

КОНФІДЕНЦІЙНІСТЬ ДАНИХ В ЕПОХУ ЦИФРОВИХ ПЛАТФОРМ: ПОТОЧНІ ТЕНДЕНЦІЇ ТА НОВІ ТРЕНДИ

Чабанець Дар'я Сергіївна,

Київський національний університет технологій та дизайну

Коваль Ольга Миколаївна

Доцент кафедри приватного та публічного права, кандидат юридичних наук
Київський національний університет технологій та дизайну

З огляду на те, що сучасний світ настільки покладається на технології, цілком природно, що цифрові платформи є невід'ємною частиною нашого повсякденного життя. Від соціальних мереж до хмарних обчислень та розумних пристроїв, вони забезпечують комунікацію, роботу для багатьох та спрощення життя. Але чим розвиненішими стають технології тим більше вони викликають величезні питання щодо конфіденційності даних. Оскільки користувачі діляться особистими даними в Інтернеті у гігантських масштабах, знання реалій конфіденційності даних та майбутніх потенційних змін у цьому питанні є надзвичайно важливим.

1. Сучасний контекст конфіденційності даних

Цифрові платформи збирають величезну кількість даних від людей, починаючи від особистих даних, використання Інтернету, місцезнаходження та закінчуючи вподобаннями у контенті. Більшість цих даних використовується для персоналізації досвіду, покращення послуг та надання актуальних рекламних акцій. Але з широким збором виникають проблеми, пов'язані зі зберіганням цих даних, їх використанням та обміном. Як на початку ери технологій та інтернету так і зараз у багатьох виникають сумніви та страхи у зв'язку з подібними зборами інформації, адже ледь не завжди доступ до даних є обов'язковою вимогою для користування застосунками та сайтами.

У світі активно запроваджують суворіші закони про захист даних, намагаючись обмежити зростаючі проблеми з конфіденційністю. Загальний регламент про захист даних Європейського Союзу є одним із найкращих видів законодавства із суворими вимогами щодо конфіденційності даних, згідно з яким компанії повинні отримувати чітку згоду користувачів та дозволяти особам переглядати та видаляти свої дані. Окрім цього, існують такі як Закон Каліфорнії про конфіденційність споживачів (CCPA), що були прийняті в інших місцях і відображають тенденцію до більшої відповідальності з боку компаній, що обробляють персональні дані.

З розголошенням сучасних проблем із витоком даних та передавання їх третім особам, зростає обізнаність та страх щодо питань конфіденційності даних у користувачів, що робить їх більш обережними при наданні своєї інформацією. Користувачі зараз вимагають від компаній забезпечити їм прозорість щодо того,

як використовуються їхні дані, і хочуть знати свої права щодо своїх персональних даних, що, очевидно, є позитивним розвитком подій.

Проте, навіть із подібною тенденцією все ще лишаються проблеми із загрозою кібербезпеки та порушення даних: випадки порушень даних стали причиною для тривоги, а гучні випадки поставили під загрозу особисту інформацію мільйонів клієнтів. Кібератаки розвиваються, тому вкрай важливо, щоб компанії інвестували у високоякісну безпеку для захисту інформації клієнтів. Клієнти сьогодні очікують, що фірми зосередять свої послуги на безпеці даних.

2. Нові та майбутні тенденції в конфіденційності даних.

Новітні технологічні розробки прокладають шлях до можливого покращення та посилення установ з приводу конфіденційності особистої інформації.

Наразі досліджуються анонімність, шифрування та технологія блокчейн для подальшого підвищення безпеки даних та надання користувачам більшої автономії щодо своїх даних. Ці технології можуть захистити індивідуальні дані, водночас дозволяючи отримувати аналітику на основі даних.

2.1. Види блокчейнів.

Технологія блокчейн — це механізм баз даних, який дозволяє прозорий обмін інформацією в межах бізнес-мережі. База даних блокчейну зберігає дані в блоках, пов'язаних між собою в ланцюжок.

Наразі відомі чотири види цієї технології:

1. Публічний - відкритий публічний блокчейн, до якого має доступ хто-завгодно без обмежень. Такий вид відкритий для перегляду записів, перевірки транзакцій та формування нових блоків.

2. Приватний - закритий вид, до якої додаються лише запрошені користувачі, і так само лише вони можуть вносити редагування. Приватний блокчейн використовується організаціями або компаніями для контролю доступу, дозволами та безпекою. Це схоже на публічний блокчейн, проте лише для запрошених осіб.

3. Блокчейн консорціуму - тут блокчейн контролюється різними організаціями. Вони перебувають у мережі одна з одною, можуть обмінюватися інформацією або займатися майнінгом.

4. Гібридний блокчейн - об'єднує закриті та відкриті блокчейни, а саме: ви можете зробити певну інформацію публічною, а певну - доступною для окремих людей. Це допомагає вам контролювати, що доступно для перегляду, кому та до чого вони можуть отримати доступ.

2.2. Штучний інтелект.

Окрім всього, розглядаючи сучасні та майбутні тенденції, окремим пунктом варто розглянути стрімко прогресуючу галузь штучного інтелекту, адже з розвитком цього інструменту також зростають етичні проблеми щодо

використання даних. Розвиваючись, штучний інтелект поглинає великі об'єми баз даних, що містять в собі зображення, відео та тексту, тож і неминуче деякі з цих даних є конфіденційними: інформація персональні дані із соціальних мереж, стан здоров'я користувачів, дані про фінанси, біометричні дані, що використовуються для розпізнавання обличчя, тощо. Оскільки зараз збирається обсяг інформації більше ніж будь-коли раніше, зростає ймовірність того, що принаймні частина з них буде розкрита або використана таким чином, що порушує права на конфіденційність.

У майбутньому, щоб не порушувати довіру своїх користувачів, компаніям доведеться збалансувати використання ШІ для персоналізації реклами, збору інформації та розвитком самого штучного інтелекту.

2.3. Міжнародна співпраця.

Під кінець можна також розглянути міжнародну співпрацю та варіанти вирішення проблеми захисту персональних даних. Очікується, що будуть запроваджені обов'язкові стандарти прозорості щодо збору, зберігання та обробки даних, які будуть запроваджені для ІТ-компаній та великих цифрових платформ.

Крім того, глобальні організації можуть ініціювати вимоги до обов'язкової сертифікації організацій, які працюють з персональними даними, та періодичних незалежних перевірок заходів безпеки цих організацій. Пріоритет буде надано створенню глобального набору етичних норм обробки даних, наприклад, заборона на використання біометричних даних та вимога розкриття діяльності алгоритмів штучного інтелекту та поширення практики ознайомлення користувачів із принципами роботи баз даних. Це не лише захистить права користувачів, але й призведе до більшої довіри до цифрових технологій у глобальному масштабі.

Висновок

Конфіденційність даних на цифрових платформах є складним питанням, яке у сучасному світі є обов'язковим до постійного розгляду та вивчення. З розвитком технологій та зміною соціальних норм зацікавлені сторони повинні надавати пріоритет безпеці даних та працювати із довірою користувачів до онлайн платформ, яким вони надають свою персональну інформацію. Завдяки культурі відкритості, інвестицій у безпеку та належного відношення організації до їх користувачів, платформи можуть забезпечити обізнаність людей у правильній онлайн-поведінці та допомогти їм почуватися безпечно в інтернет просторі. Майбутнє конфіденційності даних буде залежати від співпраці між політиками, підприємствами та споживачами у напрямку створення безпечнішого цифрового світу, який поважає права.