РОЗДІЛ 4
ГОСПОДАРСЬКЕ ПРАВО, ГОСПОДАРСЬКО-ПРОЦЕСУАЛЬНЕ ПРАВО

УДК 342.9:004.738.5(4-6ЄС)
DOI https://doi.org/10.32782/2524-0374/2024-8/32

ПРАВОВЕ РЕГУЛЮВАННЯ КОНФІДЕНЦІЙНОСТІ ДАНИХ У ЄВРОПЕЙСЬКОМУ СОЮЗІ: ВПЛИВ НА ОНЛАЙН ТОРГІВЛЮ

LEGAL REGULATION OF DATA PRIVACY IN THE EUROPEAN UNION: IMPACT ON ONLINE TRADE

Волинець В.В., д.ю.н.,
професор кафедри готельно-ресторанної справи
Київський університет туризму економіки і права

Стаття присвячується правовому регулювання конфіденційності даних у Європейському Союзі, зокрема впливу на онлайн торгівлю. Онлайн торгівля – це процес купівлі та продажу товарів і послуг через Інтернет, що включає в себе електронні платформи, інтернет-магазини та інші цифрові канали для здійснення комерційних угод. Необхідність в дослідженні обраної теми зумовлена розвитком онлайн торгівлі, яка нерозривно пов'язана із цифровізацією. Збільшення обсягів економічного зростання формує нові можливості для підприємств, допомагаючи їм ефективніше взаємодіяти зі споживачами, зокрема і в онлайн секторі. Це призводить до підвищення продуктивності праці, зниження витрат та розширення доступу до ринків та інформації. Водночас, швидка цифровізація супроводжується підсиленими викликами, пов'язаними із захистом конфіденційності даних. Зважаючи на це, актуальність дослідження правового регулювання конфіденційності даних у Європейському Союзі та його впливу на онлайн торгівлю підсилюється, оскільки все більше персональних даних обробляється та зберігається в цифровому середовищі, а тому потреба у забезпеченні їх захисту стає вкрай необхідною.

Зважаючи на це, дослідження правового регулювання конфіденційності даних у ЄС та його впливу на онлайн торгівлю необхідне, оскільки сфера онлайн бізнесу буде розвиватися і надалі. У зв'язку з цим виникає гостра необхідність у регулюванні питань, пов'язаних із захистом персональних даних та їх збереженням. Обраний вектор дослідження сприятиме узагальненню існуючих нормативних актів ЄС щодо захисту персональних даних, а також розробці нових правових елементів, які можуть впроваджуватися в законодавство ЄС, на зміну існуючим. Це дозволить не лише покращити рівень захисту персональних даних, але й підвищити довіру споживачів до онлайн платформ та сервісів. Загалом доцільність встановлення ефективного правового регулювання сприятиме створенню сприятливих умов для розвитку онлайн торгівлі, забезпечення балансу між інноваціями та безпекою. Дослідження цього питання є важливим для забезпечення стійкого розвитку цифрової економіки та захисту прав громадян у сфері онлайн торгівлі в Європейському Союзі.

Ключові слова: конфіденційність даних, онлайн торгівля, законодавство ЄС, онлайн торгівля, персональні дані.

The article is devoted to the legal regulation of data privacy in the European Union, in particular the impact on online trade. Online commerce is the process of buying and selling goods and services over the Internet, which includes electronic platforms, online stores and other digital channels for conducting commercial transactions. The need to study the chosen topic is due to the development of online trade, which is inextricably linked to digitalization. Increasing economic growth creates new opportunities for businesses, helping them interact more effectively with consumers, particularly in the online sector. This leads to increased productivity, lower costs and increased access to markets and information. At the same time, rapid digitalization is accompanied by increased challenges related to the protection of data privacy. With this in mind, the relevance of the study of the legal regulation of data privacy in the European Union and its impact on online commerce is enhanced, as more and more personal data is processed and stored in the digital environment, and therefore the need to ensure its protection becomes imperative.

With this in mind, research into EU data privacy legal regulation and its impact on online commerce is necessary, as the field of online business will continue to grow. In this regard, there is an urgent need to regulate issues related to the protection of personal data and their preservation. The selected research vector will contribute to the generalization of existing EU regulations on personal data protection, as well as the development of new legal elements that can be introduced into EU legislation, replacing the existing ones. This will not only improve the level of personal data protection, but also increase consumer trust in online platforms and services. In general, the feasibility of establishing effective legal regulation will contribute to the creation of favorable conditions for the development of online trade, ensuring a balance between innovation and security. The study of this issue is important for ensuring the sustainable development of the digital economy and protecting the rights of citizens in the field of online trade in the European Union.

Key words: data privacy, online trade, EU legislation, online trade, personal data.

Правові стандарти захисту персональних даних є найбільш узагальненими та загальновизнаними на міжнародному рівні фундаментальними правовими засадами у сфері відносин, пов'язаних із персональними даними. Формування європейських стандартів захисту персональних даних відбувалося в рамках діяльності таких організацій, як Рада Європи та Європейський Союз. У результаті співпраці держав у межах цих організацій прийнято низку міжнародних угод, які встановлюють загальні правила захисту прав осіб у зв'язку з обробкою персональних даних на рівні європейського права.

Захищати персональні дані потрібно незалежно від того, в якій сфері вони використовуються. Однією з найбільш важливих осередків, де активно використовуються персональні дані – є електронна комерція. Електронна комерція – це торгова діяльність, яка ґрунтується на отриманні прибутку. Вона формується на основі комплексної автоматизації комерційного циклу за рахунок використання захисту обчислювальної техніки. Електронна комерція здійснюється у сфері обміну електронними даними щодо наступних видів угод: купівля-продаж товарів, постачання, договори про розподіл продукції, агентські відносини, факторинг, лізинг, проектування, консалтинг, інжиніринг, інвестиційні угоди, страхування, договори про експлуатацію та концесії, банківські послуги, спільна діяльність та інші форми ділового співробітництва, транспортні послуги. До електронної комерції відносять і біржові угоди, оскільки вони також передбачають діяльність

із застосуванням мережі Інтернет. Загалом, електронна комерція в мережі Інтернет охоплює досить широке коло відносин, а відтак, передбачає наявність значного обсягу інформації, яка потребує захисту від третіх осіб.

Електронна комерція є частиною електронного бізнесу, найбільш розвиненою і втіленою у життя його формою. На думку фахівців, електронна комерція охоплює суспільні відносини, пов'язані з купівлею-продажем товарів, послуг та інформації через Інтернет, використовуючи всі доступні в мережі інструменти, зокрема Інтернет-рекламу, проведення платежів, замовлення, вирішення правових питань споживачів, організація доставки тощо [13, с. 216].

Досліджуючи питання регулювання конфіденційності даних у Європейському Союзі та їх вплив на електронну комерцію (електронну торгівлю), варто погодитися з думкою А. М. Бойко, який говорить, що захист персональних даних для європейських країн є досить актуальним питанням. Першим документом, який для європейського співтовариства визнав право на захист персональних даних, була Загальна декларація прав людини Організації Об'єднаних Націй (ООН) 1948 р. [6]. Цей документ закріпив право особи на захист від втручання інших у приватне життя, зокрема, зі сторони державних органів та держави [1, с. 97].

Захист персональних даних у країнах ЄС ґрунтується на основоположних принципах, встановлених Загальною декларацією прав людини, а також іншими нормативними актами. Стаття 8(1)Хартії основоположних прав ЄС [12] та стаття 16(1) Договору про функціонування ЄС (ДФЄС) [4] також підтримують право особи на захист своїх персональних даних. Разом з цим, Загальний регламент захисту даних встановлює суворі вимоги щодо збору, обробки, зберігання та передачі персональних даних. Основними принципами Регламенту 2016/679 [9] є законність, справедливість і прозорість, обмеження цілей, мінімізація даних, точність, обмеження зберігання, цілісність і конфіденційність. Відповідно до Регламенту кожна особа має право на захист своїх персональних даних. Захист цих прав має фундаментальний характер. Основний зміст Регламенту спрямовується на сприяння формуванню простору свободи, безпеки і правосуддя, економічного союзу, соціально-економічного розвитку, зміцнення економіки держави на внутрішньому ринку, а також сприяння добробуту фізичних осіб [9].

Сучасним нормативно-правовим актом у сфері захисту персональних даних є нормативно-правовий акт, прийнятий 25 травня 2018 року – Загальний Регламент Захисту Даних (General Data Protection Regulation). Вказаний документ визначає будь-які дії з персональними даними, їх зберіганням і передачею, а також встановлює міру юридичної відповідальності за недотримання вимог, визначених цим актом [7].

За словами дослідника Д. Скумбрія, вимога забезпечення високого рівня захисту конфіденційної інформації, зокрема персональних даних, є основоположною у Загальному регламенті захисту даних (General Data Protection Regulation, GDPR). Цей регламент забороняє проведення будь-яких операцій з даними резидентів ЄС у країнах, де рівень захисту персональних даних є нижчим, ніж в Європейському Союзі [11].

У зв'язку зі стрімким розвитком і глобалізацією, пов'язаною із виникненням різних секторів економіки, в тому числі й онлайн-торгівлі, масштаби збирання та обробки персональних даних значно зросли. Фізичні особи змушені й далі надавати свої персональні дані, на свій страх і ризик ділитися з ними в мережі Інтернет. Технології продовжують змінювати економіку і суспільство, а суспільне життя й надалі підсилює необхідність у вільному рухові персональних даних у межах ЄС, передавання їх третім країнам та організаціям, дотримуючись при цьому захисту персональних даних. Обробка персональних даних у різних сферах їх застосування повинна бути забезпечена на законодавчому рівні та відповідати правовим нормам. Фізичні особи мають бути проінформовані стосовно того, що їхні персональні дані збираються, використовуються, обговорюються або іншим чином обробляються, а також про те, в якому обсязі ці дані обробляються чи будуть оброблятися. Принцип прозорості вимагає, щоб будь-яка інформація та повідомлення стосовно обробки таких персональних даних були доступними і зрозумілими, використовуючи чіткі і прості формулювання.

Зважаючи на дослідження Р. Еннана, розвиток електронних засобів комунікації спричинив необхідність впровадження електронних підписів і відповідних послуг, пов'язаних із їх правовим оформленням та визнанням. Цей інститут спрямований на усунення існуючих перешкод у використанні електронних комунікацій і електронної торгівлі. Чітке правове регулювання використання електронних підписів сприятиме підвищенню довіри до них і, відповідно, впровадженню нових технологій. Відсутність правового регулювання електронних підписів призводить до нестачі узгодженого понятійного апарату й термінології у цій сфері. Крім того, правова неврегульованість і недостатній захист конфіденційних даних створюють ризики для безпеки особистої інформації, і, як наслідок, може вплинути на ефективність і надійність електронних підписів у ділових операціях [5, с. 89].

Використання електронних цифрових підписів на території ЄС здійснюється на основі Європейського Регламенту eIDAS від 2014 року (Регламент eIDAS) [8]. За словами Ю. Дребезової, Регламент розподіляє підписи на три типи:

1. Простий електронний цифровий підпис (SES) не передбачає надійної автентифікації підписувача чи перевірки особи. Він підходить для підписання простих документів.

2. Удосконалений електронний цифровий підпис (AES) містить додаткові кроки автентифікації користувача, серед яких: підписувача може попросити надати документ для підтвердження своєї особи, пройти біометричну перевірку із використанням унікального коду доступу після процесу підписання. Удосконалений тип цифрового підпису використовується для більш значних правочинів і має вищий рівень захисту, ніж SES. AES підходить для підписання договорів купівлі-продажу, оренди тощо.

3. Кваліфікований цифровий підпис (QES) призначений для складних регульованих операцій. Він має найвищий рівень довіри та захисту. Клієнтів просять електронно ідентифікувати себе під час підписання, підтвердивши ідентифікатор. Цифровий сертифікат, що підтверджує особу, автоматично додається до підпису після перевірки. Цей тип електронного підпису має таку саму юридичну силу, як і власноруч підписаний документ, та може використовуватися для підписання внутрішніх корпоративних документів, подачі звітності тощо [3].

Отже, оскільки електронний цифровий підпис є свідченням згоди людини на певні дії або угоди, його використання має бути максимально безпечним та надійним. Впровадження різних рівнів електронних підписів дозволяє забезпечити належний рівень захисту та відповідність юридичним вимогам. Простий електронний підпис підходить для менш значущих правочинів, тоді як удосконалений та кваліфікований електронні підписи забезпечують більшу безпеку та довіру, особливо для складних корпоративних чи бізнесових операцій. Цей процес гарантує, що цифрові підписи можуть ефективно використовуватися в різних сферах, включаючи бізнес, юридичні та адміністративні процеси. Загалом, електронні підписи сприяють цифровій трансформації, а також полегшують здійснення електронної комерції та інших онлайн-послуг.

Важливою подією для ринку цифрових послуг стало прийняття Закону про цифрові послуги (Digital Services Act (DSA) [10]. Закон про цифрові послуги (Digital

Services Act, DSA) встановлює новий, безпрецедентний стандарт відповідальності онлайн-платформ за незаконний та шкідливий контент. Цей закон має на меті забезпечити кращий захист користувачів Інтернету та їхніх основних прав, одночасно з цим він визначає єдиний набір правил для внутрішнього ринку ЄС. DSA спрямований на підтримку безпечного онлайн-середовища, де користувачі можуть впевнено використовувати цифрові послуги.

Закон про цифрові позлуги зобов'язує платформи швидко реагувати на повідомлення щодо незаконного контенту і видаляти його. Крім того, закон передбачає прозорість алгоритмів, які використовуються платформами, і гарантує, що користувачі мають можливість розуміти, як працюють ці алгоритми. Разом з тим закон включає положення про співпрацю між державами-членами ЄС, дозволяючи ефективніше боротися з незаконним контентом на міжнародному рівні, а також пропонує підтримку для малих та середніх онлайн-платформ, допомагаючи їм дотримуватися нових правил та розширювати свій бізнес. Загалом, закон сприяє інноваціям та підвищує довіру користувачів до цифрових послуг, забезпечуючи захист їхніх прав, конфіденційності даних та безпеку в Інтернеті.

Закон про цифрові послуги встановлює чотири категорії учасників, серед яких:

– компанії, що надають посередницькі послуги онлайн;
– компанії з надання послуг хостингу;
– онлайн-платформи;
– як великі так і не великі онлайн-платформи.

Закон про цифрові послуги має на меті підвищити ефективність механізмів захисту прав користувачів в Інтернеті, створити сприятливі умови для запуску та розширення цифрових послуг стосовно учасників онлайн-ринку в ЄС. Прозорість онлайн-платформ, особливо щодо алгоритмів, які використовуються у сфері реклами, буде значно підвищена. Для запобігання зловживанням зі сторони великих платформ, які охоплюють понад 10% населення ЄС, будуть введені такі заходи, як аудит та звітування. Це допоможе контролювати їхню діяльність та забезпечувати дотримання встановлених правил. Підтримка малого бізнесу та залучення нових учасників на онлайн-ринку є ще однією важливою ціллю закону, що сприятиме конкурентоспроможності та інноваціям, а також створенню безпечного і справедливого цифрового середовища для всіх користувачів.

За словами вітчизняних наковців О. С. Бондаренко та М. О. Думчикова, наразі в ЄС значна увага приділяється кібербезпеці та захисту від кіберзагроз, оскільки загрози кібербезпеці мають транскордонний характер, а самі кібератаки завдають значної шкоди системі захисту даних. Країни ЄС повинні мати сильні державні органи, які б контролювали кібербезпеку, а також співпрацювали зі своїми колегами в інших державах-членах, обмінюючись інформацією. Директива про безпеку мережевих та інформаційних систем (NIS Directive), забезпечує створення та співпрацю державних органів у сфері кіберзахисту. Цю Директиву було переглянуто наприкінці 2020 року і в результаті процесу перегляду 16 грудня 2020 року Комісія представила новий документ – Директиву про заходи для високого загального рівня кібербезпеки в Союзі (Директива NIS2). Директива набула чинності 16 січня 2023 року [2, с. 335].

Наразі проблема захисту конфіденційності даних в ЄС не зникає. З цією метою, зважаючи на ситуацію у сфері кібербезпеки, планується і надалі розробляти правові платформи, які б сприяли захисту від кібератак та втрату конфіденційності даних у всіх секторах суспільного життя, в тому числі й в онлайн торгівлі. Правові аспекти впровадження нових нормативно-правових актів лише підсилять позицію ЄС у сфері захисту даних, дозволяючи формувати потужну протидію кібератакам.

Висновки. Зважаючи на результати проведеного дослідження з'ясовано, що захист конфіденційності даних в ЄС регулюється низкою директив, регламентів та законів. Одним із найпотужніших наразі залишається Регламент 2016/679, який встановлює основні принципи та вимоги щодо обробки персональних даних. Впровадження цього регламенту значно підвищило стандарти захисту даних, забезпечуючи високий рівень прозорості та відповідальності за вчинені злочини у цій сфері. Крім того, нормативні акти, такі як Директива про електронну комерцію та Закон про цифрові послуги, доповнюють GDPR, регулюючи специфічні аспекти обробки даних в онлайн-торгівлі та на цифрових платформах.

Отже, захист конфіденційності даних є критично важливим процесом у сфері онлайн-торгівлі в Європейському Союзі. Забезпечення належного захисту персональних даних підвищує довіру споживачів до цифрових платформ, сприяючи збільшенню обсягу онлайн-транзакцій. Компанії, які дотримуються високих стандартів конфіденційності, отримують конкурентну перевагу, оскільки користувачі надають перевагу безпечним сервісам. Разом з тим, ефективне регулювання і захист даних знижують ризики кіберзлочинності та шахрайства, що значно підсилює стабільність функціонування електронної комерції. Впровадження таких нормативних актів стимулює інновації та розвиток нових технологій, які відповідають високим стандартам захисту даних, сприяючи подальшому розвитку цифрової економіки.

ЛІТЕРАТУРА

1. Бойко А. М. Законодавство Європейського Союзу у сфері захисту персональних даних. *Юридичний науковий електронний журнал. Випуск №4,* 2019. С. 96–99. URL: http://www.lsej.org.ua/4_2019/26.pdf (дата звернення 12.08.2024)

2. Бондаренко О. С., Думчиков М. О. Захист цифрової особистості: вивчення досвіду Європейського Союзу та України. *Юридичний науковий електронний журнал.* Випуск 1, 2021. С. 334–338. URL: http://www.lsej.org.ua/1_2024/77.pdf (дата звернення 13.08.2024)

3. Дребезова Ю. Кваліфікований електронний підпис в ЄС: нові можливості для України. 2023. URL: https://www.juscutum.com/news/kvalifikovaniy-elektronniy-pidpis-v-ies-novi-mozhlivosti-dlya-ukrayinskogo-biznesu (дата звернення 12.08.2024)

4. Договір про функціонування ЄС (ДФЄС). URL: https://zakon.rada.gov.ua/laws/show/994_b06#Text (15.08.2024)

5. Еннан Р. Правовідносини у сфері електронної комерції: досвід Європейського Союзу. *Юридичний вісник.* Випуск 1. 2019. С. 87–92. URL: http://yurvisnyk.in.ua/v1_2019/16.pdf (дата звернення 02.08.2024)

6. Загальна декларація прав людини від 10.12.1948. URL: https://zakon.rada.gov.ua/laws/show/995_015#Text (дата звернення 02.08.2024)

7. Нові вимоги ЄС до захисту персональних даних з травня 2018 року. URL: http://channel4it.com/publications/Nov-vimogi-S-do-zahistupersonalnih-danih-z-travnya-2018-roku-30154.html# (дата звернення 02.08.2024)

8. Регламент Європейського Парламенту і Ради (ЄС) № 910/2014 від 23 липня 2014 року про електронну ідентифікацію та довірчі послуги для електронних транзакцій на внутрішньому ринку та про скасування Директиви 1999/93/ЄС (Регламент eIDAS) URL: https://zakon.rada.gov.ua/laws/show/984_016-14#Text (дата звернення 12.08.2024)

9. Регламент Європейського Парламенту і Ради (ЄС) 2016/679 від 27 квітня 2016 року про захист фізичних осіб у зв'язку з опрацюванням персональних даних і про вільний рух таких даних, та про скасування Директиви 95/46/ЄС (Загальний регламент про захист даних) (General Data Protection Regulation) URL: https://zakon.rada.gov.ua/laws/show/984_008-16#Text (дата звернення 12.08.2024)

10. Регламент (ЄС) 2022/2065 Європейського Парламенту та Ради від 19 жовтня 2022 року про єдиний ринок цифрових послуг і внесення змін до Директиви 2000/31/ЕС (Закон про цифрові послуги) (Digital Services Act (DSA) від 19.10.2022. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32022R2065 (дата звернення 11.08.2024)

11. Скумбрій Д. Не дуже конфіденційна інформація. Захист даних: GDPR та практика ЄСПЛ. *Юридична газета онлайн,* № 23 (753). 2021. URL: https://yur-gazeta.com/dumka-eksperta/ne-duzhe-konfidenciyna-informaciya-zahist-danih-gdpr-ta-praktika-espl.html (дата звернення 12.08.2024)
12. Хартія основоположних прав ЄС. URL: https://ccl.org.ua/posts/2021/11/hartiya-osnovnyh-prav-yevropejskogo-soyuzu (13.08.2024)
13. Юрченко М. М., Костова Н. І. Міжнародно-правове забезпечення електронної комерції в Україні. *Південноукраїнський правничий часопис. Випуск 1-2.* 2022. С. 213–218. URL: http://www.sulj.oduvs.od.ua/archive/2022/1-2/39.pdf (дата звернення 12.08.2024).