УДК 347.78.01
DOI https://doi.org/10.32782/2524-0374/2024-9/26

ЗАХИСТ ПЕРСОНАЛЬНИХ ДАНИХ У ЦИФРОВОМУ СЕРЕДОВИЩІ: ДОСВІД ЄС

PROTECTION OF PERSONAL DATA IN THE DIGITAL ENVIRONMENT: EU EXPERIENCE

Яворська О.С., д.ю.н., професор,
завідувач кафедри інтелектуальної власності, інформаційного та корпоративного права
Львівський національний університет імені Івана Франка

Стаття присвячена дослідженню захисту персональних даних у цифровому середовищі в ЄС. У роботі розглядаються основні права суб'єктів даних, зокрема: право на доступ до персональних даних, право на виправлення, право на видалення (право на забуття), право на обмеження опрацювання, право на перенесення даних та право на заперечення проти обробки. Загальний регламент про захист даних встановлює суворі правила для обробки персональних даних та передбачає значні штрафи за порушення цих правил. Проте через відсутність універсальних стандартів передачі даних, колізії між різними юрисдикціями та законодавчі обмеження, пов'язані із захистом прав інших осіб, реалізація деяких прав досягається не повною мірою. Наприклад, реалізація права на мобільність даних може бути ускладнена через технічну несумісність систем або відсутність належних механізмів для передачі даних між контролерами. Також обґрунтовано, що ще однією проблемою реалізації прав суб'єктів є складність у знаходженні балансу між правом особи та правами інших. Це стосується права на видалення даних, оскільки є небезпека зловживання ним з боку як суб'єктів даних, так і держав, що може призводити до обмеження свободи слова та цензурування Інтернету.

Проаналізовано, що європейські регулятори продовжують вдосконалювати механізми захисту персональних даних, пропонуючи нові рекомендації та інструменти для забезпечення відповідності Регламенту. Однак на практиці технічні складнощі та небажання деяких компаній втрачати прибуток залишаються значними перешкодами для надійного захисту персональних даних.

Україна, як кандидат на членство ЄС, взяла на себе зобов'язання гармонізувати та адаптувати національне законодавство до права ЄС. Це передбачає впровадження в майбутньому правил, встановлених європейськими регуляторами у сфері захисту даних. Доведено, що вже зараз дотримання встановлених Регламентом правил є важливим для багатьох українських компаній, адже його дія поширюється на всіх контролерів, які обробляють персональні дані громадян ЄС. Недотримання стандартів захисту персональних даних може призвести до фінансових та репутаційних втрат.

Ключові слова: захист персональних даних, право ЄС, право на забуття, право на доступ, право на мобільність даних.

The article is devoted to the study of personal data protection in the digital environment in the EU. The paper examines the fundamental rights of data subjects, including the right of access by the data subject, right to rectification, the right to erasure (right to be forgotten), right to restriction of processing, the right to data portability, and the right to object to processing. The General Data Protection Regulation (GDPR) sets strict rules for the processing of personal data and imposes significant fines for violations of these rules. However, due to the absence of universal standards for data transfer, conflicts between different jurisdictions, and legal limitations related to the protection of other individuals' rights, the realization of certain rights is not fully achieved. For example, the implementation of the right to data portability may be complicated due to technical incompatibility between systems or the lack of proper mechanisms for data transfer between controllers. It is also substantiated that another problem in realizing data subjects' rights is the difficulty of balancing individual rights with the rights of others. This is particularly relevant for the right to erasure, as there is a risk of abuse by both data subjects and states, which could lead to restrictions on freedom of speech and internet censorship.

It has been analyzed that European regulators continue to improve mechanisms for personal data protection, offering new recommendations and tools to ensure compliance with the GDPR. However, in practice, technical challenges and the reluctance of some companies to lose profits remain significant obstacles to reliable personal data protection.

Ukraine, as an EU candidate, has committed to harmonizing and adapting its national legislation to EU law. This includes the future implementation of rules established by European regulators in the field of data protection. It has been proven that compliance with GDPR data subject rights is already important for many Ukrainian companies, as the regulation applies to all controllers processing the personal data of EU citizens. Non-compliance with personal data protection standards may lead to financial and reputational risks.

Key words: personal data protection, digital rights, EU law, right to be forgotten, right to access, right to data portability.

Виклад основного матеріалу. Захист персональних даних є одним з ключових компонентів забезпечення приватності та безпеки людини у цифрову епоху. Європейський Союз (далі – ЄС) намагається максимально захистити суб'єкта даних, розробивши ефективну правову базу для регулювання обробки інформації про особу. Основним нормативно-правовим актом у цій сфері є Загальний регламент про захист даних (далі – Регламент), який набув чинності 25 травня 2018 року [1, ст. 13]. Запропоновані у ньому підходи правового регулювання отримали як позитивні, так і негативні відгуки від юристів та науковців з усього світу. Загалом слід зазначити, що цей документ встановлює високі стандарти захисту персональних даних, достатньо чіткі правила для компаній та організацій щодо обробки особистої інформації та суттєві обмеження, відповідальність для тих, хто не дотримується вимог щодо захисту даних, включаючи значні штрафи, що стимулює бізнес-структури ретельно виконувати вимоги [2].

Відповідно до глави 3 Регламенту за суб'єктами даних закріплюються такі права, як право на доступ до своїх персональних даних (ст. 15), право на виправлення недостовірних даних (ст. 16), право на видалення даних (право на забуття) (ст. 17), право на обмеження опрацювання (ст. 18), право на мобільність даних (ст. 20), право на заперечення проти обробки даних (ст. 21). На практиці вони мають фіксуватися у політиках приватності та безпеки компанії та відображатися у всіх процесах її діяльності [3].

Право на доступ до персональних даних є одним із ключових прав суб'єкта даних. Воно реалізується шляхом подання запиту, за допомогою якого суб'єкт даних може отримати від контролера підтвердження факту обробки своїх персональних даних і, у випадку підтвердження, – доступ до цих даних. Право на доступ також включає отримання інформації про цілі обробки; категорію таких даних; одержувача, якому дані були або будуть розкриті; період, протягом якого передбачається, що такі відомості будуть зберігатись (чи критерії визначення такого періоду); інформацію про походження даних, якщо вони не були зібрані від самого суб'єкта даних; існування автоматизованого вироблення й ухвалення рішень, у тому числі профайлінгу тощо. Регламент не обмежує контролера у формі відповіді на запит. Зазвичай інформація повідомляється контролеру у письмовій формі в тому числі за необхідності, електронними засобами. Проте допускається й усне повідомлення, «за умови, що особу суб'єкта даних доведено іншими засобами» [4]. Якщо

дані знаходяться у процесі опрацювання контролер повинен надати їх копію. Потрібно пам'ятати, що за повторне надання копій контролер може «стягувати розумну плату» [4], що ґрунтується на адміністративних витратах. Стандартний час очікування відповіді на запит – один місяць. Однак, залежно від складності запиту або кількості запитів, контролер може продовжити цей термін до трьох місяців, повідомивши про це суб'єкта даних протягом місяця.

Згідно зі статтею 20 Регламенту у суб'єкта даних також є право отримати свої персональні дані, які вони надали контролеру, у структурованому, загальновживаному та машиночитному форматі. Особа може скористатися такою можливістю за умови, що ці дані оброблялися саме автоматизованими засобами на підставі згоди або договору.

Основна мета права на мобільність даних – це дозволити користувачу легко змінювати постачальників послуг, одночасно зберігаючи історію своїх даних. Така практика покликана зменшити кількість монополій на ринку та сприяти розвитку конкуренції між контролерами. Звичайно, при передачі даних іншій компанії чи сервісу, все ще зустрічається ряд технічних і юридичних перешкод:

– юридичні перепони, що пов'язані з захистом прав інших осіб,

– відсутність чітких стандартів для передачі;

– невизначеність у правах та обов'язках щодо обробки даних між контролерами;

– відсутність уніфікованих технічних рішень для забезпечення семантичної та технічної сумісності.

Окрім того, варто пам'ятати, що це право поширюється лише на персональні дані суб'єкта, а не на всі дані, що були згенеровані у процесі взаємодії з сервісами або обробки даних. Таким чином як зазначає Барбара да Роза Лазаротто «сфера застосування все ще є проблематичною через контекстуальний та мінливий характер персональних даних» [5].Однак, закріплення такого нового права сприяє зміні ринкових умов на такі, що більш якісно захищають дані користувачів, а Закон про цифрові ринки (DMA) та Закон про дані розширюють право на перенесення даних обмежуючи влив великих платформ.

Регламент закріплює за суб'єктом право в будь-який час заперечувати проти обробки своїх даних. Особі достатньо у будь-якій формі звернутися безпосередньо до контролера даних такою вимогою [6]. Підставами для відмови може бути: доведення контролером «наявності істотних законних підстав для опрацювання, що переважають над інтересами, правами та свободами суб'єкта даних» [4], обробка даних для цілей захисту правових претензій чи виконання завдання на підставах суспільного інтересу.

Через швидше накопичення інформації у цифровому середовищі та її доступність користувачі потребують інструментів впливу на дані про себе. Право на виправлення недостовірних даних та право на забуття покликані допомогти суб'єктам даних більшою мірою контролювати загальнодоступну інформацію про себе.

Право на виправлення дозволяє особі виправити неправильну, недостовірну інформацію про неї та у разі потреби додати відсутні відомості. Воно тісно пов'язане з обов'язком контролерів забезпечувати точність, актуальність персональних даних і без затримки видаляти або виправляти, якщо вони є неточними (ст. 5(1(д)) [4]. Суб'єкт даних може реалізувати своє право на виправлення, надіславши повідомлення безпосередньо контролеру. Контролер, своєю чергою, зобов'язаний повідомити всіх одержувачів персональних даних про внесені зміни, за винятком випадків, коли це вимагає непропорційних зусиль або є неможливим. Проте фактично суб'єкти даних часто стикаються зі складнощами у процесі виправлення, адже частина інформації може мати суб'єктивний характер, що ускладнює доведення її недостовірності. Контролер може відмовити у виконанні запиту, якщо він необґрунтований чи надмірний. До прикладу, особа робить запит, але потім пропонує відкликати його в обмін на певну вигоду від контролера чи у випадку коли особа систематично надсилає контролеру різні запити з наміром спричинити перешкоди. У таких випадках важливо, щоб контролер у межах часу на відповідь (без невиправданої затримки та не пізніше ніж протягом одного місяця після отримання запиту за звичайних умов) повідомив суб'єкта даних про причини відмови.

Регламентом закріплене також досить нове та дискусійне «право на забуття». Воно полягає у можливості особи звернутися з вимогою про видалення або анонімізацію персональних даних до контролера за наявності хоча б однієї з таких шести підстав [7]: персональні дані більше не потрібні для первісної цілі обробки; персональні дані опрацьовували незаконно; суб'єкт даних відкликає згоду на опрацювання; суб'єкт даних заперечує проти опрацювання; персональні дані необхідно стерти для дотримання встановленого законом зобов'язання; дані збирали у зв'язку з пропонуванням послуг інформаційного суспільства безпосередньо дитині. Зауважуємо, що поки практика реалізації цього права стикається з низкою юридичних та технічних проблем. Зокрема, експерти виділяють такі [8]:

– конфлікт права на видалення з іншими правами людини (правом на інформацію, на свободу слова);

– юридичні колізії між юрисдикціями при відсутності кордонів для цифрового середовища (ці фактори роблять геоблокування недостатньо дієвим інструментом);

– ризик зловживання правом на видалення з боку не демократичних країн.

Менш радикальним методом обмеження доступності персональних даних в мережі Інтернет є реалізація права на обмеження опрацювання. Воно як і право на видалення та право на виправлення не є абсолютним і полягає у можливості звернення до контролера з вимогою лише зберігати, але не обробляти дані, окрім випадків, передбачених законом. Право на обмеження доступності даних часто реалізується паралельно з іншими правами. Наприклад, на час очікування проведення перевірки щодо точності даних чи переважання законних підстав контролера даних над законними інтересами суб'єкта даних. Відтак, це важливий механізм для захисту суб'єкта даних, що дає змогу тимчасово призупинити подальшу обробку персональних даних до вирішення спірних питань.

Дотримання встановлених Регламентом прав суб'єктів даних може бути важливим і для українських компаній. Багато українських компаній вже працюють або планують виходити на європейський ринок. Для уникнення штрафів та інших негативних наслідків для бізнесу їм важливо дотримуватися правил збору та обробки персональних даних, прав суб'єктів даних – громадян ЄС [9]. Доцільно зауважити, що дотримання Регламенту обов'язкове і для компаній, які ведуть бізнес в Україні, але мають серед своїх клієнтів резидентів Євросоюзу. Наприклад, це актуально для розробників застосунків, які доступні для завантажування у країнах ЄС або для українських банків, що відкривають рахунки громадянам ЄС.

Принагідно варто звернути увагу, що Україна також поступово робить кроки до приведення законодавства про захист персональних даних у відповідність до права ЄС [10]. Так, у лютому 2024 року Верховна Рада відновила розгляд законопроєкту про захист персональних даних № 8153 від 25 жовтня 2022 року [11]. Цей законопроєкт було включено до порядку денного парламенту, і наразі триває його неофіційне громадське обговорення [9].

Висновки. Захист персональних даних є важливою частиною захисту приватності у цифрову епоху. Європейський Союз намагається оперативно реагувати на технічний прогрес, адаптуючи своє законодавство, щоб ефективно регулювати нові виклики у сфері захисту даних. Загальний

регламент про захист даних встановив стандарти захисту даних, поклавши на контролерів досить великий обсяг зобов'язань. Одним із ключових досягнень цього документу стало закріплення таких нових прав для суб'єктів даних, як право на забуття та право на мобільність даних. Ці права спрямовані на надання людям можливості контролювати власну інформацію та обмежувати її використання третіми сторонами. Водночас реалізація багатьох прав стикається з технічними і юридичними перешкодами, зокрема через відсутність універсальних стандартів передачі даних, ризики правових колізій між різними юрисдикціями. Також існує небезпека перетворення деяких прав суб'єктів даних на інструменти маніпуляції для обмеження свободи слова чи доступу до інформації.

Зважаючи на євроінтеграційні процеси досвід ЄС у сфері захисту персональних даних є важливим орієнтиром для України. Для українських компаній, які працюють з резидентами ЄС, або мають намір виходити на європейський ринок, дотримання вимог Регламенту є необхідною умовою для уникнення значних штрафів та репутаційних ризиків. Таким чином, впровадження європейських стандартів захисту даних допоможе українським компаніям уникнути юридичних перешкод у співпраці з європейськими партнерами та розширить можливості для міжнародного розвитку бізнесу. Окрім економічних вигод, впровадження стандартів Регламенту підвищить рівень захисту прав українських громадян у цифровому просторі, що є важливим елементом підвищення інформаційної безпеки країни.

ЛІТЕРАТУРА

1. Бем М., Городиський І. Захист персональних даних: правове регулювання та практичні аспекти: науково-практичний посібник.2021.С.13 URL: https://shorturl.at/t65CF (дата звернення 27.09.2024).

2. Дем'янець В. GDPR або General Data Protection Regulation. Тренди 2022. 2022. URL: https://legalitgroup.com/gdpr-novi-eu-tendentsii/ (дата звернення 27.09.2024).

3. Шадська У. Захист персональних даних за правилами GDPR. Експертний центр з прав людини. URL: https://ecpl.com.ua/news/zakhyst-personal-nykh-danykh-za-pravylamy-gdpr/(дата звернення: 25.09.2024).

4. Загальний регламент про захист даних (GDPR). GDPR TEXT. URL: https://gdpr-text.com/uk/ (дата звернення: 25.09.2024).

5. Lazarotto B. The right to data portability: A holistic analysis of GDPR, DMA and the Data Act. European Journal of Law and Technology (EJLT). 2024. URL: https://ejlt.org/index.php/ejlt/article/view/988 (дата звернення: 27.09.2024).

6. The right to object to the use of your data. Information Commissioner's Office. URL: https://ico.org.uk/for-the-public/the-right-to-object-to-the-use-of-your-data/ (дата звернення 27.09.2024).

7. Кіріяк О.В. Право на забуття: як не забути про головне. Право на забуття: зб. ст. за ред. І.В. Спасибо-Фатєєвої. Харків. ЕКУС. 2021. С. 15-24.

8. Andreas von Arnauld, Kerstin von der Decken, Mart Susi. The Cambridge Handbook of New Human Rights. Recognition, Novelty, Rhetoric. Cambridge University Press. Part IV – New Technology Rights. 2020. URL: https://www.cambridge.org/core/books/abs/cambridge-handbook-of-new-human-rights/right-to-be-forgotten/EF35C0E8438CE6A0445406E6EE1C5CF7 (дата звернення: 27.09.2024).

9. Штрафи за порушення законодавства про захист персональних даних у розмірах наближених до GDDR? Що очікувати фізичним та юридичним особам в Україні від Законопроєкту про захист персональних даних? Sayenko Kharenko. 2024. URL: https://shorturl.at/DSssV (дата звернення: 21.09.2024).

10. Мала Ю. Правила GDPR: як українським компаніям обробляти персональні дані громадян ЄС. Stalirov&Co. 2023. URL: https://stalirov.lawyer/uk (дата звернення: 25.09.2024).

11. Про захист персональних даних. Проект Закону від 25.10.2022. № 8153. URL: https://itd.rada.gov.ua/billInfo/Bills/Card/40707(дата звернення: 21.09.2024).