УДК 342.7
DOI https://doi.org/10.24144/2307-3322.2024.82.2.41

ЗАХИСТ ПЕРСОНАЛЬНИХ ДАНИХ В МЕРЕЖІ ІНТЕРНЕТ

Самагальська Ю.Я.,
кандидат юридичних наук,
доцент кафедри інтелектуальної власності, інформаційного
та корпоративного права
Львівського національного університету ім. І. Франка
ORCID: https://orcid.org/0000-0001-7313-8623
e-mail: ysamagalska@gmail.com

Самагальська Ю.Я. Захист персональних даних в мережі Інтернет.

В процесі щоденної комунікації особи передають та отримують велику кількість інформації. Так, звичне відвідування веб-сайту вже може надавати його власнику інформацію щодо його користувачів (файли cookie). А реєстрація, купівля товарів надасть власнику конфіденційну інформацію про особу. З огляду на це, виникла необхідність захистити фізичну особу та врегулювати окремий підвид такої інформації під назвою «персональні дані» з метою забезпечити особі право на невтручання в особисте життя у зв'язку з їх обробкою.

Поняття «персональні дані» не є новим для України, адже Закон «Про захист персональних даних» був прийнятий ще у 2010 році, проте практика його застосування свідчить про те, що суб'єкти відносин, пов'язаних із персональними даними, трактують його досить поверхнево. Так, володільці та розпорядники персональних даних формально, без уточнення мети і способу обробки, повідомляють суб'єкту персональних даних, що його персональні дані будуть оброблятись. А суб'єкти персональних даних надають таку згоду, не читаючи порядок обробки персональних даних та політики конфіденційності. Ймовірність, що бази персональних даних суб'єктів будуть видалені після припинення правовідносин з їхнім володільцем чи розпорядником є доволі мала. Через неналежний захист та контроль бази персональних даних є постійними об'єктами зливів та викрадень, що в свою чергу, сприяє іншим правопорушенням, особливо в мережі Інтернет.

В даній статті приділена окрема увага дослідженню збору персональних даних на веб-сайтах українських політичних партій, адже ці персональні дані в розумінні законодавця є особливими (чутливими) і їх обробка мала б здійснюватися ще більш прискіпливо. В умовах військового стану витік таких персональних даних прихильників певної політичної сили може становити для них фізичну небезпеку.

З огляду на це, автор робить висновок про необхідність приведення національного законодавства про захист персональних даних до вимог Загального регламенту про захист даних ЄС та посилення контролю за його додержанням. Також в статті пропонується закріпити поняття права на забуття та посилити відповідальність за порушення законодавства про захист персональних даних.

Ключові слова: інформація, захист інформації, право на приватність, бази даних, конфіденційна інформація, політика конфіденційності, чутливі персональні дані, право на забуття, цифрове середовище, цифрові права.

Samahalska Y. Personal data protection in the Internet.

A personal daily communication is connected with giving and receiving a large amount of information. A common visit to a website can provide its owner with information about its users (cookies). A registration will provide the owner with a confidential information. In this view, it became necessary to protect a person and to regulate a separate subtype of such information called "personal data".

The concept of "personal data" is not new for Ukraine. The Law "On Protection of Personal Data" was adopted in 2010, however, the practice of its realization shows that the subjects of relations related to personal data interpret it quite superficially. Thus, the owners and managers of personal data formally,

without specifying the purpose and method of processing, notify the subject of personal data that his personal data will be processed. And the subjects of personal data give such consent without reading the procedure for personal data processing or the privacy policy. The probability that the personal database will be deleted after the termination of the legal relationship by the owner or manager is quite small. Due to inappropriate protection and control personal database are constant objects of leaks and thefts, which turn to other crimes, especially on the Internet.

The article pays special attention to the research about the collection of personal data on the websites of Ukrainian political parties, because such personal data are sensitive and their processing should be carried out especially carefully. The leakage of personal data supporters of a certain political force may pose a physical danger to them in martial law conditions.

The author concludes it is necessary to bring the national legislation on protection of personal data to the requirements of the General Data Protection Regulation and to strengthen the control over its compliance by increasing responsibility for violations of the legislation on the protection of personal data.

Key words: information, information protection, right to privacy, database, confidential information, privacy policy, sensitive personal data, right to be forgotten, digital environment, digital rights.

Постановка проблеми. Національне законодавство України про захист персональних даних вважається доволі прогресивним та декларує європейське розуміння необхідності захисту персональних даних, закріплює всі основні вимоги та гарантії захисту суб'єктів відносин, пов'язаних із персональними даними. Не зважаючи на це, дослідження зазначених правовідносин дозволяє прийти до висновку про постійне порушення чинного законодавства та неусвідомлення їх суб'єктами всіх ризиків, які з цими порушеннями пов'язані, особливо в контексті цифрової безпеки громадян під час війни.

Стан опрацювання. Велика кількість українських вчених приділяла увагу проблематиці захисту персональних даних, особливо в час прийняття відповідного законодавства в Україні (2010–2012) та оновлення європейського підходу після прийняття Генерального регламенту (2016–2018). Серед них І.В. Арістова, О.І. Брель, В.П. Радкевич, Н.В. Семчук, В.І. Теремецький, А.М. Чернобай, М.Я. Швець та інші. Та в правовій доктрині досі бракує досліджень, пов'язаних з практикою застосування законодавства про захист персональних даних.

Метою статті є аналіз чинного законодавства про захист персональних даних на відповідність європейським стандартам та його практичне застосування на прикладі збору персональних даних українськими політичними партіями та комерційними платформами в мережі Інтернет.

Виклад основного матеріалу. Відповідно до Закону України «Про захист персональних даних» [1] від 1 червня 2010 року персональні дані – це відомості чи сукупність відомостей про фізичну особу, яка ідентифікована або може бути конкретно ідентифікована. В розумінні законодавця це будь-яка інформація, що дозволяє ідентифікувати конкретну людину (наприклад, номер телефону чи фотографія). Такий підхід відповідає європейському щодо даних про особу, закріпленому в Конвенції Ради Європи про захист осіб у зв'язку з автоматизованою обробкою персональних даних від 1981 року та Загальному регламенту про захист даних ЄС [2] від 2018 року, на які Україна рівняється відповідно до Плану заходів КМУ з виконання Угоди про Асоціацію між Україною, з однієї сторони, та Європейським Союзом, Європейським співтовариством з атомної енергії і їхніми державами-членами, з іншої сторони від 25 жовтня 2017 року.

Закон зобов'язує всіх осіб, які мають справу з персональними даними, обробляти їх лише з конкретно визначеною метою за згодою фізичних осіб та в порядку, що прямо встановлений в Законі. Володільці, розпорядники персональних даних та треті особи зобов'язані забезпечити захист цих даних від випадкових втрати або знищення, від незаконної обробки, у тому числі незаконного знищення чи доступу до персональних даних.

На виконання цього Закону володільці повинні розробити та впроваджувати власну політику приватності щодо персональних даних фізичних осіб. Вона закріплюється переважно в положеннях чи інших локальних документах, які регулюють діяльність володільця персональних даних.

Уповноважений Верховної Ради України з прав людини, як орган, що уповноважений здійснювати контроль за додержанням законодавства про захист персональних даних, своїм Наказом затвердив Типовий порядок обробки персональних даних від 08.01.2014 року, який має слугувати орієнтиром суб'єктам відносин, пов'язаних із персональними даними.

Спершу володілець має визначитись, які відомості, що становлять персональні дані, необхідні відповідній особі з огляду на мету її діяльності. Закон вказує, що склад та зміст персональних даних мають бути відповідними, адекватними та ненадмірними стосовно визначеної мети їх обробки не довше, ніж це необхідно для законних цілей, у яких вони збиралися або надалі оброблялися, а отже визначення строку обробки персональних даних є обов'язковим.

Володілець персональних даних також зобов'язаний визначити порядок обробки персональних даних, а саме: спосіб збору, накопичення персональних даних; умови зберігання персональних даних; умови та процедуру зміни, видалення або знищення персональних даних; умови та процедуру передачі персональних даних та перелік третіх осіб, яким можуть передаватися персональні дані; порядок доступу до персональних даних осіб, які здійснюють обробку, а також суб'єктів персональних даних; заходи забезпечення захисту персональних даних; процедуру збереження інформації про операції, пов'язані з обробкою персональних даних та доступом до них.

В положенні про порядок обробки персональних даних повинні міститися ті організаційні заходи, які володілець здійснюватиме для збирання, використання та захисту персональних даних. Це: визначення порядку доступу до персональних даних уповноважених осіб у володільця/розпорядника; визначення порядку ведення обліку операцій, пов'язаних з обробкою персональних даних суб'єкта та доступом до них; розробку плану дій на випадок несанкціонованого доступу до персональних даних, пошкодження технічного обладнання, виникнення надзвичайних ситуацій; регулярне навчання співробітників, які працюють з персональними даними тощо.

Варто звернути увагу, що у володільця чи розпорядника персональних даних має вестись облік працівників, які мають доступ до персональних даних, та визначатись рівень доступу зазначених працівників до цих персональних даних. Кожен із цих працівників користується доступом лише до тих персональних даних (їх частини), які необхідні йому у зв'язку з виконанням своїх професійних чи службових або трудових обов'язків. Вони дають письмове зобов'язання про нерозголошення персональних даних, які їм було довірено, або які стали їм відомі у зв'язку з виконанням професійних чи службових або трудових обов'язків. У разі звільнення працівника, який мав доступ до персональних даних, або переведення його на іншу посаду, що не передбачає роботу з персональними даними, вживаються заходи щодо унеможливлення доступу такої особи до персональних даних, а документи та інші носії, що містять персональні дані, передаються іншому працівнику.

Важливо зазначити, що Закон вимагає, щоб згода суб'єкта персональних даних на їх обробку повинна бути добровільною та інформованою. Згода може надаватися суб'єктом у письмовій або електронній формі, що дає змогу зробити висновок про її надання. Вона може бути передбачена окремим пунктом договору, що укладається з фізичною особою, або ж шляхом поставлення відмітки під час реєстрації в інформаційно-телекомунікаційній системі. Документи (інформація), що підтверджують надання суб'єктом згоди на обробку його персональних даних, зберігаються володільцем впродовж часу обробки таких даних.

Також Закон передбачає, що у разі зміни визначеної мети обробки персональних даних на нову мету, яка є несумісною з попередньою, для подальшої обробки даних володілець персональних даних повинен отримати згоду суб'єкта персональних даних на обробку його даних відповідно до зміненої мети, якщо інше не передбачено Законом.

Варто звернути увагу, що Загальний регламент вимогливіше ставить питання про надання згоди на обробку персональних даних, яку необхідно надавати шляхом чіткого ствердження, адже мовчання, автоматичне заповнення клітинок позначками або бездіяльність не сприймаються як надання згоди. Згода повинна поширюватися на всі види опрацювання даних, що здійснюють для однакової цілі або цілей. У разі, якщо опрацювання передбачає досягнення множинних цілей, згода потрібна для кожної з них. Суб'єкти персональних даних мають бути ознайомленими з обов'язками та відповідальністю контролера щодо будь-якого опрацювання персональних даних, яке здійснює контролер, або яке здійснюють від імені контролера.

Важливою гарантією захисту суб'єкта персональних даних відповідно до Генерального регламенту є запровадження права бути забутим. Так, суб'єкт даних повинен мати право на видалення своїх персональних даних та припинення їхнього опрацювання, якщо персональні дані більше не є потрібними щодо цілей, для яких їх збирають або іншим чином опрацьовують, якщо суб'єкт даних відкликав свою згоду або заперечує проти опрацювання його персональних даних, або якщо опрацювання його персональних даних іншим чином не відповідає цьому Регламенту (наприклад,

коли суб'єкт даних надав свою згоду, будучи дитиною, та не є повністю обізнаним про ризики, пов'язані з опрацюванням, а пізніше хоче видалити такі персональні дані, особливо з мережі Інтернет). У разі, коли суб'єкт персональних даних відкликає свої дані або ж строк їх обробки закінчився, то контролер повинен забезпечити видалення персональних даних, що були наданні для обробки. Відкликати згоду має бути так само просто, як і надати.

Варто зазначити, що хоча саме поняття «право на забуття» не використовується в національному Законі, та фактично законодавець забезпечує таке право закріпивши можливість суб'єкту персональних даних відкликати згоду на обробку персональних даних, пред'являти вмотивовану вимогу володільцю персональних даних із запереченням проти обробки своїх персональних даних або щодо зміни або знищення своїх персональних даних будь-яким володільцем та розпорядником персональних даних, якщо ці дані обробляються незаконно чи є недостовірними. Також персональні дані повинні бути видалені або знищені у разі: закінчення строку зберігання даних; припинення правовідносин між суб'єктом персональних даних та володільцем чи розпорядником; за рішенням суду чи Уповноваженого з прав людини.

За порушення законодавства щодо захисту персональних даних передбачена відповідальність. Зокрема, адміністративна та цивільна відповідальність, яка не надто лякає володільців та розпорядників персональних даних. Уповноважений з прав людини має проводити на підставі звернень або за власною ініціативою виїзні та безвиїзні, планові, позапланові перевірки володільців або розпорядників персональних даних в порядку, проте кількість проведених ним заходів є недостатньою задля зміни сприйняття захисту персональних даних з формального на реальну необхідність.

Ще одним важливим кроком із забезпечення ефективного захисту персональних даних було б проведення більшої кількості освітніх інформаційних заходів, які покликанні покращити обізнаність суб'єктів відносин, пов'язаних із персональними даними. Адже усвідомлення своїх прав, обов'язків, відповідальності, а головне – можливостей для їх реалізації, покращує волю відповідних суб'єктів дотримуватись чинного законодавства.

Окрім великих сум штрафів за порушення важливою новелою Загального регламенту, яку варто було б запровадити Україні, є повідомлення суб'єкта персональних даних та відповідального наглядового органу протягом 72 годин про і витік персональних даних з описом наслідків порушення безпеки (для прикладу, я особисто отримувала електронне повідомлення від польського онлайн-магазину про те, що у зв'язку з хакерською атакою для захисту персональних даних необхідно змінити пароль до мого електронного кабінету). Це дає змогу мінімізувати збитки, завдані таким витоком.

З огляду на вищевикладене, можна зробити висновок, що національний Закон «Про захист персональних даних» в цілому відповідає європейському розумінню щодо персональних даних та їх захисту, проте практика його застосування свідчить про декларативність таких норм. Це пов'язано, в першу чергу, з недостатнім контролем та відсутністю постійних прикладів притягнення до відповідальності володільців чи розпорядників персональних даних. Так, представники ГО «Рух ЧЕСНО» провели дослідження щодо обробки персональних даних політичними партіями, політиками, громадськими та благодійними ініціативами в Україні [3] та прийшли до висновку, що вони не дотримуються норм чинного законодавства. Подібні дослідження є дуже важливі, адже українські громадяни переважно не усвідомлюють, які відомості щодо себе вони передають в цифровому середовищі, зокрема в мережі Інтернет, та про наявність в них цифрових прав як таких. До речі, політичні погляди, членство в політичних партіях, матеріальне становище є персональними даними, обробка яких дозволяється чинним Законом лише за особливих умов.

В правовій доктрині такі персональні дані називаються особливими або ж чутливими, оскільки їх розголошення може призвести до дискримінації суб'єкта. В умовах військового стану через російську агресію витік бази даних політичних партій може становити небезпеку для життя і здоров'я її членів та симпатиків. Саме тому, така обробка здійснюється із забезпеченням відповідного захисту релігійною організацією, громадською організацією світоглядної спрямованості, політичною партією або професійною спілкою, що створені відповідно до закону, за умови, що обробка стосується виключно персональних даних членів цих об'єднань або осіб, які підтримують постійні контакти з ними у зв'язку з характером їх діяльності, та персональні дані не передаються третій особі без згоди суб'єктів персональних даних.

В проведеному дослідженні вказується, що абсолютна більшість проаналізованих веб-сайтів використовувала інструменти веб-аналітики, що збирають інформацію про користувачів (на двох

веб-сайтах було зафіксовано використання продуктів для відстеження відвідувачів від російської компанії «Яндекс»), що лише окремі організації на своїх сайтах повідомляли про способи збору та обробки персональних даних користувачів, а ще менше з них передбачали можливість надання згоди на обробку (тільки один раз було зафіксовано право на відкликання такої згоди), хоча більшість закликали до надання своїх персональних даних через реєстрацію, підписку, звернення чи благодійний внесок [3].

Кращою видається ситуація щодо захисту персональних в електронній комерції. Проаналізувавши корпоративні політики глобальних технологічних компаній на веб-сайтах та застосунках можна прийти до висновку, що вони дотримуються вимог чинного законодавства та європейських стандартів щодо захисту персональних даних. Не зважаючи на це в Експертному дослідженні ГО «Інтерньюз-Україна» під назвою «Індекс захисту персональних даних 2023» вказується на потребу мінімізувати збір персональних даних, скоротити строк їх зберігання для дотримання цифрових прав користувачів, а також деталізувати персональні дані та спосіб їх передачі третім особам (чи вони на території України, ЄС, третіх країн) [4].

Висновок. Окрім формального приведення національного законодавства до європейських стандартів, українській державі в особі її контролюючих органів варто було приділити більше уваги правореалізації, оскільки більшість володільців та розпорядників персональних даних не усвідомлюють тих ризиків, які можуть бути пов'язаними з їх розголошенням. Суб'єктам персональних даних, в свою чергу, необхідно більш виважено надавати згоду на їх обробку, попередньо ознайомившись з політикою конфіденційності відповідного володільця чи розпорядника.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. Про захист персональних даних : Закон України від 01 червня 2010 р. № 2297-VI / Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/2297-17?find=1&text=%D1%81%D1%82%D1% 80%D0% BE% D0% BA#n25 (дата звернення: 15.04.2024).
2. Про захист фізичних осіб у зв'язку з опрацюванням персональних даних і про вільний рух таких даних та про скасування Директиви 95/46/ЄС: Регламент (ЄС) від 27 квітня 2016 р. № 2016/679 / Європейський Парламент і Рада ЄС. URL: https://zakon.rada.gov.ua/laws/show/984_008-16#Text (дата звернення: 15.04.2024).
3. Богданова Т. Персональні дані в Україні: війна, безпека і політика : Дослідження проведено ГО «Рух ЧЕСНО» за підтримки Міжнародної фундації виборчих систем (IFES). Київ, 2024. URL: https://www.chesno.org/post/5909/.
4. Авдєєва Т., Волкова Л., Мороз В., Бєлоусов П., Правдиченко А. Індекс захисту персональних даних 2023. Експертне дослідження ГО «Інтерньюз-Україна» у межах проєкту «Актуалізація конфіденційності у цифровій сфері в Україні» за підтримки ABA ROLI Ukraine / Rule of Law Initiative. 2023. URL: https://uadigital.report/about.html.