ПРИДАТКО Д. О.,
orcid.org/0009-0009-7383-7497
аспірант кафедри цивільно-правових дисциплін
(Навчально-науковий інститут права імені Іоаннікія Малиновського Національного університету «Острозька академія»)

УДК 342.7:004.056
DOI https://doi.org/10.32842/2078-3736/2025.6.38

ПОРІВНЯЛЬНИЙ АНАЛІЗ ПРАВОВОГО РЕГУЛЮВАННЯ ЗАХИСТУ ЧУТЛИВИХ ПЕРСОНАЛЬНИХ ДАНИХ У ЄВРОПЕЙСЬКОМУ СОЮЗІ ТА УКРАЇНІ

У статті здійснено порівняльно-правовий аналіз положень Закону України «Про захист персональних даних» та Регламенту 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 з метою виявлення розбіжностей у правовому регулюванні обробки чутливих персональних даних. Проаналізовано основні принципи, підстави, умови та обмеження щодо обробки таких даних, особливості реалізації прав суб'єктів персональних даних, порядок отримання та відкликання згоди на обробку персональних даних, а також положення про відповідальність за порушення законодавства у цій сфері. Встановлено, що Закон України «Про захист персональних даних» має фрагментарний характер, не містить чітко визначених принципів обробки, вимог до форми та порядку надання згоди суб'єктом даних, не регламентує захист персональних даних дітей і не визначає ефективних механізмів реалізації прав фізичних осіб. Натомість Регламент Європейського Парламенту і Ради про захист фізичних осіб у зв'язку з опрацюванням персональних даних передбачає більш глибоку деталізацію процедур, ширше коло прав суб'єктів персональних даних, чітку систему відповідальності із визначеними розмірами санкцій пропорційними тяжкості порушення. Порівняльний аналіз засвідчив, що ключові розбіжності між українським і європейським законодавством полягають у рівні системності, комплексності, глибині регулювання та практичній орієнтованості норм. Зроблено висновок про необхідність гармонізації національного законодавства з вимогами Загального регламенту про захист даних, запровадження єдиних принципів і механізмів реалізації прав суб'єктів даних, що дозволить підвищити ефективність захисту чутливих персональних даних, зміцнити гарантії права на приватність та сприятиме подальшій євроінтеграції України.

Ключові слова: *персональні дані, чутливі персональні дані, захист даних, права людини, європейські стандарти, право на приватність, конфіденційна інформація.*

Prydatko D. O. Comparative analysis of legal regulation of sensitive personal data protection in the European Union and Ukraine

The article provides a comparative legal analysis of the provisions of the Law of Ukraine 'On the Protection of Personal Data' and Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection

of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC in order to identify differences in the legal regulation of the processing of sensitive personal data. The main principles, grounds, conditions and restrictions on the processing of such data, the specifics of the implementation of the rights of personal data subjects, the procedure for obtaining and withdrawing consent to the processing of personal data, as well as the provisions on liability for violations of legislation in this area are analysed. It has been established that the Law of Ukraine 'On the Protection of Personal Data' is fragmentary in nature, does not contain clearly defined principles of processing, requirements for the form and procedure for obtaining consent from the data subject, does not regulate the protection of children's personal data and does not define effective mechanisms for the exercise of the rights of individuals. In contrast, the Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data provides for more detailed procedures, a wider range of rights for data subjects, and a clear system of liability with defined penalties proportional to the severity of the violation. A comparative analysis showed that the key differences between Ukrainian and European legislation lie in the level of consistency, comprehensiveness, depth of regulation and practical orientation of the norms. It was concluded that there is a need to harmonise national legislation with the requirements of the General Data Protection Regulation, introduce uniform principles and mechanisms for the implementation of data subjects' rights, which will increase the effectiveness of sensitive personal data protection, strengthen privacy guarantees and contribute to Ukraine's further European integration.

Key words: *personal data, sensitive personal data, data protection, human rights, European standards, right to privacy, confidential information.*

Постановка проблеми. Відповідно до статті 15 Угоди про асоціацію між Україною та Європейським Союзом, «сторони домовились співробітничати з метою забезпечення належного рівня захисту персональних даних відповідно до найвищих європейських та міжнародних стандартів, зокрема відповідних документів Ради Європи» [1].

Таким чином, на Україну покладається обов'язок забезпечити належний рівень захисту персональних даних шляхом приведення національного законодавства та правозастосовної практики у відповідність до найвищих європейських стандартів. Особливе значення має орієнтація на документи Ради Європи, що очевидно вказує на відповідність національного законодавства до Регламенту 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 (далі – Регламент). Це означає необхідність імплементації відповідних норм, застосування уніфікованих підходів до обробки та захисту даних, а також гарантування ефективних механізмів контролю й захисту прав суб'єктів персональних даних.

Як слушно зауважують В. Кальченко та В. Ободяк, ключовим нормативним актом у сфері захисту персональних даних в Україні є Закон України «Про захист персональних даних», який було розроблено з урахуванням положень Директиви 95/46/ЄС. Водночас сама Директива 95/46/ЄС нині визнана застарілою та була скасована у зв'язку з прийняттям Регламенту. У результаті чинний український законодавчий акт значною мірою не відповідає сучасним європейським стандартам у сфері захисту персональних даних, що зумовлює потребу в його оновленні та гармонізації з вимогами Регламенту [2].

Відповідно, і регулювання захисту чутливих персональних даних також не відповідає стандартам Регламенту. Українське законодавство не забезпечує належного рівня деталізації та чіткості у визначенні категорій чутливих даних, підставах і процедурах їх обробки, а також у встановленні спеціальних гарантій для суб'єктів таких даних. Це призводить до

прогалин у правозастосовній практиці та ускладнює забезпечення ефективного контролю за діяльністю розпорядників персональних даних.

Зазначене об'єктивно зумовлює гостру необхідність оновлення та гармонізації українського законодавства у сфері захисту персональних даних відповідно до сучасних європейських стандартів. Така гармонізація сприятиме не лише забезпеченню належного рівня гарантій прав фізичних осіб та створенню ефективних механізмів їх реалізації й захисту, але й підвищенню довіри суспільства до державних інституцій і суб'єктів, які здійснюють обробку персональних даних.

Водночас приведення законодавства у відповідність до вимог Регламенту є важливим кроком на шляху європейської інтеграції України, оскільки воно відкриває можливості для тіснішої співпраці з державами-членами ЄС, сприяє розвитку цифрової економіки, формуванню безпечного інформаційного середовища, а в перспективі надає Україні можливість стати повноправним членом Європейського Союзу.

Аналіз попередніх досліджень та публікацій. Проблематика вдосконалення правового регулювання у сфері захисту персональних даних була предметом наукових розвідок таких дослідників, як Я. Котляревський, М. Сірик, М. Дяченко.

У працях О. Легкої, К. Врублевської-Місюни та В. Тичини розглядалися питання захисту персональних даних у межах вітчизняного та міжнародного досвіду, а також аналізувалися міжнародні стандарти охорони інформації про особу, їх зміст і значення для формування уніфікованих підходів у сфері захисту персональних даних.

Питання європейських правових стандартів у сфері захисту персональних даних, а також інтеграцію цих стандартів у національне законодавство досліджувалося О. Різенко та І. Кульчій.

Окремі аспекти забезпечення захисту чутливих персональних даних у зарубіжних правових системах були проаналізовані у працях П. Гуйвана та Є. Кобрусєвої.

Водночас, попри наявність значної кількості наукових напрацювань, питання правового регулювання обробки саме чутливих персональних даних в Україні залишаються недостатньо розробленими. Актуальність даного дослідження зумовлена потребою комплексного осмислення особливостей правового статусу чутливих персональних даних, виявлення прогалин у національному законодавстві та необхідністю його гармонізації з нормами права Європейського Союзу.

Мета дослідження полягає у комплексному аналізі правового регулювання обробки чутливих персональних даних в Україні, виявленні прогалин і недоліків чинного законодавства, порівняно з положеннями Загального регламенту про захист даних.

Виклад основного матеріалу. Європейський Союз сформував один із найдетальніших і найбільш комплексних підходів до регулювання обробки персональних даних, що закріплений у Регламенті. Цей акт має пряму дію на всій території держав-членів ЄС та встановлює уніфіковані правила обробки як звичайних, так і чутливих персональних даних.

Показовим є приклад законодавства Французької Республіки. У статті 6 Закону № 78-17 від 6 січня 1978 року «Про інформаційні технології, файли даних і громадянські свободи», закріплено загальну заборону на обробку даних, що можуть свідчити про расове чи етнічне походження, політичні погляди, релігійні або філософські переконання, членство фізичної особи у професійних спілках, а також генетичних даних, біометричних даних із метою унікальної ідентифікації особи, даних про стан здоров'я, сексуальне життя чи сексуальну орієнтацію. Водночас передбачено винятки з такої заборони, які прямо визначені пунктом 2 статті 9 Регламенту (ЄС) 2016/679 від 27 квітня 2016 року. [3]

Аналогічний підхід простежується і в законодавстві Федеративної Республіки Німеччини. Так, у розділі 22 «Обробка спеціальних категорій персональних даних» Федерального закону про захист даних від 30 червня 2017 року передбачено винятки із загальної заборони обробки чутливих персональних даних, які частково відрізняються від визначених у Регламенті. Водночас сам перелік чутливих персональних даних

у законі прямо не наведено. Натомість законодавець відсилає до визначення, закріпленого у Регламенті [4].

Таким чином, попри певні відмінності у законодавчій техніці та підходах до формулювання норм у державах Європейського Союзу, ключовим орієнтиром для регулювання обробки чутливих персональних даних є саме Регламент.

Як вірно зазначають Котляревський Я., Сірик М., Дяченко М. «Регламент та Закон України «Про захист персональних даних» є нормативно-правовими актами, які доволі вагомо розрізняються між собою, що зумовлено як часом їхнього ухвалення, історичними передумовами, а також власне кількістю держав, для яких застосування цих законодавчих актів є обов'язковим. Порівняно з Законом Регламент урегульовує більший перелік питань, пов'язаних з обробленням персональних даних, має ширшу сферу застосування та глибшу деталізацію абсолютно усіх процесів та процедур щодо персональних даних» [5].

Якщо ж розглядати детальніше, то стаття 6 Закону України «Про захист персональних даних» містить перелік загальних вимог до обробки персональних даних. Зокрема встановлено, що «мета обробки даних персональних даних має бути сформульована в законах, інших нормативно-правових актах, положеннях, установчих чи інших документах, які регулюють діяльність володільця персональних даних, та відповідати законодавству про захист персональних даних, обробка персональних даних здійснюється відкрито і прозоро із застосуванням засобів та у спосіб, що відповідають визначеним цілям такої обробки, персональні дані мають бути точними, достовірними та оновлюватися в міру потреби, визначеної метою їх обробки, склад та зміст персональних даних мають бути відповідними, адекватними та ненадмірними стосовно визначеної мети їх обробки» [6].

Аналізуючи такі вимоги та порівнюючи з нормами Регламенту, можна дійти висновку, що подібні норми містяться у статті 5 Регламенту та є принципами опрацювання персональних даних. Разом з тим, законодавець не назвав дані вимоги саме принципами обробки персональних даних. Такий підхід істотно звужує їх правове значення, оскільки у праві Європейського Союзу принципи виконують роль фундаментальних засад, на яких будується вся система захисту даних, і які застосовуються під час тлумачення та практичного застосування законодавства. Відсутність чіткої категоризації у вигляді принципів у Законі України «Про захист персональних даних» призводить до того, що вони розглядаються як технічні вимоги, а не як універсальні стандарти, обов'язкові для виконання в усіх аспектах обробки.

Сам по собі перелік вимог до обробки персональних даних визначений у законі значною мірою поступається принципам у Регламенті в частині деталізації. Крім вже зазначених спільних норм, принципи Регламенту покладають на осіб, що обробляють персональні дані, обов'язок забезпечувати належних захист персональних даних, що включає в себе захист від несанкціонованого доступу, знищення, втрати, тощо [7].

Глава II Регламенту носить назву «Принципи» і окрім вже окреслених принципів у статті 5 містить ряд деталізованих норм. Стаття 6 Регламенту визначає низку підстав, наявність принаймні однієї з яких робить обробку персональних даних законною. Серед таких підстав виділяють, зокрема, необхідність обробки для виконання договору, виконання юридичних зобов'язань контролера, захист життєво важливих інтересів суб'єкта даних, виконання завдань, що становлять суспільний інтерес або здійснюються у межах державних повноважень, а також обробку на підставі законної згоди суб'єкта даних. Цей перелік встановлює чіткі критерії для оцінки законності обробки та слугує базою для гармонізації практики захисту персональних даних у державах-членах ЄС [7].

Зазначеній статті відповідає стаття 11 Закону України «Про захист персональних даних», у якій зазначено, що підставами для обробки персональних даних є: згода суб'єкта; дозвіл, наданий законом для здійснення повноважень володільця; укладення чи виконання правочину або дії, що йому передують; захист життєво важливих інтересів; виконання обов'язків, передбачених законом; а також захист законних інтересів володільця чи третьої особи, за винятком випадків, коли пріоритет мають права та свободи суб'єкта даних [6].

Порівняння з положеннями Регламенту свідчить, що обидва акти мають спільні риси, адже вони ґрунтуються на подібних базових підставах обробки. Разом із тим, Регламент містить додаткову умову законності обробки – «виконання завдань у суспільних інтересах». Слід також наголосити, що наявність суспільного інтересу у європейському праві визнається не лише загальною підставою для обробки персональних даних, а й окремою підставою для опрацювання чутливих персональних даних, що ще більше підкреслює його значення у забезпеченні балансу між приватними правами та публічними потребами.

Стаття 7 Регламенту встановлює умови надання згоди суб'єктом персональних даних. Відповідно до даної статті, контролер зобов'язаний довести факт її отримання, якщо згода надається у складі письмової декларації, вона має бути чітко відокремлена від інших положень і викладена зрозумілою мовою, суб'єкт даних має право відкликати згоду у будь-який момент, причому таке відкликання не впливає на законність обробки, здійсненої до нього, при оцінці вільності згоди враховується, чи не ставиться виконання договору або надання послуги в залежність від обробки даних, що не є необхідними для виконання такого договору [7].

Подібних норм національне законодавство не містить, що ускладнює визначення меж правомірності дій володільців даних та створює правову невизначеність. Це також обмежує можливості контролю і забезпечення прав суб'єктів даних, адже відсутні чіткі критерії для оцінки, чи відповідає обробка вимогам закону.

Окрему увагу слід звернути на те, що статті 9 та 10 Регламенту встановлюють загальну заборону на обробку чутливих персональних даних, а також даних про судимості та вчинення кримінальних правопорушень. Такий підхід має фундаментальне значення, оскільки він розглядається не просто як окреме обмеження, а як один із ключових принципів у сфері захисту персональних даних. Водночас національне законодавство України також передбачає заборону щодо опрацювання зазначених категорій даних, однак формулює їх у менш системний спосіб та не надає їм статусу принципів, що зумовлює відмінності в юридичній природі таких положень [7].

Якщо звернутися до переліку чутливих персональних даних, то у європейському та українському законодавстві він загалом має схожий характер. Проте, у Законі України «Про захист персональних даних» серед таких даних виокремлюються, зокрема, відомості про належність до політичних партій, однак відсутні положення щодо інформації про сексуальну орієнтацію особи.

Варто відзначити й винятки, коли обробка чутливих даних є допустимою. Окрім загальних підстав, таких як отримання чіткої згоди суб'єкта, необхідність захисту його життєво важливих інтересів чи реалізація трудових правовідносин володільцем даних, законодавство встановлює і більш спеціальні випадки, які відрізняються від положень європейського законодавства. До них, зокрема, належить ведення військового обліку осіб, які підлягають призову, військовозобов'язаних та резервістів [8].

Водночас, як слушно зазначає П. Гуйван, наявність таких положень у національному законодавстві є позитивним явищем. Проте для їхньої реальної дієвості необхідно продовжувати правотворчу роботу, спрямовану на конкретизацію та деталізацію правил обробки та поширення чутливих персональних даних. Це дозволить усунути двозначність загальних приписів ч. 2 ст. 7 Закону. Зокрема, хоча норма і передбачає отримання однозначної згоди суб'єкта даних, закон не визначає ні її форми, ні порядку, ні строків надання. Додаткового тлумачення потребує й положення про віднесення до складу чутливих даних відомостей, необхідних для захисту чи обґрунтування правової вимоги. Така нечіткість створює можливості для довільного застосування та потенційних зловживань, зокрема з боку органів слідства чи суду [9].

Регламент містить і специфічні положення щодо доступу до чутливих персональних даних. Зокрема, якщо їх обробка є необхідною для цілей превентивної медицини, охорони праці, оцінки працездатності, медичної діагностики, надання чи адміністрування послуг

у сфері охорони здоров'я або соціального забезпечення, вона може здійснюватися виключно медичним працівником або під його відповідальністю. Обов'язковою умовою при цьому є дотримання професійної таємниці відповідно до законодавства ЄС, держав-членів чи норм, встановлених компетентними органами.

Також Регламент виокремлює в окрему категорію персональні дані, що стосуються судимостей та вчинених кримінальних правопорушень, тоді як українське законодавство розглядає їх у межах чутливих персональних даних. Подібне розмежування, запроваджене європейським законодавцем, має швидше формальний характер, тоді як з точки зору практичного забезпечення прав суб'єктів даних доцільно було б уніфікувати ці підходи.

Специфічною особливістю європейського законодавства є встановлення обмежень щодо обробки персональних даних малолітніх та неповнолітніх осіб. Згідно із Регламентом, опрацювання даних дитини вважається законним, якщо вона досягла щонайменше 16 років. У разі, коли дитина молодша, обробка є законною лише за умови, що згоду надано або санкціоновано особою, яка несе батьківську відповідальність. Регламент також дозволяє державам-членам ЄС знижувати віковий поріг для надання згоди батьками, проте мінімальний вік не може бути менше 13 років. Національне законодавство, зокрема Закон України «Про захист персональних даних», подібних обмежень не містить, що є суттєвим недоліком української правової системи.

У контексті захисту чутливих персональних даних важливо враховувати й права суб'єктів, передбачені досліджуваними актами. Так, стаття 8 Закону України «Про захист персональних даних» гарантує фізичній особі право знати джерела збирання, місцезнаходження та мету обробки своїх даних, а також інформацію про умови доступу й третіх осіб, яким вони передаються. Особа має право на доступ до власних персональних даних і їх змісту, отримання відповіді про факт їх обробки, а також можливість подавати вмотивовані вимоги щодо заперечення проти обробки, внесення змін недостовірних чи незаконно оброблюваних даних. Закон також забезпечує захист від незаконної обробки, втрати чи пошкодження персональних даних, передбачає право звертатися зі скаргами до Уповноваженого або до суду та застосовувати правові засоби захисту. Крім того, суб'єкт даних може відкликати надану згоду, вносити застереження щодо її обмеження, знати механізм автоматизованої обробки та вимагати захисту від автоматизованих рішень, які можуть мати для нього правові наслідки [6].

Важливо підкреслити, що зазначена стаття фактично лише перераховує основні права суб'єкта персональних даних, не надаючи їм належної деталізації чи конкретних механізмів реалізації. На відміну від Регламенту, який детально регламентує порядок реалізації кожного права, встановлює часові рамки, обов'язки контролера та передбачає дієві механізми контролю, українське законодавство залишається надто загальним.

Глава III Регламенту присвячена правам суб'єкта даних. Її положеннями забезпечуються усі ті ж самі права, що окреслені вище, однак більш деталізовано. Праву суб'єкта на отримання інформації щодо обробки його персональних даних кореспондує обов'язок контролера вжити необхідних заходів для надання будь-якої інформації, вказаної в статтях 13 і 14 та в будь-якому повідомленні згідно зі статтями 15–22 і 34 щодо опрацювання, суб'єкту даних у стислій, прозорій, доступній для розуміння та легко доступній формі. Також на контролера покладається обов'язок усіляко сприяти реалізації прав суб'єкта даних.

У випадку коли персональні дані збираються безпосередньо від суб'єкта, контролер зобов'язаний надати йому інформацію про себе, цілі та правові підстави обробки, можливих одержувачів, а також умови передачі даних за кордон. Якщо ж дані отримуються не від суб'єкта, додатково повідомляються їхні категорії та джерело походження.

Окрім базових відомостей, контролер має повідомити суб'єкта про строки зберігання даних, його права (доступ, виправлення, стирання, обмеження чи заперечення опрацювання, перенесення), можливість відкликати згоду, подати скаргу до наглядового органу, а також про обов'язковість чи добровільність надання даних і наслідки відмови. Так, якщо обробка

чутливих персональних даних здійснюється на підставі згоди, суб'єкт має право відкликати згоду в будь-який момент без шкоди для законності попередньої обробки. Це право особливо важливе для чутливих персональних даних, забезпечуючи контроль суб'єкта над опрацюванням надзвичайно чутливої інформації.

За наявності автоматизованого ухвалення рішень чи профайлінгу контролер зобов'язаний роз'яснити їхню логіку та наслідки. Крім того, особу необхідно повідомити, що вона має майже необмежено право не підлягати рішенню, що ґрунтується винятково на автоматизованому опрацюванні чутливих персональних даних. Винятком є випадки, коли така обробка здійснюється на підставі згоди суб'єкта або з метою виконання завдань у суспільних інтересах.

Також досліджувана глава приділяє увагу праву суб'єкта даних на стирання (право бути забутим). Суб'єкт має право вимагати видалення своїх персональних даних, а контролер зобов'язаний виконати таку вимогу без необґрунтованої затримки, якщо існують визначені підстави, зокрема коли дані більше не потрібні для цілей обробки, відкликано згоду без іншої законної підстави, висловлено заперечення проти опрацювання без переваги законних інтересів, дані оброблялися незаконно, або їх необхідно видалити для дотримання законодавства чи надання послуг інформаційного суспільства. Водночас дане положення не застосовується якщо опрацювання чутливих персональних даних здійснюється на підставах суспільного інтересу в сфері охорони суспільного здоров'я, а також у разі надання медичних, соціальних послуг [7].

Національне законодавство також гарантує особі право на знищення її персональних даних. Це право може бути реалізоване шляхом подання вмотивованої вимоги до володільця чи розпорядника персональних даних у випадках, коли їх обробка здійснюється незаконно або ж коли дані виявляються недостовірними. Водночас законодавство не визначає жодних чітких критеріїв щодо вмотивованості такої вимоги, унаслідок чого питання її обґрунтованості фактично залишається на розсуд володільців та розпорядників персональних даних [6].

Також закон окреслює й інші підстави для видалення або знищення персональних даних, зокрема у разі їх законної обробки: закінчення строку зберігання, визначеного згодою суб'єкта або законом; припинення правовідносин між суб'єктом і володільцем чи розпорядником даних (якщо інше не передбачено законом); видання припису Уповноваженим чи його уповноваженими посадовими особами; а також набрання законної сили рішенням суду про видалення чи знищення персональних даних.

Важливим аспектом правового регулювання будь якої сфери суспільних відносин є встановлення відповідальності за порушення встановлених норм права. Закон України «Про захист персональних даних» у цьому аспекті є надзвичайно скупим. Стаття 28 зазначає, що за порушення законодавства про захист персональних даних тягне за собою відповідальність, встановлену законом. Тобто зазначена норма відсилає до інших нормативно-правових актів які встановлюють відповідальність за порушення у сфері захисту персональних даних. До прикладу, за порушення законодавства у сфері персональних даних особа може бути притягнута за статтею 188-39 Кодексу України про адміністративні правопорушення [10]. Максимальне покарання за порушення у сфері захисту персональних даних передбачене у випадку повторного протягом року недодержання встановленого порядку їх захисту, що призвело до незаконного доступу або порушення прав суб'єкта даних. У такому разі штраф може сягати від 1000 до 2000 неоподатковуваних мінімумів доходів громадян. В цілому ж санкції для громадян варіюються від 100 до 500 мінімумів, тоді як для посадових осіб та суб'єктів підприємницької діяльності – від 200 до 2000 мінімумів.

У Регламенті відповідальність за порушення встановлена значно суворіше, ніж у національному законодавстві України. Регламент передбачає диференційовану систему штрафів, розмір яких залежить від характеру та тяжкості порушення, категорій персональних даних, на які вплинуло порушення, наявність попередніх порушень, тощо.

Зокрема, за менш суттєві порушення, пов'язані з невиконанням певних технічних чи організаційних вимог, наприклад, недотримання обов'язку вести внутрішній реєстр операцій з даними або відсутність належних заходів безпеки, може накладатися штраф у розмірі до 10 мільйонів євро або до 2% від загального річного світового обороту компанії за попередній фінансовий рік (залежно від того, яка сума є більшою).

Водночас за більш тяжкі порушення – наприклад, незаконну обробку чутливих персональних даних – передбачений штраф до 20 мільйонів євро або до 4% від загального річного світового обороту компанії за попередній рік (також застосовується більша з двох сум).

Крім фінансових санкцій, Регламент передбачає й інші заходи впливу, зокрема: обмеження чи заборону обробки даних, тимчасове чи остаточне припинення передачі даних до третіх країн, а також зобов'язання виправити або видалити неправомірно оброблені дані.

Висновки. У результаті проведеного дослідження встановлено, що Закон України «Про захист персональних даних» значно поступається Регламенту за рівнем деталізації та системності правового регулювання у сфері захисту персональних даних. Національне законодавство не закріплює чітких принципів обробки та захисту персональних даних, обмежуючись лише окремими формальними правилами. Закон лише перелічує права суб'єктів персональних даних, не забезпечуючи ефективного механізму їх реалізації. Натомість Регламент не лише чітко формулює принципи захисту даних, а й детально характеризує кожне право особи, встановлює обов'язки для контролерів і операторів даних, а також прямо передбачає відповідальність за порушення законодавства у цій сфері. Крім того, Регламент досить чітко визначає розмір санкцій та критерії, від яких він залежить, тоді як українське законодавство лише відсилає до інших нормативних актів, які передбачають значно менш суворі покарання.

Зазначене створює додаткові труднощі як для належного розуміння особами власних прав, так і для їх практичної реалізації. Саме тому, виникає об'єктивна необхідність удосконалення національного законодавства у сфері захисту персональних даних, його гармонізації з європейськими стандартами та запровадження більш чітких і дієвих механізмів реалізації прав суб'єктів персональних даних.

Список використаних джерел:

1. Угода про асоціацію між Україною, з однієї сторони, та Європейським Союзом, Європейським співтовариством з атомної енергії і їхніми державами-членами, з іншої сторони : Угода Україна від 27.06.2014: станом на 30 листоп. 2023 р. URL: https://zakon.rada.gov.ua/laws/show/984_011#Text (дата звернення: 02.10.2025).

2. Кальченко В., Ободяк В. Порівняльна характеристика нормативних вимог України та ЄС у сфері кіберзахисту персональних даних в інформаційно-комунікаційних системах. *Інформаційні технології та суспільство.* 2023. №5(11). С. 14–20. URL: https://doi.org/10.32689/maup.it.2023.5.2 (дата звернення: 02.10.2025).

3. Про інформаційні технології, файли даних і громадянські свободи : Закон Французької Республіки від 06.01.1978 № № 78-17. URL: https://www.legifrance.gouv.fr/loda/id/JORFTEXT000000886460.

4. Федеральний закон (ФРН) «Про захист даних» від 30 червня 2017 р. Bundesgesetzblatt Teil I Nr. 30, 02.07.2017, S. 1074–1091. URL: https://www.gesetze-im-internet.de/englisch_bdsg/

5. Котляревський Я.В., Сірик М.В., Дяченко М.О. Перспективні напрями удосконалення регулювання сфери захисту персональних даних в Україні. *Економіка та право*. 2022, № 1. С. 45–64. https://doi.org/10.15407/econlaw.2022.01.045

6. Про захист персональних даних: Закон України від 01.06.2010 № 2297-VI : станом на 14 черв. 2025 р. URL: https://zakon.rada.gov.ua/laws/show/2297-17#Text (дата звернення: 30.09.2025).

7. 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): Регламент Європ. Союзу від 27.04.2016 № 2016/679. URL: https://zakon.rada.gov.ua/laws/show/984_008-16#Text (дата звернення: 18.08.2025).

8. Придатко Д.О. Правова природа та особливості регулювання чутливих персональних даних. *Актуальні питання у сучасній науці*. Випуск № 9(39), 2025.

9. Гуйван П. Д. Міжнародний досвід захисту чутливих категорій персональних даних. *Альманах Міжнародного Права*. 2019. Т. 22. С. 3–14. URL: https://doi.org/10.32841/ila.2019.22.01 (дата звернення: 16.08.2025).

10. Кодекс України про адміністративні правопорушення (статті 1 – 212-24): Кодекс України від 07.12.1984 № 8073-X: станом на 1 верес. 2025 р. URL: https://zakon.rada.gov.ua/laws/show/80731-10#Text (дата звернення: 02.10.2025).

Дата першого надходження рукопису до видання: 18.11.2025
Дата прийнятого до друку рукопису після рецензування: 15.12.2025
Дата публікації: 31.12.2025