УДК 342.72
DOI https://doi.org/10.24144/2307-3322.2023.78.2.7

ЗАРУБІЖНИЙ ДОСВІД ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ У СОЦІАЛЬНИХ МЕРЕЖАХ

Кравчук В.О.,
аспірантка кафедри конституційного і адміністративного права
Національний авіаційний університет
ORCID ID: https://orcid.org/0009-0003-6660-2952

Кравчук В.О. Зарубіжний досвід захисту персональних даних у соціальних мережах.

У статті проаналізовано захист персональних даних на основі зарубіжного досвіду. Визначено, що соціальні мережі є одним із найвидатніших культурних явищ, які виникли в епоху Web 2.0. Вони забезпечують зв'язок користувачів і полегшують обмін інформацією між ними.

З'ясовано, що Європейський Союз прийняв нову систему захисту персональних даних під назвою Загальний регламент захисту даних (GDPR), основними цілями якого є: надання особам інструментів для контролю їхніх персональних даних, впровадження сучасних стандартів захисту особистої інформації, розвиток цифрового простору Європейського Союзу для захисту персональних даних, забезпечення суворого дотримання правил усіма сторонами та юридичний супровід міжнародної передачі особистої інформації.

Проаналізовано законодавчі документи США, які стосуються основних аспектів захисту даних і конфіденційності, а саме: Закон Каліфорнії про конфіденційність споживачів (CCPA); Закон про захист конфіденційності дітей в Інтернеті (COPPA); Закон про перенесення та підзвітність медичного страхування (HIPAA); Закони штату про повідомлення щодо порушення даних.

Визначено, що у Китаї діє комплексна правова база, яка регулює захист персональних даних і включає такі нормативно-правові акти, як: Закон про захист персональної інформації (PIPL) і Закон про безпеку даних (DSL).

Сформовані висновки, згідно з якими терміновість і важливість захисту персональних даних у соціальних мережах зумовлені швидким технологічним прогресом, зростанням загроз кібербезпеці та глобальним розповсюдженням цих платформ. Захищаючи особисті дані, люди можуть зберегти власну конфіденційність, запобігти несанкціонованому використанню даних, зберегти довіру користувачів, зменшити ризики порушень та дотримуватися взятих на себе юридичних зобов'язань. Питання забезпечення мобільності та сумісності в соціальних мережах надає особливого значення захисту персональних даних, оскільки вони стосуються саме цих даних, а не лише технологій, як це може бути в секторі телекомунікацій. Вказане вимагає додаткових роздумів та заходів забезпечення конфіденційності та безпеки даних. Тому при розробці правових механізмів захисту для онлайн-соціальних мереж необхідно враховувати і вирішувати проблеми, пов'язані з захистом персональних даних.

Ключові слова: соціальні мережі, персональні дані, захист персональних даних, зарубіжний досвід, кібербезпека, США, інформаційні технології.

Kravchuk V. Foreign experience of personal data protection in social networks.

The article analyzes the protection of personal data based on foreign experience. Social networking has been identified as one of the most prominent cultural phenomena to emerge in the Web 2.0 era. They keep users connected and facilitate the exchange of information between them.

The European Union has adopted a new personal data protection system called the General Data Protection Regulation (GDPR). Its main goals include providing individuals with tools to control their personal data, implementing modern standards for the protection of personal information, developing the digital space of the European Union to safeguard personal data, ensuring strict compliance by all parties, and providing legal support for the international transfer of personal information.

United States legislative documents related to aspects of data protection and privacy were analyzed, namely: California Consumer Privacy Act (CCPA); Children's Online Privacy Protection Act (COPPA); Health Insurance Portability and Accountability Act (HIPAA); State data breach notification laws.

It is noted that China has a comprehensive legal framework that regulates the protection of personal data, and includes the following legal acts: Personal Information Protection Law (PIPL) and Data Security Law (DSL).

Conclusions were made that the urgency and importance of protecting personal data in social networks is due to rapid technological progress, the growth of cyber security threats and the spread of these platforms. By protecting personal data, people can maintain privacy, prevent abuse, maintain user trust, reduce risk, and comply with legal obligations. The issue of ensuring mobility and interoperability in social networks gives particular importance to the protection of personal data, as it relates to this particular data, and not just to technology, as it may be in the telecommunications sector. This requires additional thought and measures to ensure privacy and data security. Therefore, when developing legal protection mechanisms for online social networks, it is necessary to take into account and solve problems related to the protection of personal data.

Key words: social networks, personal data, protection of personal data, foreign experience, cyber security, USA, information technology.

Постановка проблеми. Сьогодні, у зв'язку зі стрімким розвитком інформаційних технологій та використанням соціальних мереж у повсякденному житті, Інтернет містить персональні дані користувачів, які необхідно захищати належним чином і використовувати виключно за призначенням та за згодою особи, якій вони належать. Порушення правил поводження з персональними даними може призвести до значної моральної та матеріальної шкоди, спричинити неминучі наслідки як для окремого користувача, так і для суспільства в цілому, що також пояснює нагальну необхідність захисту персональних даних, які надходять до соціальних мереж. Оскільки ймовірність порушення персональних даних залишається дуже високою, Європейський Союз намагається використовувати нормативно-правову базу, що спрощує обробку, зберігання даних, а також підвищує безпеку персональних даних [1, с. 497].

З метою утвердження принципів верховенства права та права на приватність в Україні вважаємо за необхідне проаналізувати зарубіжний досвід захисту персональних даних у соціальних мережах. Крім того, в контексті європейської інтеграції держава зобов'язана адаптувати пріоритетні положення про захист особистісної інформації кожної особи до європейських та світових стандартів.

Стан опрацювання проблематики. На сьогодні дослідники все більше зосереджують свою увагу на сфері захисту персональних даних в Інтернеті і цифрових правах особи загалом. Це викликано потребою вирішення проблем, пов'язаних з інтенсивним обміном інформацією та комунікацією в онлайн-середовищі, а також серйозними загрозами недозволеного розповсюдження персональних даних в мережі. Серед видатних науковців, які займаються дослідженнями в цій галузі, варто відзначити А. Баранова, Ю. Базанова, В. Брижко, І. Бачило, В. Наумова, А. Антопольського, Е. Талапіну, В. Архіпова, О. Войніканіс, Н. Варламову, А. Кардаша та інших. Разом з тим, захист персональних даних в мережі Інтернет потребує подальших досліджень і вироблення підходів до розуміння та вирішення проблем, пов'язаних з захистом персональних даних та збереженням приватності в онлайн-середовищі.

Метою статті є аналіз зарубіжного досвіду захисту персональних даних у соціальних мережах.

Виклад основного матеріалу. В умовах глобальної невизначеності та зростання соціальних ризиків, сучасній юридичній науці варто звернути увагу на проблеми конфіденційності і особистих прав в соціальних мережах. Захист персональних даних у соціальних мережах має вирішальне значення для збереження конфіденційності та захисту прав особи. Користувачі повинні мати контроль над своєю особистою інформацією та можливість вирішувати, як вона поширюється та використовується. Захист персональних даних має важливе значення для збереження особистої автономії та запобігання необґрунтованому втручанню в приватне життя.

Окрім типового місця для повсякденної діяльності та соціального спілкування, соціальні мережі є унікальним місцем, де можна спостерігати різні моделі поведінки та взаємодії. Більшість користувачів соціальних мереж активно надають особисті дані у своїх профілях з переконанням, що ці дані будуть доступні тільки їхнім знайомим та доброзичливим учасникам мережі, і не стануть об'єктом неправомірного використання чи спотворення. Зловживання персональними даними, зібраними сайтами соціальних мереж, відбувається дуже часто [2, с. 62].

Отже, соціальні мережі є одним із найвидатніших культурних явищ, які виникли в епоху Web 2.0. Вони служать для зв'язку користувачів і сприяють обміну інформацією між ними. Проте, користувачі, несвідомо розголошуючи значну кількість особистої інформації через соціальні мережі,

не усвідомлюють ризики для конфіденційності та безпеки, пов'язані з такими діями. Законодавство Європейського Союзу, спрямоване на захист персональних даних, може виступати ефективним засобом захисту користувачів від неправомірної обробки їхньої особистої інформації [3, с. 199]. Проте, існують певні проблеми, пов'язані з практичним застосуванням цього законодавства.

– Важливо зазначити, що з однієї сторони, соціальні мережі пропонують численні переваги, а з іншої – вони також викликають занепокоєння щодо конфіденційності, безпеки даних, кіберзалякування та поширення дезінформації. Досягнення балансу між перевагами та проблемами соціальних мереж -обробляються на основі дотримання принципів «прозорості», «законності» відповідно до згоди суб'єкта даних;

– збираються для виконання договору чи вступу в договір;

– обробляються як необхідна умова для дотримання встановленого законом зобов'язання;

– можуть бути видалені або виправлені без затримки, якщо персональні дані є неточними, з огляду на цілі, для яких вони обробляються;

– зберігаються у формі, яка дозволяє ідентифікувати суб'єктів даних не довше, ніж це необхідно для цілей, для яких обробляються персональні дані;

– обробляються у спосіб, який забезпечує належну безпеку персональних даних, включаючи захист від несанкціонованої або незаконної обробки та від випадкової втрати, знищення або пошкодження, використовуючи відповідні технічні або організаційні заходи [5].

GDPR встановлює новий баланс прав, обов'язків і санкцій, що базується головним чином на концепціях підзвітності та конфіденційності за проектом. Це матиме наслідки для питань управління персональними даними в організаціях, які повинні будуть адаптуватися до підвищеного принципу відповідальності. Прийнята регуляторна модель ґрунтується на соціальному пакті між державними та приватними суб'єктами, необхідному для розробки та застосування правил, що забезпечують дотримання європейських правил. Обов'язковість дотримання GDPR для компаній не лише накладає нові обмеження, але й відкриває можливості бути більш прозорими щодо політики захисту персональних даних. Це сприяє підвищенню довіри громадян до управління їхніми даними шляхом включення в процес спільного регулювання та відповідального впровадження нововведень [6].

У контексті нашого дослідження, вважаємо за необхідне проаналізувати зарубіжний досвід захисту персональних даних у соціальних мережах.

Станом на вересень 2021 року Сполучених Штатах немає всеосяжного федерального закону, спеціально присвяченого захисту персональних даних у соціальних мережах. Однак у США існує кілька законодавчих документів, які стосуються аспектів захисту даних і конфіденційності. Ось деякі ключові нормативно-правові акти, що стосуються захисту персональних даних:

1) Закон Каліфорнії про конфіденційність споживачів (CCPA) – це закон штату Каліфорнія, який покликаний надати більше контролю жителям Каліфорнії над тим, як їхні персональні дані зберігаються та обробляються. Цей знаковий закон закріплює нові права на конфіденційність для споживачів у Каліфорнії, зокрема:

– право знати про особисту інформацію, яку компанія збирає про них, а також про те, як вона використовується та передається;

– право на видалення особистої інформації, зібраної з них (за деякими винятками);

– право відмовитися від продажу чи передачі своєї особистої інформації;

– право на недискримінацію для реалізації своїх прав згідно з CCPA [7];

2) Закон про захист конфіденційності дітей в Інтернеті (COPPA) – це федеральний закон, який регулює збір особистої інформації дітей віком до 13 років. Він накладає особливі вимоги на операторів веб-сайтів або онлайн-сервісів, які націлені на дітей [8];

3) Закон про перенесення та підзвітність медичного страхування (HIPAA) -Закони штату про повідомлення щодо порушення даних. У багатьох штатах прийнято такі закони, які вимагають від компаній інформувати осіб, коли відбувається порушення обігу персональних даних, оскільки вони можуть скомпрометувати або поставити під загрозу особисту інформацію [10]. Ці закони зазвичай визначають вимоги та терміни сповіщення постраждалих осіб.

У Китаї діє комплексна правова база, яка регулює захист персональних даних, у тому числі даних у соціальних мережах. Швидке розширення цифрових послуг, збільшення генерації, збору, обробки та використання даних, а також численні інциденти, що загрожували інформаційній безпеці привело до актуалізації питань захисту даних у політичному порядку денному країн по всьому світу, включаючи Китай. У зв'язку з цим, у 2021 році урядом Китаю було оприлюднено Закон про захист персональної

інформації (PIPL) і Закон про безпеку даних (DSL). Ці закони, формують комплексну основу для захисту персональних даних у Китаї.

Основним законом, що стосується захисту персональних даних у Китаї, є Закон про захист персональних даних (PIPL), який було прийнято 20 серпня 2021 року. PIPL запроваджує комплексні правила щодо збору, використання та обробка особистої інформації організаціями [11]. Вважаємо за необхідне, представити основні положення та вимоги PIPL щодо захисту персональних даних у соціальних мережах: згода (організації отримують інформовану згоду осіб перед збором і обробкою їх персональної інформації); специфікація та мінімізація мети; заходи безпеки (організації, що обробляють особисту інформацію, мають впроваджувати відповідні заходи безпеки, щоб захистити дані від несанкціонованого доступу); транскордонна передача даних (організації мають пройти оцінку безпеки або отримати сертифікат від визнаної сторонньої організації для передачі персональних даних на територію іншої іноземної держави); права користувача (право доступу, виправлення, видалення та обмеження обробки їх особистої інформації); локалізація даних (зберігання та обробка особистої інформації в Китаї).

За останні 5 років Китайська Народна Республіка прискорила зусилля щодо створення правової архітектури захисту даних. З оприлюдненням Закону про захист персональної інформації (PIPL) і Закону про безпеку даних (DSL) простежується значний вплив на потоки даних усередині Китаю та за його межами. На сьогодні, уряд Китаю пропонує новий підхід до захисту даних, які підлягають порівняльному аналізу, і можуть мати вагомий вплив на розвиток законодавства щодо захисту даних в інших державах, особливо тих, які мають тісні цифрові зв'язки з їхньою країною. Для цього потрібне глибше розуміння того, як це законодавство формується в політичному та економічному контексті Китаю.

Через відносно концентрований характер ринку та домінування окремих соціальних мереж соціальні онлайн-мережі можуть стати наступною цифровою послугою, яка зіткнеться з пильною увагою Європейської комісії. На сьогодні, соціальні мережі є невід'ємною частиною життя багатьох людей і мають мільярди користувачів у всьому світі. Величезний обсяг персональних даних, які передаються та зберігаються на цих платформах, робить критично важливим захист цієї інформації від зловживань та експлуатації.

Висновки. На сьогодні захист персональних даних у соціальній мережі вийшов на новий якісний рівень. Після кількох резонансних випадків витоку персональних даних у соціальній мережі світова спільнота зрозуміла, що ефективний захист персональних даних є гострою потребою сьогодні. Як наслідок, у 2016 році Європейський Союз прийняв правила GDPR, які через свою екстериторіальність можуть регулювати відносини із захисту персональних даних навіть в Україні. Терміновість і важливість захисту персональних даних у соціальних мережах зумовлені швидким технологічним прогресом, зростанням загроз кібербезпеці та розповсюдженням цих платформ. Провідні держави світу створюють не лише технологічні, а й правові механізми захисту персональних даних у соціальних мережах. Українське законодавство про захист персональних даних є порівняно застарілим і не враховує сучасні виклики, ризики та глобальність соціальних мереж. Актуальним питанням є створення закону про соціальні мережі, який містив би порядок збору, отримання, зберігання, використання, передачі персональних даних у соціальних мережах в Україні.

Список використаних джерел:

1. Токарєва К.С. Проблеми захисту персональних даних у сфері охорони здоров'я в умовах інформатизації. *Юридичний науковий електронний журнал*. 2022. № 11. С. 496–499. DOI https://doi.org/10.32782/2524-0374/2022-11/120.
2. Vilić V., Radenković I. Possibilities of Protecting Personal Data Published on Social Network Sites in the Light of the Law on Personal Data Protection. *The Internet and Development Perspective*: Paper presented at Sinteza 2016 – International Scientific Conference on ICT and E-Business Related Research., January 2016. Pp. 62–65.
3. 3.Kosta E., Kalloniatis C., Mitrou L. and Gritzalis S. Data protection issues pertaining to social networking under EU law, Transforming Government: People, Process and Policy, 2010. Vol. 4 No. 2, Pp. 193-201. URL: https://doi.org/10.1108/17506161011047406.
4. 4.Skendžić A., Kovačić B., Tijan E. General data protection regulation – Protection of personal data in an organisation. *41st International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO)*, Opatija, Croatia 2018. Pp. 1370–1375. URL: https://doi.org/10.23919/MIPRO.2018.8400247.

5. General Data Protection Regulation (GDPR) : Regulation of the European Union of 27.04.2016 no. 2016/679. URL: https://gdpr-info.eu/.
6. Gola R. Le règlement européen sur les données personnelles, une opportunité pour les entreprises au-delà de la contrainte de conformité. LEGICOM, 2017. Vol. 59. Pp. 29–38. URL: https://doi.org/10.3917/legi.059.0029.
7. The California Consumer Privacy Act (CCPA): state statute of 28.06.2018 No. 375. URL: https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180AB375.
8. California Consumer Privacy Act of 2018: state statute of 03.01.2018 no. 16 CFR Part 312. URL: https://www.ftc.gov/system/files/2012-31341.pdf.
9. Health Insurance Portability and Accountability Act of 1996: United States Act of Congress of 21.08.1996 no. 110 Stat. 1936. URL: https://aspe.hhs.gov/reports/health-insurance-portability-accountability-act-1996.
10. Nuzhnyy V. Channel for IT. New EU requirements for personal data protection from May 2018. URL: http://channel4it.com/publications/ Nov-vimogiS-do-zahistu-personalnih -danih-z-travnya2018-roku-30154.html.
11. Creemers R. China's emerging data protection framework. *Journal of Cybersecurity*. 2022. Volume 8, Issue 1. URL: https://doi.org/10.1093/cybsec/tyac011.