УДК 342.721

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

ВІДОБРАЖЕННЯ СУЧАСНИХ ІНТЕРНЕТ-ТРЕКЕРІВ У ЗАКОНОДАВСТВІ

Анотація. *У статті досліджується феномен Інтернет-трекерів та ризиків, які вони несуть у сфері захисту персональних даних та ризиків приватності користувача. Розвиток інформаційних технологій створив розквіт електронної комерції та цифрових комунікативних технологій, але разом з цим стали з'являтися ризики у сфері захисту персональних даних, безпеки та кібербезпеки користувачів. 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, трекер, приватність, Privacy Policy, Cookies Policy, кібербезпека.*

Summary. *This article explores phenomena of internet-trackers and risks of their usage in the field of personal data protection and privacy risks of the user. 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 appeared in the field of personal data protection, security and cybersecurity of users. Author considers regulations and conditions of personal data processing in global computer network Internet in foreign and domestic legislation. Beside this, need to use modern explanation of foreign regulators and understanding technology field when creating part in creating modernize Ukrainian regulation on personal data protection is considered.*

Keywords: *GDPR, CCPA, personal data protection, tracker, privacy, Privacy Policy, Cookies Policy, cybersecurity.*

Постановка проблеми: Розвиток та впровадження сучасних ІТ-технологій, а саме розвиток Інтернет-маркетингу та міжсайтового відстеження створили практику порушення права конфіденційності особи. Інтернет-компанії збирають значну кількість особистої інформації, а саме історію веб-переглядів та дії виконані користувачем на веб-ресурсах. Це практика ідентифікації користувача за його унікальними технічними характеристиками пристрою, що створює унікальний "відбиток", завдяки якому можливе профілювання.

Захист конфіденційності вважається пріоритетним явищем у юриспруденції, але з розвитком технологічного прогресу з'явилися новітні виклики у питаннях приватності. Правове питання використання інструментів "відслідковування користувачів" (далі – трекери) знаходиться у площині кібербезпеки, інформаційної безпеки та питань захисту персональних даних.

Результати аналізу наукових публікацій. Питання захисту конфіденційності, приватності та захисту персональних даних неодноразово порушувалось вітчизняними вченими, серед них В. Брижко, О. Баранов, В. Пилипчук та іншими. У плані кібербезпеки та інформаційної безпеки саме питання використання трекерів, на науковій основі, не розглядалося.

Дослідження щодо порушень приватності особи при використанні трекерів містяться у звітній документації національних спеціалізованих органів у сфері захисту

персональних даних. Але регуляція відносин стосовно трекерів визначається лише у технічному плані. Сучасне українське законодавство не визначає регулювання дій щодо трекерів, а саме питання використання Інтернет-трекерів майже не вивчене.

Метою статті є визначення проблем щодо сучасних Інтернет-трекерів на підставі аналізу нормативно-правової бази та світової практики регуляторних політик у сфері захисту персональних даних для створення підґрунтя, що сприятиме модернізації українського законодавства у період цифрових трансформаційних процесів.

Виклад основного матеріалу. Технологічний розвиток людства та повсякчасна імплементація новітніх інформаційно-комунікаційних технологій сприяє нововведенням у сфері взаємодії суб'єктів суспільних відносин. Розвиток електроніки та ІТ-технологій у симбіозі з розвитком комунікаційних можливостей створює умови для розвитку електронної комерції у вигляді Інтернет-маркетів, рекламних компаній у мережі Інтернет та у програмному забезпеченні для комунікаційних пристроїв – смартфонів та планшетів. Але разом із технологічним розвитком бізнес-процесів у цифровій комунікаційній мережі Інтернет з'явилися ризики для особи у сфері інформаційної безпеки, кібербезпеки та у сфері захисту приватності особи. Найбільш поширений ризик – передача персональних даних особи при взаємодії між пристроєм користувача та веб-ресурсом за допомогою певних технологічних рішень, які являють собою один з основних принципів роботи у мережі Інтернет. Саме на зборі, обробці, класифікації персональних даних користувачів і побудовано принцип надання таргетованої, релевантної реклами користувачам. Принцип полягає у ідентифікації користувача та отриманні його пошукових запитів.

Передача персональних даних особи відбувається при взаємодії пристрою користувача та веб-ресурсу. Існують певні технологічні рішення для отримання, зберігання, ідентифікації користувачів. У кожної компанії, яка займається впровадженням рекламних оголошень, методика взаємодії з рекламною аудиторією буде схожа, але методи отримання, обробки та ідентифікації користувача будуть дещо різними як у технічному, так і в юридичному аспектах. Простота збору, використання та продажу персональних даних користувача залежить від законодавчого відношення до питання приватності та персональних даних. Окремо слід відзначити регуляторну політику законодавства до можливості продажу персональних даних користувача та регуляторної політики у сфері Інтернет-маркетингу.

Інструмент "відслідковування користувачів" – походить від англійського "Tracking Device", скорочено – "трекер". Але офіційного визначення даного явища немає у Регламенті ЄС-2016 (GDPR), CCPA та закону про захист персональних даних. Проте у офіційних документах CNIL даний термін використовується.

Сам Інтернет-трекер являє собою програмний засіб для отримання певної інформації, але із-за відсутності чіткого визначення його також називають технологією (іноді під термін "трекер" підпадає кілька програмних засобів об'єднаних лише тим, що вони виконують схожі функції, але можуть відрізнятися за методом виконання свого функціоналу). Методика отримання персональних даних від користувача буде залежати від вибраного ІТ-рішення для вирішення даної задачі.

Виходячи з ситуації, коли саме визначення відсутнє, пропонуємо своє бачення даного питання:

Інтернет-трекер (далі – трекер) – програмний засіб, який створений для збору персональних даних, профілювання та ідентифікації пристроїв користувача при взаємодії з веб-ресурсом у комунікаційній цифровій мережі Інтернет або інших цифрових мережах.

Взаємодія користувача з трекером, а саме початок юридичних відносин починається з моменту прийняття або відхилення згоди на обробку персональних даних, але навіть при повній відмові від надання персональних даних, існують певні обов'язкові дані, що у будь-якому разі надаються до веб-ресурсу. До речі, сучасне українське законодавство не регламентує застосування або заборону певних видів трекерів, тобто можливо використовувати усі види. У ситуації, коли компанія власниця веб-ресурсу хоче працювати у ЄС або США, тоді необхідно відповідати критеріям захисту персональних даних GDPR або CCPA.

Трекери збирають персональні дані користувачів, тобто Закон України "Про захист персональних даних" має регулювати діяльність пов'язану зі збором, обробкою та використанням такої інформації. Визначення, що дає законодавець, стосовно персональних даних – "відомості чи сукупність відомостей про фізичну особу, яка ідентифікована або може бути конкретно ідентифікована" [6]. Але дане формулювання розмите, відсутня класифікація, ознаки зазначених даних. Така позиція не дає можливості віднесення даних, що збирають трекери до сфери персональних даних. Також не визначено правил контролю за збором, продажем та застосуванням персональних даних користувачів як на території України, так і умови їх використання за кордоном. Закон "Про рекламу" також не визначає правил щодо використання інструментів для збору та застосування Інтернет-даних та персональних даних [7].

Закон штату Каліфорнія про приватність споживачів – CCPA (California Consumer Privacy Act) наводить чіткі пункти, за якими можливо ідентифікувати особу у цифровій комунікаційній мережі Інтернет: 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 [8]. Позиція стосовно збору персональних даних – вона апріорі законна та може здійснюватися компаніями, але у інтересах захисту прав суб'єктів даних кожна особа має право направити компанії вимоги щодо заборони продажу її персональних даних. Позиція закону досить проста – персональні дані можна збирати, продавати та використовувати на власний розсуд. Таким чином було вирішено питання трекерів.

Європейський Регламент захисту персональних даних GDPR визначає "персональні дані" як інформацію, що стосується фізичної особи, яку ідентифіковано або можливо ідентифікувати (суб'єкт даних); фізична особа, яку можна ідентифікувати, є такою особою, яку можна ідентифікувати, прямо чи опосередковано, зокрема, за такими ідентифікаторами як ім'я, ідентифікаційний номер, дані про місцеперебування, онлайн-ідентифікатор або за одним чи декількома факторами, що є визначальними для фізичної, фізіологічної, генетичної, розумової, економічної, культурної чи соціальної сутності такої фізичної особи [9]. Позиція стосовно збору, використання та продажу персональних даних жорстко регламентована. Перш за все слід відзначити поняття "Privacy Policy" – згода на обробку персональних даних. При цьому, згода йде до моменту отримання персональних даних від особи. Стосовно Privacy Policy існують певні критерії, порушення яких призводить до штрафних санкцій [10].

Необхідно відзначити, що GDPR регламентує роботу систем збору персональних даних та відстеження користувачів-трекерів. Слід зазначити, що CNIL – контролюючий орган Франції розробив інструкції саме для застосування трекерів [11]. Позиція регулятора полягає у тому, що будь-яка існуючі технологія та майбутні розробки повинні виконувати усі принципи та вимоги GDPR і E-Privacy Derective [12]. Незважаючи на тип технології або трекеру необхідно повідомити про збір персональних даних користувача, а також надати змогу відмовитися від відслідковування. Також

заборонено створювати умови, при яких користувач не може отримати інформацію з веб-ресурсу без погодження на передання персональних даних – принцип Cookie Wall.

Сучасні технології трекерів можна поділити на кілька видів – трекери, що відносяться до веб-сегменту, трекери соціальних мереж та трекери пристроїв та трекери мобільних додатків. Кожен з видів систем збору та ідентифікації користувача має певні властивості та застосовує характерні для нього технологічні аспекти, які мають на меті обійти регламент GDPR, E-Privacy.

Трекери для веб-сегменту необхідно розглядати у залежності від технології, за яким вони працюють та яким саме принципом взаємодіють з персональними даними пристрою користувача. Мета трекерів – зібрати максимальний об'єм інформації про пристрій користувача.

Файли "cookies" – технологічне рішення, яке являє собою невеликі текстові файли, що передаються в тілі запитів веб-серверу та відповідей пристрою користувача. Зберігаються у спеціальних директоріях веб-браузера користувача. Файли "cookies" – відповідають за створення веб-сесії, тобто процесу, який починається з запиту від користувача до певного веб-ресурсу, отримання запиту та направлення відповіді на пристрій користувача, закриття сесії за умови запиту користувача або примусового припинення взаємодії. Функціонал файлів "cookies" полягає:

- збереження особистих налаштувань, а саме мова, тема оформлення, геолокація, формати дати та часу, валюта, кількість елементів на сторінці, розширення екрану. При повторній взаємодії веб-ресурс, на основі збережених файлів "cookies", відтворить налаштування;
- швидке завантаження веб-сайту завдяки збереженій технічній інформації;
- аналіз якості роботи веб-сайту;
- збір статистики про відвідування сайту;
- збір рекламних даних користувача для формування таргетованої та ревалентної реклами [13].

Файли "cookies" можуть зберігатися певний час на пристрої користувача – Persistent cookies або видалятися відразу після сесії – Session cookies. Ці види файлів відносяться до first party cookies – вони передаються виключно між пристроєм клієнта та веб-ресурсом.

Розвиток рекламного бізнесу та ринку продажу персональних даних створив необхідні умови для нав'язування технологічному рішенню взаємодії між клієнтом та веб-сервісом додаткових можливостей у сфері збору та ідентифікації персональних даних пристроїв користувачів. Корпорація Google – у своїй політиці конфіденційності прямо вказує на застосування файлів "cookies" для збору, вказує на використання отриманих персональних даних для показу таргетованої та релевантної реклами під кожного користувача. Такий процес можливий у разі ідентифікації та створення рекламного профілю користувача, який можливо користується кількома різними пристроями. Тобто точність ідентифікації сягає майже 100 % [14]. Одна з модифікацій файлів "cookies" – Third party cookies. Така технологія використовується не самим веб-ресурсом, а його партнерами. Зібрані дані передаються до рекламної компанії, яка реалізує рекламу на веб-ресурсі. Ця технологія дає змогу стежити за користувачем, навіть коли він переходить з сайту на сайт, збираючи інформацію про його дії на тому чи іншому сайті. У подальшому дана інформація буде використана для таргетованої, ревалентної реклами. З появою GDPR та Privacy Policy активність компаній, що використовують third party cookies та інших трекерів дещо змінилась. Адже тепер необхідно зазначення та дотримання певних пунктів [15]:

- найменування та контактні дані контролера, у разі потреби – його представника;
- контактні дані інспектора, якщо така особа має бути 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 третю державу або міжнародну організацію;
- строк зберігання персональних даних;
- право подання скарг у наглядовий орган;
- наявність прав вимагати від контролера доступу до персональних даних;

Наявність процесу автоматизованого прийняття рішення, включаючи профілювання, відповідно до статті 22 GDPR [16].

Питання використання трекеру (third part cookies) частково вирішується за допомогою технології SSO – single sight-on. Суть технології – створення одного контролера, який зберігає та опрацьовує отримані персональні дані. Реклама надається завдяки певному списку постачальників реклами, завдяки якому власник може проводити модерацію у плані таргетингу та релевантності реклами у залежності від профілю користувача. Зі сторони користувача створюється його профіль та надається форма згоди на передачу персональних даних або заборону. Також у профілі зберігається інформація щодо пошукових запитів. Коли користувач заходить на веб-ресурс, який співпрацює з рекламною компанією з технологією SSO, то він тільки одного разу обирає форму згоди, але при наступному зверненні до будь-якого веб-ресурсу партнеру даної рекламної компанії – згоду переробляти не потрібно.

SSO, як метод збору та обробки персональних даних, ґрунтується на положенні GDPR, що правовою основою для обробки персональних даних є законний інтерес, який переслідує контролер або третя сторона [17]. Тут можливо апелювати тим, що свобода ведення бізнесу являє собою законний інтерес, але також слід враховувати те, що European Data Protection Board (EDPB – Європейська Рада з захисту даних) визначила, що збір та обробка персональних даних для створення профілів та реклами не являє собою законний інтерес [18].

Технологія “відбитку пальця” або Fingerprint – відстеження веб-браузерів за конфігурацією та параметрами системи користувача. За зібраними даними створюється ідентифікатор користувача. Анонімний режим браузера або видалення даних браузера не дає змоги змінити відбиток браузера, на відміну від видалення файлів “cookie”. Зібрана інформація збирається та зберігається у спеціалізованій бібліотеці. “Відбиток пальця” – це збір характеристик, які унікальні для кожного користувача – браузер та технічні характеристики обладнання, а також та інформація, яку браузер надсилає для доступу на веб-ресурс. За допомогою сценаріїв відстеження така інформація буде містити також дрібні дані типу роздільної здатності екрану, встановлені шрифти та інші, які будуть окремо розглянуті. Веб-сайти відстеження збирають, аналізують та формують унікальний відбиток для кожного пристрою. Розробники такої системи вказують точність ідентифікації відвідувача 99,5 % з точною вказівкою його місцезнаходження [19]. Важкість виявлення, складність перешкоджанню відстеження та доступність роблять таку технологію розповсюдженою.

Певні показники, які збираються незалежно від розробника програмного забезпечення для збору відбитків браузера:

- Заголовки http_accept – веб-заголовки, які використовуються, щоб повідомляти серверу, які типи вмісту може обробляти браузер.

- Деталі плагіна браузера – збір даних стосовно плагінів встановлених до браузера. Хоча ця технологія вже не використовується за прямим призначенням, але для ідентифікації вона ідеальна.

- Зсув часового поясу та часовий пояс використовується для визначення загального місцеположення користувача.

- Розмір та глибина кольору – використовується для доповнення інформації щодо користувача.

- Системні шрифти – список шрифтів, які ви встановили на своєму комп'ютері, загалом узгоджений і пов'язаний із певною операційною системою. Якщо встановлюється лише один шрифт, який є незвичним для конкретного браузера, то це показник трекер фіксує.

- Дозвіл на отримання файлів "cookies" – параметр може бути вимкнено чи вимкнуто, але у поєднанні з іншими деталями допомагає ідентифікації.

- Обмежений тест supercookie. Supercookies – не являють собою файли кукі, хоча також збирають та зберігають унікальні ідентифікатори. Досить складно виявити та видалити з системи.

- Хеш-відбиток полотна. Сайт відстеження виконує певний тест елемента <canvas> HTML5 у браузері. Цей показник є унікальною ідентифікацією, яку трекер призначає браузеру користувача після виконання цього тесту. Трекер створює графічний файл з форм, кольорів та тексту за допомогою JavaScript. Отримані дані розшифровуються для визначення відеокарти, встановленої системи, версія мікропрограм, версія графічного драйвера та встановлені шрифти.

- Хеш-відбитка webgl – використовується для виявлення незначних відмінностей у схожих браузерах. Ідентифікує користувача за принципом створення графічного полотна за допомогою 2D та 3D графіки.

- Постачальник і рендерер webgl. Бібліотека, що дозволяє браузерам відтворювати 3D-графіку. Як і інші методи відстеження на основі графіки, трекери шукають будь-які незначні відмінності між тим, як пристрої відображають 3D-зображення, порівняно з пристроями інших користувачів. Постачальник і рендерер WebGL доступні для прямого пошуку за допомогою JavaScript, тому трекери можуть отримати до них доступ. Заголовок DNT. Веб-заголовок, який використовується, щоб повідомити серверу про небажання відстеження.

- Мова – за умови, що встановлена мова буде незвичною для регіону, трекер отримує чіткий ідентифікатор пристрою користувача.

- Система, що встановлена на пристрій.

- Використання блокувальника реклами, його типи.

- Відбиток AUDIOCONTEXT – створюється зразок аудіо файлу для отримання характеристик пов'язаних з аудіо обладнанням та встановленими драйверами. Інформація корисна у плані ідентифікації пристрою користувача.

- Апаратний паралелізм – кількість ядер у центрального процесора пристрою. Параметр корисний разом з іншими параметрами.

- Пам'ять пристрою – параметр корисний разом з іншими параметрами

Зазвичай розробники програмного забезпечення вказують, що їхній трекер відповідає політиці GDPR і CCPA та являє собою процесор даних, тобто програмне забезпечення, яке обробляє дані від імені контролера даних, але не несе відповідальності за них [20]. Посилання на законний інтерес досить прозаїчне – використання ідентифікації користувачів з метою запобігання шахрайським діям. Слід відмітити, що з приводу відповідності GDPR, а саме відповідність дотримання інструкції CNIL

необхідно проводити спеціальне дослідження кожного програмного засобу, адже деякі розробники вказують, що їхня система fingerprint може працювати у "тихому режимі" та все одно отримувати необхідну інформацію [11]. Такого роду дослідження проводилися, досліджували трекери на технологічному рішенні SSO [21].

Кожна соціальна мережа розробляє свій трекер з загальними властивостями – Pixel. Відслідковує дії користувача – огляд сторінок, заповнення форм та час проведений на кожний сторінці веб-ресурсу. Даний інструмент збирає статистику, дозволяючи дослідити аудиторію та легко настроїти таргетинг. Прив'язка зібраної інформації про користувачів основується на базі даних самої соціальної мережі. Точна ідентифікація профілю користувача береться з файлів "cookies" браузеру та зводиться з зібраною інформацією. Таким чином користувач соціальної мережі буде отримувати релевантну, таргетовану рекламу прямо у своєму профілі соціальної мережі. Легкість встановлення на веб-ресурс завдяки використанні технології Java Script. Після встановлення плагіну – створюється картинка розміром у піксель, завдяки якій і відбувається аналіз дій користувача. До речі, звідси і береться назва Pixel.

У даному випадку веб-ресурс виступає процесором даних, у той час коли соціальна мережа виступає контролером. Соціальні мереж залишають за собою право передавати персональні дані до третіх сторін, а саме до рекламодавців, соціальних досліджень. Цікавий аспект – соціальна мережа зберігає інформацію про всі дії користувача, разом з його профілем, рекламним профілем та географічним місцем входу у профіль.

Використання трекерів мобільних додатків являє собою створення профілю користувача після встановлення додатку на смартфон або планшет. Існує кілька варіантів виконання такого виду трекеру.

Після встановлення додатку – створення рекламного профілю зв'язаного з акаунтом додатку або з рекламним ідентифікатором пристрою. Таргетованої реклами немає, збору персональних даних та доступу до контактів користувача або технічних засобів пристрою не відбувається.

Отримання додатком до персональних даних користувача, а саме телефонної книги, можливості отримати дані електронної пошти, GPS-модулю. Досить часто використовується визначення назви мереж Wi-Fi та підключених пристроїв Bluethooth, отримання доступу до медичних даних та технічної інформації пристрою. Тобто отримання усіх можливих персональних даних користувача.

Можливість отримання додатком персональних даних стає більш складною процедурою. Компанія Apple створює для своїх користувачів більше засобів контролю за персональними даними та не дозволяє моніторинг веб-трафіку, тому корпорація Meta, що є власником FaceBook та Instagram, не може вільно збирати дані своїх користувачів. Для обходу даної заборони вони створили свій браузер, який працює "зсередини" додатку. Завдяки такому рішенню кожна дія користувача, при переході на веб-ресурс відстежується, профілюється та зберігається [22].

Питання відстеження дій користувача та збір персональних даних з смартфону або планшету залежить від кількох факторів – тип браузера, тип операційної системи – відкрита чи закрита та рекламного ідентифікатора.

Рекламний ідентифікатор – унікальний ідентифікаційний номер на смартфонах, який надається рекламодавцям для відправки персоналізованої та таргетованої реклами. Методика роботи схожа з файлами "cookies", але у залежності від операційної системи існують певні відмінності. Для операційної системи Android дозволяє відстежувати активність у додатках та пошукових запитах. Є можливість заборонити персоналізовану рекламу, тоді рекламодавець не зможе надсилати таргетовану рекламу, а збір інформації

з інших додатків буде припинено. Для смартфонів на операційній системі IOS різниця полягає у тому, що для отримання персональної або будь-якої іншої інформації програмне забезпечення запитує у користувача дозвіл. До речі, автоматизоване збирання у "тихому" режимі не відбувається.

Існують трекери, які "вбудовані" у пристрої, наприклад, після створення фотографії до її даних заноситься географічні координати місця зйомки, час та дата, серійний номер камери та її модель. До речі, соціальні мережі використовують координати локації саме з таких даних.

Завдяки технічним особливостям застосування технічних пристроїв при роботі у цифровій комунікаційній мережі Інтернет відбувається вимушений обмін певними персональними даними, які надалі використовуються для ідентифікації користувача та завдяки розвитку ринку персональних даних передаються до третіх осіб. Постає питання стосовно певної градації персональних даних – адже виявлення, оприлюднення, перепродаж персональних даних стосовно раси, кольору шкіри, сексуальних уподобань та релігійних переконань являється незаконною діяльністю, а інформація, яка може надати точне місце розташування користувача – ні. Навіть якщо розділити персональні дані на ті, які дозволяють ідентифікувати особу без спеціальних знань або обладнання та спеціалізовані дані – машинного використання, то все одно виходить, що данні споріднені. Застосування трекерів дає можливість відслідковувати пошукові запити, основні веб-ресурси, які відвідує користувач, аккаунти користувача та навіть місця перебування, тобто можливо повністю деанонізувати особу, а це означає що будуть оприлюднені персональні дані – фото, місце перебування, конфіденційна інформація та навіть медичні дані. Такий спосіб отримання інформації виконується комплексним підходом (навіть з застосуванням технології відбитку пальця) компонуючи з інформацією з відкритих джерел. Як приклад – OSINT-розвідка. З практичного боку застосування така ситуація може привести до явища кіберсталкінгу та його активного розвитку [23].

Окремо слід розглянути ситуацію з "відбитком пальця", адже даний трекер має можливість прихованого збору даних та профілювання користувачів, таким чином що його виявити досить важко. З позиції законодавства України, така діяльність підпадає під формулювання "Незаконне придбання або збут спеціальних технічних засобів негласного отримання інформації, а також незаконне їх використання", а для використання розробки, придбання або продажу, необхідно отримувати ліцензію «провадження господарської діяльності, пов'язаної з розробленням, виготовленням, постачанням спеціальних технічних засобів для зняття інформації з каналів зв'язку та інших технічних засобів негласного отримання інформації" [24; 25]. Завдяки тому що немає регуляторної політики стосовно програмного забезпечення та використання трекерів на території України, то їхнє регулювання не відбувається. Але за умови, якщо Українська компанія захоче вийти на ринок Євросоюзу, тоді власникам веб-ресурсу необхідно буде відповідати вимогам GDPR та керуватися інструкціями CNIL та E-Privacy Directive. Але навіть ці закони та правила не дають захисту від "тихого" режиму використання. Відсутність прямої заборони на використання трекерів, яких важко виявити, дає можливість подальшого розвитку та імплементації даного виду трекерів. Питання протистояння "відбитку пальця" підняли розробники веб-браузерів, але не законодавці [26]. Поки що не відомо жодного судового рішення або постанови регуляторів стосовно заборони або штрафних санкцій стосовно власників веб-ресурсів що використовують трекер "відбиток пальця". Якщо вже компанії, що створюють програмне забезпечення для перегляду веб-ресурсів створюють практичні умови для блокування техніки відслідковування користувачів, то це означає що

законодавство вже не може повністю регулювати роботу даного виду програмного забезпечення та захисту персональних даних.

З погляду науковців проблема інформаційної безпеки та приватності у сфері захисту персональних даних – це, насамперед, проблема захисту людини від реальних і потенційних загроз та зловживань "інформаційною владою" у будь-якій сфері життєдіяльності суспільства і держави [27]. Майже безконтрольний збір, використання та передача третім особам персональних даних пристроїв користувачів, зібраних під час звернень до веб-ресурсу і є реальна та потенційна загрози. CCPA не бачить у даному випадку ніякого порушення, адже позиція, якщо персональні дані є – їх можна збирати та використовувати, не дає захисту від протиправних дій третіх осіб. У GDPR політика захисту персональних даних під час взаємодії з веб-ресурсами регулюється, але про повну анонімність та абсолютний захист приватності користувача, поки мова не йде. Виходить, що для захисту персональних даних своїх пристроїв кожен користувач повинен подбати самостійно. Жодним законом або регламентом не заборонено використовувати програмні засоби щодо блокування збору та обробки персональних даних пристроїв – блокувальників реклами та браузерів, що блокують технології відстеження типу "відбитку пальця". Ідеальний варіант взаємодії між пристроями користувача та веб-ресурсу – мінімальний обмін лише необхідними персональними даними та повна заборона на використання трекерів. Такий режим зможе забезпечити збереження персональних даних та створення анонімності при використанні веб-ресурсів. Але у такому випадку багатомільйонна індустрія реклами зазнає краху, що позначиться на світовій економіці, або корпораціям доведеться шукати нові способи для демонстрації персоналізованої та таргетованої реклами.

Захист персональних даних пристроїв користувачів – необхідно розглядати комплексно. З позиції інформаційної, кібербезпеки та захисту приватності персональних даних при взаємодії з веб-ресурсом, завдяки трекерам, отримаємо першу стадію Cyberkiller Chain – а саме розвідку [28]. Отримання третьою стороною технічних даних дає можливість аналізу та планування кібератаки на визначений технічний прилад.

У роботі [29] надається таке визначення поняття "кібербезпека" – "це такий стан захищеності життєво важливих інтересів особистості, суспільства і держави в умовах використання комп'ютерних систем та/або телекомунікаційних мереж, за якого мінімізується завдання їм шкоди через: неповноту, невчасність та невірогідність інформації, що використовується; негативний інформаційний вплив; негативні наслідки функціонування інформаційних технологій; несанкціоноване поширення, використання і порушення цілісності, конфіденційності та доступності інформації".

Разом з вказаним слід зазначити, що в українському законодавстві немає словосполучення "безпека приватності персональних даних" (або "безпека персональних даних"), закріплено лише термін "інформаційна безпека" у Законі України "Про Основні засади розвитку інформаційного суспільства в Україні на 2007-2015 роки" від 09.01.07 р. № 537-V. Згідно п. 13 Розділу ІІІ Закону інформаційна безпека – "це стан захищеності життєво важливих інтересів людини, суспільства і держави, при якому запобігається нанесення шкоди через: неповноту, невчасність та невірогідність інформації, що використовується; негативний інформаційний вплив; негативні наслідки застосування інформаційних технологій; несанкціоноване розповсюдження, використання і порушення цілісності, конфіденційності та доступності інформації".

Але, що важливо, про "процес" захищеності інформації не йдеться [30].

Персональні дані являють собою інформацію, тому об'єктом інформаційної безпеки виступає людина та інформація. Також слід враховувати, що саме завдяки

регуляторній політиці та адміністративно-правовим нормам, які регулюють доступ та розповсюдження (можливість отримання та передачі інформації) та головне – принципи збору, використання та знищення інформації [31]. Безпека людини та кібербезпека пристроїв користувача залежать від законодавчої бази та регулятивної політики, яка обов'язково повинні враховувати рівень та процес науково-технічного розвитку кібербезпекових технологій. Приватність при використанні телекомунікаційних засобів також залежить від законодавчої ініціативи та можливостей у питаннях кібербезпеки.

Виникає питання, а чи слід розділяти поняття "приватність" на приватність при взаємодії у комунікаційних мережах та загальне поняття? Властивість персональних даних, а саме можливість ідентифікації особи або/та технічного пристрою зберігаються. Хоча слід окремо виділити необхідність введення такого терміну як цифрова особистість – сукупність всіх дій, аккаунтів, творчості, історії соціальних мереж та персональних даних. Аккаунт особи у соціальній мережі також являє собою персональні дані, але надані особою самостійно. Але завдяки аккаунту у соціальній мережі можливо провести ідентифікацію особи. Сучасне ставлення до поняття цифрової особистості здебільшого використовується у OSINT дослідженнях щодо певної особи.

Існує необхідність введення до законодавства понять як "інформаційна приватність" та "приватність у комунікаціях".

Під *інформаційною приватністю* розуміється встановлення правил збору, використання, поширення та захисту відомостей про особу (персональних даних) від їх нецільового та несанкціонованого використання, що визначає: а) право людини бути захищеною від втручання в її особисте життя та стосунки чи її родини через публікацію інформації; б) право людини знати, ким, коли, яким чином і в яких межах інформація про неї може бути або буде використовуватися іншими особами [27, с. 62; 30, с. 37].

Приватність комунікацій – усе, що пов'язано з техніко-технологічними засобами і способами забезпечення телефонних розмов, електронних повідомлень, особистого поштового листування та інших видів інформаційно-комунікаційних зв'язків. При цьому, в умовах програмно-технологічного розвитку Інтернету приватність комунікацій все більше пов'язується з інформаційною приватністю, тобто з тим, що передбачає захист персональних даних людини, а також інформаційної безпеки людини, суспільства і держави [27, с. 62]. По-перше, це надасть можливість активніше створювати, розвивати та впроваджувати культуру поводження та захисту персональних даних, по-друге – законодавче застосування даних понять дасть можливість для регулювання методів збору, обробки, та застосування персональних даних, отриманих під час роботи у комунікаційних мережах.

Висновки.

Позиція законотворців стосовно такого явища як трекер не однозначна. З одного боку існують певні правила та обмеження на збір персональних даних з боку GDPR, інструкцій CNIL, E-Privacy Derective та EDPB, але у той самий час відсутня регуляція у плані заборони використання певних типів трекерів типу "відбитку пальця" та відповідальність за їхнє застосування. Відсутність заборони на використання трекерів, які збирають персональні дані у "тихому" режимі, мовчання, регуляторів та DPO, з даного приводу наводить на роздуми, що роботи у даному напряму не ведуться. Заяви від розробників веб-браузерів щодо проведення власних розробок у сфері блокування трекерів типу "відбиток пальця" та інших технік відслідковування та профілювання користувачів, також наводять на роздуми щодо певної паузи у розвитку європейського законодавства.

Сучасний стан розвитку трекерів дає можливість відслідковувати пристрій користувача, його профіль та навіть місце знаходження, що вже дає можливість говорити про відсутність анонімності та можливого порушення кібербезпеки та безпеки приватності людини. Збір персональних даних у "тихому режимі" порушує принципи збору персональних даних [12].

Позиція паузи у створенні законодавчих ініціатив стосовно трекерів здебільшого обумовлена інертністю суспільства. Впровадження культури відношення, ставлення та взаємодії з персональними даними, дасть поштовх до соціальних змін у сфері суспільного ставлення до питання взаємодії, роботи та захисту персональних даних.

Українське законодавство у сфері захисту персональних даних потребує модернізації, але слід використати досвід Євросоюзу у плані регуляції взаємодії з персональними даними, зробити можливість швидко реагувати на нові виклики та загрози та вносити зміни до законодавства. За умови, що трекери типу "відбитку пальця" вже не нові, то зміни до законодавства з урахуванням даного фактору вже необхідно було розглянути, дослідити та імплементувати до законодавчої бази. При створенні модернізованого законодавства слід впровадити позицію щодо визначення "інформаційної приватності" та "приватності комунікацій".

Окремо треба відзначити відсутність загально ратифікованої конвенції про права людини у світових комунікаційних мережах, у якій повинно бути визначено окремим пунктом недоторканність приватних даних особи та юридичну відповідальність за такі дії.

Використана література

1. The right to be left alone. The Enjoyment of Financial and Personal Privacy Is Fundamental to a Free and Civil Society. Mark Skousen. 01.05.2002. URL: https://fee.org/articles/the-right-to-be-left-alone (дата звернення: 01.08.2022).

2. The Holocaust Encyclopedia. Locating the victims. United States Holocaust Memorial Museum. URL: https://encyclopedia.ushmm.org/content/en/article/locating-the-victims (дата звернення: 01.08.2022).

3. IBM and the Holocaust: The Strategic Alliance between Nazi Germany and America's Most Powerful Corporation. ByEdwin Black. New York: Crown, 2001. 519 pp. Cloth. ISBN 0-609-60799-5.

4. Dehomag D11 sorter. United States Holocaust Memorial Museum. URL: https://collections.ushmm.org/search/catalog/irn521587 (дата звернення: 01.08.2022).

5. Загальної декларація ООН про права людини від 1948 року. Стаття 29. URL: https://www.coe.int/uk/web/compass/the-universal-declaration-of-human-rights-full-version (дата звернення: 01.08.2022).

6. Про захист персональних даних: Закон України від 01.10.10 р. № 2297-VI. URL:https://zakon.rada.gov.ua/laws/show/2297-17/conv#n11 (дата звернення: 01.08.2022).

7. 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: 01.08.2022).

8. CCPA. 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: 01.08.2022).

9. General Data Protection Regulator від 25 травня 2016 року. Art 4 GDPR. URL: https://gdpr-text.com/uk/read/article-4 (дата звернення: 01.08.2022).

10. General Data Protection Regulator від 25 травня 2016 року. Art 12 GDPR. URL: https://gdpr-text.com/uk/read/article-12 (дата звернення: 01.08.2022).

11. 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: 01.08.2022).

12. E-Privacy Directive 2002/58/ЄС від 25.11.2009. URL: https://edps.europa.eu/sites/default/files/publication/08-04-10_e-privacy_en.pdf (дата звернення: 01.08.2022).

13. Рильков С. Що таке файли “cookies” і для чого вони потрібні? URL: https://highload.today/cookies (дата звернення: 01.08.2022).

14. Політика конфеденційності та умови використання. Google. URL: https://policies.google.com/technologies/cookies?hl=ua (дата звернення: 01.08.2022).

15. 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.

16. General Data Protection Regulator від 25 травня 2016 року. Art 22 GDPR. URL: https://gdpr-text.com/uk/read/article-22 (дата звернення: 01.08.2022).

17. General Data Protection Regulator від 25 травня 2016 року. P1-f. Art 6 GDPR. URL: https://gdpr-text.com/uk/read/article-6 (дата звернення: 01.08.2022).

18. Інструкція щодо згоди. Guidelines on Consent under Regulation 2016/679. URL: https://ec.europa.eu/newsroom/article29/items/623051 (дата звернення: 01.08.2022).

19. Fingerprint JS. Служба ідентифікації відвідувачів. URL: https://github.com/fingerprintjs/fingerprintjs (дата звернення: 01.08.2022).

20. General Data Protection Regulator від 25 травня 2016 року. Art 28 GDPR. URL: https://gdpr-text.com/uk/read/article-28 (дата звернення: 01.08.2022).

21. C. Matte, N. Bielova, C. Santos. Do Cookie Banners Respect my Choice?: Measuring Legal Compliance of Banners from IAB Europe’s Transparency and Consent Framework. DOI: 10.1109/SP40000.2020.00076. URL: https://ieeexplore.ieee.org/abstract/document/9152617/references#references (дата звернення: 01.08.2022).

22. F. Krause. IOS Privacy: Instagram and Facebook can track anything you do on any website in their in-app browser. URL: https://krausefx.com/blog/ios-privacy-instagram-and-facebook-can-track-anything-you-do-on-any-website-in-their-in-app-browser (дата звернення: 01.08.2022).

23. Карєв І.Ю., Фурашев В.М. Кіберсталкінг: відображення у національному законодавстві. *Інформація і право.* № 1(36)/2021. С. 29-34. URL: http://ippi.org.ua/kar%D1%94v-iyu-furashev-vm-kiberstalking-vidobrazhennya-u-natsionalnomu-zakonodavstvi-s-29-34 (дата звернення: 01.08.2022).

24. Кримінальний кодекс України: Закон України від 05.04.01 р. № 2341-ІІІ. (Ч. 1 ст. 359). URL: https://zakon.rada.gov.ua/laws/show/2341-14/conv#n2480 (дата звернення: 01.08.2022).

25. Деякі питання щодо спеціальних технічних засобів для зняття інформації з каналів зв’язку та інших технічних засобів негласного отримання інформації: Постанова Кабінету Міністрів України від 22.09.16 р. № 669-2016-п. URL: https://zakon.rada.gov.ua/laws/show/669-2016-%D0%BF#Text (дата звернення: 01.08.2022).

26. Firefox 72 blocks third-party fingerprinting resources. Mozzila Security Blog. URL: https://blog.mozilla.org/security/2020/01/07/firefox-72-fingerprinting (дата звернення: 01.08.2022).

27. Пилипчук В.Г., Брижко В.М., Інформаційна безпека та приватність у сфері захисту персональних даних. *Інформація і право.* № 4(19)/2016 р. С. 60-70. URL: http://ippi.org.ua/pilipchuk-vg-brizhko-vm-informatsiina-bezpeka-ta-privatnist-u-sferi-zakhistu-personalnikh-danikh-sto (дата звернення: 01.08.2022).

28. Cyber Killer Chain. Lockhead Martin Corporation. URL: https://www.lockheedmartin. com/en-us/capabilities/cyber/cyber-kill-chain.html (дата звернення: 01.08.2022).

29. Баранов О.А. Про тлумачення та визначення поняття “кібербезпека”. *Правова інформатика*. № 2(42)/2014. С. 54-62. URL: http://ippi.org.ua/sites/default/files/14boavpk.pdf (дата звернення: 01.08.2022).

30. Брижко В.М., Пилипчук В.Г. Приватність, конфіденційність та безпека персональних даних. *Інформація і право.* № 1(32)/2020. С. 33-46.

31. Фурашев В.М. Сутність та визначення понять “інформаційна безпека” і “безпека інформації”. *Правова інформатика*. № 2(34)/2012. С. 51-59. URL: http://ippi.org.ua/sites/default/files/12fvmbbi.pdf (дата звернення: 01.08.2022).

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