УДК 347:342.9:341.1
DOI https://doi.org/10.24144/2307-3322.2023.80.1.84

ПРИВАТНІСТЬ ЗА ЗАМОВЧУВАННЯМ. КОРИСТУВАЦЬКА МОДЕЛЬ ДАНИХ ЯК ОСНОВА ЗАХИСТУ ПРИВАТНОСТІ ТА ПЕРСОНАЛЬНИХ ДАНИХ В СОЦІАЛЬНИХ МЕРЕЖАХ

Пристай Р.А.,
аспірант кафедри адміністративного та фінансового права
Львівського національного університету імені Івана Франка
ORCID: 0000-0002-8980-1650
e-mail: rostyslaw.law@gmail.com

Пристай Р.А. Приватність за замовчуванням. Користувацька модель даних як основа захисту приватності та песрональних даних в соціальних мережах.

Стаття розкриває поняття та особливості концепції приватності за замовчуванням. Здійснено аналіз законодавства Європейського Союзу, яке регламентує обов'язок дотримання даної концепції – а саме положень Загального регламенту про захист персональних даних. В рамках концепції приватності за замовчуванням, досліджено поняття та ознаки користувацької моделі даних, як такої, що спрямована на зміну правового регулювання та технічого забезпеченння інформаційної безпеки та безпеки персональних даних в соціальних мережах.

З метою досягнення цілей лослідження, проаналізовано необхідність запровадження зазначеної моделі захисту даних – практичні проблеми захисту персональних даних з огляду на особливості ринку послуг провайдерів сервісів соціальних мереж. Обгрунтовано необхідність трактування персональних даних та мета даних користувача соціальних мереж як об'єкта права власності, а також трактування самих мета даних як персональної інфорації про особу яка може бути використана для розпізнавання або відстеження особи окремо або в поєднанні з іншою інформацією, що прямо зазначено в Акті ОМВ № А-130 [1], однак аналогічно не трактується ні в Регламенті про захист даних, ні в законодавстві України.

Наведено основні переваги впровадження користувацької моделі даних, а саме переваги для власників даних, бізнесу, держави та провайдерів хмарних послуг з надання та обслуговування моделі.

Законодавство в сфері захисту персональних даних в ЄС, зокрема в сфері соціальних мереж, є більш комплексним на надціональному та національному рівнях і забезпечене окремим як нормативним, так і організаційним механізмом, який відрізняється від того, який існує на сьогодні в Україні. Механізм захисту персональних даних в Європейському Союзі передбачає створення незалежних публічних органів, які є відповідальними за виконання та дотримання вимог Загального регламенту про захист даних. В статті виокремелено необхідність створення єдиного окремого органу в сфері захисту персональних даних в Україні, який зможе здійснювати функцію моніторингу та забезпечення дотримання вимог відповідного законодавства, зокрема, дотримання приватності за замовчуванням.

Ключові слова: захист персональних даних, приватність за замовчуванням, користувацька модель даних, приватність в соціальних мережах.

Prystai R. Privacy by design. User-held data model as a basis for privacy and personal data protection in social networks.

The article reveals the concept and features of privacy by design approach. An analysis of the legislation of the European Union, which regulates the obligation to comply with mentioned concept, namely the provisions of the General Data Protection Regulation, was carried out. Within the framework of the concept of privacy by design, the concepts and pecularities of using user-held data model are studied, which aims to change the legal regulation and technical support of information security as well as the security of personal data in social networks.

In order to achieve the goal of the research, the need to introduce the specified model of data protection was analyzed – namely practical problems of personal data protection within the peculiarities of the market of social network service providers. The need of the interpretation of personal data as an object of property right was outlined, as well as the interpretation of the purpose of the meta data itself as personal information about a person that can be used to recognize or track a person separately or in combination with other information, which is directly stated in the OMB Act No. A-130, however, is neither interpreted similarly in the Data Protection Regulation nor in the legislation of Ukraine. The main advantages of implementing a user-held data model are presented, namely the advantages for data owners, businesses, the state, and cloud service providers for providing and maintaining the model.

Legislation in the field of personal data protection in the EU, in particular in the field of social networks, is more complex at the supranational and national level. It is provided with a separate regulatory and organizational mechanisms, which are different from the one that exists today in Ukraine. The mechanism for the protection of personal data in the European Union provides the creation of independent public authority that is responsible for the implementation and compliance with the requirements of the General Data Protection Regulation. The article highlights the need to create a single separate body in the field of personal data protection in Ukraine, which will be able to perform the function of monitoring and ensuring compliance with the requirements of the relevant legislation, in particular, compliance with privacy by design.

Key words: personal data protection, privacy by default, user data model, privacy in social networks.

Постановка проблеми. Станом на 2023 рік загальна кількість користувачів соціальних мереж становить 4,76 млрд користувачів у світі та близько 28 млн в Україні. Поряд з цим, росте і кількість порушень в соціальних мережах, які стосуються персональних даних особи. Лише за перший квартал 2023 року понад шість мільйонів записів даних було розкрито в усьому світі через витік даних. З першого кварталу 2020 року найбільшу кількість відкритих записів даних було виявлено в четвертому кварталі 2020 року, майже 125 мільйонів наборів даних.

Такі порушення часто носять внутрішній характер – а саме приватного життя особи внаслідок неналежного використання, зловживання чи захисту сервісом соціальних мереж персональних даних користувача. Втім, до категорії персональних даних не завжди відносять мета дані, оскільки до цієї категорії даних часто входить інформація, за якою прямо ідентифікувати особу неможливо. Внаслідок вказаного підходу, а також часткового нівелювання значення метаданих для подальшого впливу на особу (наприклад, в маркетингових цілях), превалююче становище сервісів соціальних мереж стає все більш домінуючим і здатним використовувати свій статус при розробці подальших Політик конфіденційності, Договорів з користувачем, а також рекламній політиці. Це, в свою чергу, призводить до звуження свободи вибору сервісу користувачем, можливості схиляння користувача до дій, які б він не вчинив за інших обставин – непотрібних покупок чи транзакцій (мова йде про недобросовісну комерційну практику або ж продаж соціальними мережами даних третім особам), а також створенні умов, за яких право власності користувача на інформацію про себе чи пов'язані з ним обставини не припускається і не визнається.

Така ситуація, на нашу думку, є недопустимою в сучасному демократичному суспільстві і повинна негайно бути змінена шляхом запровадження чіткого регулювання порядку одержання інформації про особу сервісами соціальних мереж – як персональних даних, так і мета даних, а також запровадженням юридично обов'язкової технічної структури захисту даних – користувацької моделі даних, як складової концепції приватності за замовчуванням. Дотримання цієї концепції є нормативною вимогою в законодавстві Європейського Союзу, і її втілення, зокрема, повинно поширюватись на сервіси соціальних мереж, які функціонують як в ЄС, так і в Україні. З цією метою необхідним є подальше дослідження поняття приватності за замовчуванням, а також користувацької моделі даних та її подальшої інкорпорації в законодавство України та створення наглядових органів, які будуть здатними ефективно здійснювати моніторинг та заходів належного і пропорційного правового примусу для забезпечення безпеки користувачів.

Стан опрацювання. Питання запровадження користувацької моделі в роботі соціальних мереж, а також в інших сферах досліджували Paul Jurcys, Antti Poikola, Kai Kuikkaniemi, Ossi Kuittinen, Harri Honko, Aleksi Knuutila, Viivi Lähteenoja та інші науковці і фахівці в сфері захисту персональних даних.

Метою статті є аналіз поняття приватності за замовчуванням та користувацької моделі даних, як інструмента її забезпечення, обгрунтування їх запровадження в сферу захисту персональних даних в соціальних мережах.

Виклад основного матеріалу. Організації, які здійснюють обробку персональних даних, включно з соціальними мережами, повинні визначити, як найкраще захистити дані користувачів та як ці дані можуть і будуть використовуватися протягом життєвого циклу даних. Зазначений цикл включає в себе кожний етап обробки даних – від моменту їх збору і до моменту видалення чи знищення. Оскільки в межах організації можуть існувати різні рівні використання даних і типи технологій, що використовуються для обробки персональних даних, дрібні деталі кожного етапу відрізнятимуться від організації до організації. Як правило, спеціалісти з захисту персональних даних виділяють п'ять етапів життєвого циклу даних: збір; використання; передача; зберігання та знищення персональних даних. В межах законодавства України такий умовний поділ розширено до збирання, реєстрації, накопичення, зберігання, адаптування, зміни, поновлення, використання і поширення (розповсюдження, реалізація, передача), знеособлення, знищення персональних даних [2].

Приватність за замовчуванням – це концепція побудови стану забезпечення приватності протягом усього життєвого циклу обробки персональних даних, включаючи технології, системи, процеси, практики та політики, від раннього стану їх розробки до впровадження, використання даних та, зрештою, їх видалення. Приватність та її забезпечення повинно органічно включатись в усі рівні операцій з даними, а не розглядатися як компроміс чи щось, що слід враховувати після створення продукту, системи, послуги чи процесу.

Стаття 25(1) [3] передбачає, що контролери повинні розглядати приватність за замовчуванням на ранній стадії, коли вони планують нову операцію яка передбачає обробку даних. Контролери повинні впроваджувати її перед обробкою, а також постійно під час обробки, регулярно переглядаючи ефективність вибраних заходів і заходів безпеки. Приватність за замовчуванням також застосовується і до існуючих систем, які обробляють персональні дані [4].

Від приватності за замовчуванням до користувацької моделі даних. З огляду на специфіку та типи порушень конфіденційності в соціальних мережах, наступна модель роботи з даними є своєрідним захистом від внутрішніх та деяких зовнішніх порушень персональних даних. Незважаючи на те, що дані, незалежно від того, наскільки вони захищені, завжди можуть бути використані - наприклад, виставлені в соціальних мережах зображення, дані, надані сервісу під час реєстрації або під час роботи з сервісом (мета-дані), можуть бути надійно захищені за допомогою даних, які зберігаються в користувацькій моделі, яка здатна забезпечити захист від внутрішніх порушень.

Для кращого опису користувацької (людино-орієнтованої) моделі даних, необхідно звернути увагу на такі аспекти: передумови, що створюють необхідність її впровадження, концепцію самої моделі (термін і філософія), її основні особливості та переваги, які можна використовувати з метою захисту даних у соціальних мережах.

Щодо передумов. Розвиток існуючих ринків товарів і послуг, соціальних мереж онлайн і, як наслідок, зростання комунікацій, призвели до збільшення кількості обробок персональних даних. Це призвело до накопичення великої кількості даних у великих компаніях (таких як GAFA [5]). Така обробка, звичайно, вимагала нормативного регулювання, яке було втілено в ухваленні таких актів як GDPR, CCPA та Каліфорнійський закон про права на конфіденційність («CPRA)».

Проте, намагаючись врегулювати підхід до обробки персональних даних, нові нормативні акти принесли з собою нові вимоги, такі як право бути поінформованим, право на доступ, право на виправлення, видалення, обмеження обробки, перенесення даних та інші. Такий підхід є правильним, оскільки забезпечує права споживачів, однак не вирішує всіх проблемних питань. Ці проблеми можна умовно розділити на дві категорії: а) ті, що виникають по відношенню до компаній – оскільки нові правила означають збільшення витрат на відповідність; б) щодо споживачів – щодо зручності управління їхніми даними, можливості управляти ними настільки, наскільки це дозволяє їх природа, а не законодавча база та потреби ринку. Саме тому був запропонований новий підхід до управління даними (користувацька модель даних).

Концепція. Модель даних користувача (користувацька модель), насамперед, передбачає створення окремої хмари персональних даних. Ця хмара наповнюється даними завдяки підключенню (прив'язці) до неї різних джерел даних – смартфонів, розумних годинників, персональних комп'ютерів, Інтернету речей, облікових записів соціальних мереж тощо. Таким чином, усі дані про суб'єкта даних та створені ним (зокрема метадані в соціальних мережах) буде розміщено в особистому середовищі, недоступному для третіх осіб. Важливим фактором є те, що після потрапляння в хмару ці дані будуть автоматично уніфіковані в одному форматі, що значно спрощує їх

сприйняття (чого важко, наприклад, досягти при запитах щодо інформації користувачів, яка використовується у великих компаніях, де ця інформація просто не читається). І ще одна особливість, чи не найважливіша з точки зору захисту даних, полягає в тому, що сторонні особи зможуть отримати доступ до певних даних лише за згодою власника даних. Додатки зможуть запускатися локально поверх хмари, що зведе до мінімуму використання даних лише до тих, які дійсно необхідні для коректної роботи додатку та які в той же час будуть зрозумілі користувачеві.

Якщо спробувати визначити цю модель одним терміном, дана модель являє собою закритий хмарний сервіс, який наповнюється деякими персональними та метаданими, уніфікує дані в єдиному, зрозумілому для власника даних форматі та дає власнику можливість самостійно приймати рішення. про використання або заборону використання даних третіми особами.

Ідея запропонована компанією Prifina, яка будує екосистему на основі даних користувачів. Зазначається, що це технологічна архітектура, де кожна людина може підключати різні джерела даних до власної «хмари персональних даних». Основний принцип моделі даних, орієнтованої на користувача, полягає в тому, що особа повинна повністю володіти своїми особистими даними та контролювати їх. Основними принципами є: право власності на дані користувача, згода та контроль, обмеження цілей, мінімізація даних, законність, справедливість і прозорість, безпека персональних даних, сумісність даних [6].

Як показує дослідження Paulius Jurcys, Marcelo Corrales Compagnucci та Mark Fenwick «Майбутнє міжнародної передачі даних», моделі даних, які зберігаються користувачами, здебільшого мають справу з даними, створеними на переносних пристроях із датчиками, які вимірюють місцезнаходження, щоденні кроки, частоту серцевих скорочень та фіксують багато інших фізичних параметрів [7]. Тим не менш, у соціальних мережах все ще генерується величезна кількість метаданих, які також, в свою чергу, не є власністю компаній і належать лише користувачеві.

Політика Facebook щодо метаданих полягає в зборі, використанні та обміні метаданими з метою надання та покращення своїх послуг. Метадані – це інформація, яка генерується або збирається про дії користувача на Facebook, наприклад час і дата публікацій, оцінки «подобається», коментарі та інші взаємодії. Однак такі дані, відповідно до Акту OMB № A-130, де під терміном «Інформація, яка дозволяє ідентифікувати особу» (PII) ми маємо розуміти інформацію, яка може бути використана для розпізнавання або відстеження особи окремо або в поєднанні з іншою інформацією. які пов'язані або можуть бути пов'язані з конкретною особою, – також можуть тлумачитися як персональні дані.

Це означає, що модель захисту персональних даних за замовчуванням, а саме модель даних користувача, також може і повинна застосовуватися до цих даних, оскільки їх власником є не компанія чи служба, а користувач, який їх створив. Така інформація є корисною та вигідною для сервісу, а тому не повинна за замовчуванням передаватись у власність або користування сервісам соціальних мереж. Facebook не є винятком, майже всі компанії збирають метадані, наприклад: Telegram [8], WhatsApp [9], Snapchat [10], Viber [11] та багато інших.

Постійною темою такої моделі є надання людям зручних інструментів для збереження конфіденційності, які надають людям більше свободи волі та контролю над споживчими продуктами, що керуються даними, і, відповідно, своїм життям, і водночас допомагають компаніям відійти від бізнес-моделей, зосереджених на продукті, і запропонувати більш привабливий, але безперешкодний досвід клієнтів, зокрема в соціальних мережах.

Основними особливостями моделі даних, орієнтованої на користувача, є: право власності на персональні дані, яке передбачає, що власник персональних даних зберігає всі свої дані у власному хмарному середовищі, – фактично, те, що він створює, залишається в ньому, а не на сервері чи в іншому місці. Друга особливість полягає в тому, що особисті дані є конфіденційними за замовчуванням, незважаючи на те, що вони генеруються програмами, вони залишаються фактично конфіденційними, оскільки розміщуються в безпечному середовищі без доступу сторонніх осіб. Третя особливість – ліміти використання даних, які зменшені, оскільки власник сам вирішує, чи надавати ці дані, і чітко розуміє мету їх використання. Це також включає власну згоду власника на використання метаданих, законність їх використання відповідно до GDPR, CCPA, CPRA, безпеку та портативність даних.

Переваги. Основні переваги в цьому випадку можна розділити на кілька категорій:

а) переваги для власників даних (про які було зазначено вище – захищеність даних, доступність, право власності на свої дані тощо);

б) переваги для бізнесу (торгівельні платформи, додатки, постачальники послуг тощо), які не потребуватимуть інвестувати великі кошти, щоб забезпечити відповідність своєї діяльності закону;

в) для держави, оскільки модель даних користувача забезпечуватиме дотримання відповідного масиву правових норм у сфері захисту персональних даних – зокрема ст.6 Закону України «Про захист персональних даних»;

г) переваги для провайдерів хмарних послуг з надання та обслуговування, оскільки, швидше за все, якщо модель даних користувача стане широко поширеною, виникнуть нові виклики щодо її розвитку і виникне необхідність в залученні нових спеціалістів в її розробці, технічній підтримці тощо.

Окрім цього, слід зазначитти, що для впровадження такої моделі опрацювання та зберігання особистої інформації, необхідним є її чітке технічне окреслення, сертифікація, доктринальне визнання та законодавча імплементація. В разі створення нормативного акта, який би зміг встановити юридичну обов'язковість таокї моделі, необхідним є і створення відповідного контролюючого органу, який зміг би належним чином здійснювати моніторинг функціонування користувацької моделі та, в разі необхідності, вживати заходів для забезпечення прав користувачів. З цією метою пропонується покласти цю функцію на існуючі контролюючі органи – наприклад національні орани з захисту персональних даних, т.зв. DPA (Data Protection Authrities), або створити профільні органи в державах, де такі органи не функціонують – наприклад, в Україні, де питання захисту персональних даних покладено на Уповноваженого Верховної Ради України з прав людини, роль якого в даній сфері зводиться до актів реагування. Напротивагу цьому, механізм захисту персональних даних в Європейському Союзі передбачає створення незалежних публічних органів, які є відповідальними за виконання та дотримання вимог Загального регламенту про захист даних. Вказані органи надають експертні консультації з питань захисту даних і розглядають скарги, подані щодо порушення Загального регламенту захисту даних і відповідних національних законів. Рішення зазначених органів створюють прецеденти за межами їх юрисдикції і можуть істотно впливати на підхід інших органів ЄС із захисту даних до різних питань у контексті платформ соціальних мереж [12].

Висновки. Запропонована модель захисту персональних даних спрямована на створення умов, за яких постачальники послуг не зможуть використовувати створені користувачами дані за замовчуванням. Право власності на персональні дані належить користувачеві, проте існуюча практика збору та використання метаданих за замовчуванням, хоча і передбачена в Угоді з користувачем, є скоріш неминучою. Такі угоди з користувачем за своєю правовою природою є договорами приєднання, і без деяких послуг соціальних мереж майже неможливо вести професійну діяльність, що ставить користувача в безвихідне становище і тим самим змушує його приєднатися до існуючих умов використання сервісу. Незважаючи на те, що сама модель даних користувача була винайдена для застосування до даних з носимих пристроїв, на нашу думку, вона здатна запропонувати найбільшу популярність і практичну користь саме в контексті соціальних мереж, оскільки може повністю змінити підхід до розуміння персональних даних та забезпечити дотримання вимог законодавства у сфері захисту персональних даних. Крім того, ця модель здатна мінімізувати ризик транскордонної передачі персональних даних і кількість внутрішніх порушень з боку сервісів соціальних мереж.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. CIRCULAR NO. A-130, (Transmittal Memorandum No. 4) (November 28, 2000).
2. Закон України «Про захист персональних даних», № 2297-VI, від 01.06.2010, електронний ресурс: https://zakon.rada.gov.ua/laws/card/2297-17.
3. GDPR text, Article 25 GDPR. Data protection by design and by default, from https://gdpr-text.com/uk/read/article-25/.
4. European Data Protection Board, Guidelines 4/2019 on Article 25 Data Protection by Design and by Default, 20 October 2022.
5. Whats.com, GAFA (the big four) – definition, Compliance, risk and governance, May 2019, from https://www.techtarget.com/whatis/definition.
6. JURCYS P., User-Centric, User-Held Data Model: Key Principles, Medium, Aug 3, 2020, Published in Prifina, from https://medium.com/prifina/user-centric-data-model.

7. Jurcys P., Compagnucci M.C., Fenwick M., The future of international data transfers: managing legal risk with a ‘user-held’ data model, The Computer Law and Security Review, Vol. 46 (2022), 17 Jan 2022.
8. Rakuten Viber, Viber Privacy Policy, August 22, 2023, from https://www.viber.com/en/terms/viber-privacy-policy/.
9. Telegram Privacy Policy, 8 July 2023, from https://telegram.org/privacy/ua.
10. Meta, Help Center, What information does WhatsApp share with the Meta Companies?, from https://faq.whatsapp.com/1303762270462331.
11. Snapchat Support, About Snap and Chat Metadata, from https://help.snapchat.com/hc/en-gb/articles/7012318664852-About-Snap-and-Chat-Metadata.
12. Columbia Univerity, Italian Data Protection Authority v. TikTok, Case analysis, from https://globalfreedomofexpression.columbia.edu/cases/italian-data-protection-authority-v-tiktok/.