбуватися на основі технічного аналізу появи нових методів та технологій використання трекерів.

Практично існуючий у державі несанкціонований ринок персональних даних, які використовуються для показу ревалентної реклами, також має бути законодавчо врегульований. Необхідно створення закону “про електронні ринки”, який буде регулювати взаємовідносини у сфері продажу персональних даних у рекламних цілях.

Окремо треба звернути увагу на правомірність примусового показу реклами та рекламних оголошень. Будь-яка реклама у цифровій комп'ютерній мережі Інтернет показується користувачу без згоди на її отримання. В той же час, за допомогою Інтернет-засобів виникає можливість отримання інформації про користувача та його ідентифікація. Й це вже напряму стосується проблемних питань свободи та забезпечення приватності людини у період трансформаційних процесів та розвитку комунікаційних технологій.

Висновки.

Завдяки впровадженню ІТ-технологій, сучасний світ постійно змінюється у соціальному, економічному та технологічному планах. Процеси діджиталізації та імплементації новітніх комунікативних технологій змушують законодавців активніше розробляти нові закони для захисту прав та свобод людини. Сурові реалії такі, що обробка персональних даних відбувається як у матеріальному світі, так і у віртуальному. Високі юридичні стандарти захисту приватності, які встановив GDPR, дають змогу особі мати впевненість у захисті своєї приватності. Стрімкий процес діджиталізації суспільства ставить нові виклики та задачі до законодавця. Адже розвиток законодавчої бази повинен йти разом з технологічним розвитком. Тому сьогоднішнє питання стосовно регуляції файлів "cookies" та інших програмно-апаратних засобів автоматизованої обробки персональних даних стоїть досить гостро. Сучасні ІТ-технології, що змогли змінити звичний світ у економічному та соціальному планах, а саме розвиток веб-ресурсів та Інтернет-магазинів спричинив появу такого явища як поява технології відслідковування персональних даних користувача для певних цілей веб-ресурсу. З одного боку ці файли необхідні для покращення роботи веб-сайту, але існує ризик, що дана інформація буде передана до третіх осіб, тобто відбудеться процес передачі персональних даних до третіх осіб. Сучасне українське законодавство слабко регулює це питання, але існує європейський досвід, який дає змогу захистити приватність користувача, та у той же час не допустити витоку інформації. Необхідність модернізації українського законодавства також полягає у виконанні взятих на себе зобов'язань стосовно асоціації з ЄС [22]

Останній законопроект щодо сфери захисту персональних даних від 07.06.21 р. № 5628 [23], як вважаємо, може сприяти можливості подальшого приведення законодавчої бази до рівня Євросоюзу. Він спрямований на модернізацію GDPR, але з модифікаціями, що спростять його застосування в українських умовах.

Пропонується при подальшому оновленні вітчизняного законодавства у сфері захисту персональних даних враховувати існуючу практику застосування європейських правових стандартів, у першу чергу позиції регуляторів у розумінні особливостей використання окремих технологій, у тому числі технології файлів "cookies", відмовившись від простого механічного запозичення законодавчих приписів.

Використана література

1. Защита персональных данных / Баранов А., Брыжко В., Базанов Ю. Киев: Національне агентство по інформатизації при Президентові України, ВАТ КП ОТІ, 1998. 128 с. ISBN 966-7308-10-3; Становлення і розвиток правових основ та системи захисту персональних даних в Україні: монографія / В.Г. Пилипчук, В.М. Брижко, О.А. Баранов, К.С. Мельник; за ред. В.М. Брижка, В.Г. Пилипчука. Київ: ТОВ "Видавничий дім "АртЕк", 2017. 226 с. ISBN 978-617-7264-95-7.

2. Про захист персональних даних: Закон України від 01.06.10 р. № 2297-VI. URL: https:// zakon. rada.gov.ua/laws/show/2297-17/conv#n11 (дата звернення: 30.05.2022).

3. Регламент (ЄС) 2016/679 від 27.04.16 р. "Про захист фізичних осіб у зв'язку з обробкою персональних даних та про вільне переміщення таких даних, а також про скасування Директиви

95/46/ЄС (Загальний Регламент про захист даних)". Art 4 GDPR. URL: https://gdpr-text.com/uk/read/article-4 (дата звернення: 30.05.2022).

4. California Consumer Privacy Act (CCPA). State of California Department of Justice. URL: https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180SB1121 (дата звернення: 30.05.2022).

5. Регламент (ЄС) 2016/679 від 27.04.16 р. Art 12 GDPR. URL: https://gdpr-text. com/uk/read/article-12 (дата звернення 30.05.2022)

6. Privacy policy generator. URL: https://www.privacypolicies.com/ (дата звернення 30.05.2022).

7. Кобрін А., Корчинський Д., Некрутенко В. GDPR: посібник з виживання; під ред. Д. Іванова. Одеса: Видавничий дім "Гельветика", 2022. С. 114. ISBN 978-966-992-729-3.

8. Coventry M., Jeske D., Blynthe M., Turland J., Brigs P. Personality and Social Framing in Privacy Decision-Making: A Study on Cookie Acceptance. 07.09.2016. URL: https://doi.org/10.3389/fpsyg.2016.01341 (дата звернення: 30.05.2022).

9. EDPB Guidelines 05/2020 on consent under Regulation 2016/679. 04.05.2020. URL: https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202005_consent_en.pdf (дата звернення: 30.05.2022).

10. Політика конфеденційності та умови використання. Google. URL: https://policies.google.com/technologies/cookies?hl=ua (дата звернення: 30.05.2022).

11. Ляськівський І. CCPA, GDPR, Закон України "Про захист персональних даних". Вони однакові? – (Legal IT Group). URL: https://legalitgroup.com/ccpa-gdpr-zakon-ukrayini-pro-zahist-personalnih-danih-voni-odnakovi (дата звернення: 30.05.2022).

12. What is a web session? *Hazelcast glossary*. URL: https://hazelcast.com/glossary/web-session

13. CNIL. Cookies and other tracking devices. 23.06.2019. URL: https://www.cnil.fr/en/cookies-and-other-tracking-devices-cnil-publishes-new-guidelines (дата звернення 30.05.2022).

14. Рильков С. Що таке файли "cookies" і для чого вони потрібні? URL: https://highload.today/cookies

15. E-privacy. Directive 2002/58/ЄС. 25.11.2009. URL: https://edps.europa.eu/sites/default/files/publication/08-04-10_e-privacy_en.pdf (дата звернення: 30.05.2022).

16. Guidelines on the use of cookies and other tracking tools. 10 June 2021. *Official Journal of the Italian Republic*. No 163 of 9 July 2021. URL: https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9677876#english (дата звернення: 30.05.2022).

17. Регламент (ЄС) 2016/679 від 27.04.16 р. P. 1. Art 6. URL: https://gdpr-text.com/uk/read/article-6/ (дата звернення: 30.05.2022).

18. Opinion 03/2013 on purpose limitation (WP 203) adopted on 2 april 2013. URL: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf (дата звернення: 30.05.2022).

19. Opinion 06/2014 on the notion of legitimate interests of the data controller under article 7 of Directive 95/46/EC (WP 217). URL: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217en.pdf (дата звернення: 30.05.2022).

20. ENISA. Data Pseudonymisation: Advanced Techniques and Use Cases. 28.01.2021. URl: https://www.enisa.europa.eu/publications/data-pseudonymisation-advanced-techniques-and-use-cases (дата звернення: 30.05.2022).

21. Про рекламу: Закон України від 03.07.96 р. № 270/96-ВР. URL: https://zakon.rada.gov.ua/laws/show/270/96-%D0%B2%D1%80/conv#n11 (дата звернення: 30.05.2022).

22. План заходів з виконання Угоди про асоціацію між Україною, з однієї сторони, та Європейським Союзом, Європейським співтовариством з атомної енергії і їхніми державами-членами, з іншої сторони. П. 11. URL: https://zakon.rada.gov.ua/laws/show/984_011 (дата звернення: 30.05.2022).

23. Про захист персональних даних: проект закону від 07.06.21 р. № 5628. URl: http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=72160 (дата звернення: 30.05.2022).

~~~~~~~~~~~~~ * * * ~~~~~~~~~~~~~
~~~~~~~~~~~~~