

## ГОСПОДАРСЬКЕ ПРАВО ТА ПРОЦЕС

**ВОЛИНЕЦЬ В. В.,**  
доктор юридичних наук,  
професор кафедри готельно-ресторанної  
справи  
(Київський університет туризму  
економіки і права)

УДК 347.918:342.7:004.738.5  
DOI <https://doi.org/10.32842/2078-3736/2024.5.21>

### ЗГОДА НА ОБРОБКУ ДАНИХ В ОНЛАЙН ТОРГІВЛІ: ЮРИДИЧНІ ВИМОГИ ТА КРАЩІ ПРАКТИКИ

У статті досліджується правове регулювання захисту персональних даних в Україні в контексті міжнародних стандартів та вимог. Аналізуються ключові положення Закону України «Про захист персональних даних» та їх відповідність Загальному регламенту захисту даних (GDPR) Європейського Союзу. Особлива увага приділяється визначенню поняття «персональні дані», яке в українському законодавстві трактується як будь-яка інформація, що прямо або опосередковано стосується визначеної або ідентифікованої фізичної особи. Це включає різноманітні види даних, які можуть дозволити встановити особу, навіть за наявності лише непрямих вказівок.

Аналізується концепція згоди на обробку персональних даних як правочину, що має юридичну силу. Згода повинна бути добровільною, інформованою, конкретною та наданою однозначно, що є обов'язковою умовою для її дійсності. Висвітлюється питання форми надання згоди, зокрема, електронної згоди, та необхідність її підтвердження через активну дію суб'єкта даних, що відповідає міжнародним стандартам.

Розглядаються випадки, коли обробка персональних даних може здійснюватися без згоди суб'єкта даних, підкреслюючи важливість правових основ для таких дій. Зокрема, це стосується виконання договірних або юридичних зобов'язань, захисту життєво важливих інтересів суб'єкта даних або іншої фізичної особи, а також виконання завдань, що здійснюються в суспільних інтересах або в рамках офіційних повноважень.

На підставі проведеного аналізу запропоновано шляхи вдосконалення правового регулювання обігу персональних даних, серед яких гармонізація національного законодавства з міжнародними стандартами, розвиток механізмів міжнародного співробітництва, підвищення ефективності діяльності наглядових органів та підвищення обізнаності громадян про їхні права. У висновках ідеться про необхідність подальшого розвитку правових механізмів та інституційної спроможності для забезпечення належного рівня захисту персональних даних.

**Ключові слова:** персональні дані, правове регулювання, захист даних, згода на обробку, GDPR, національне законодавство, міжнародне право, правозастосування, цифрова трансформація, чутливі дані, cookies.



**Volynets V. V. Consent for data processing in online commerce: legal requirements and best practices**

The article examines the legal regulation of personal data protection in Ukraine within the context of international standards and requirements. It analyzes the key provisions of the Law of Ukraine "On Personal Data Protection" and their compliance with the General Data Protection Regulation (GDPR) of the European Union. Special attention is given to the definition of "personal data," which is interpreted in Ukrainian legislation as any information that directly or indirectly relates to an identified or identifiable natural person. This includes various types of data that may allow the identification of an individual, even in the presence of only indirect indications.

The concept of consent for personal data processing as a legal transaction with binding legal force is analyzed. Consent must be voluntary, informed, specific, and unequivocally given, which is a mandatory condition for its validity. The article highlights the issue of the form in which consent is provided, particularly electronic consent, and the necessity for its confirmation through an active action by the data subject, which aligns with international standards.

The article discusses cases where personal data processing may be carried out without the consent of the data subject, emphasizing the importance of legal grounds for such actions. In particular, this concerns the fulfillment of contractual or legal obligations, the protection of the vital interests of the data subject or another natural person, as well as the performance of tasks carried out in the public interest or within the framework of official authority.

Based on the conducted analysis, the article proposes ways to improve the legal regulation of personal data circulation, including the harmonization of national legislation with international standards, the development of mechanisms for international cooperation, enhancing the effectiveness of supervisory authorities, and raising public awareness about their rights. The conclusions emphasize the need for further development of legal mechanisms and institutional capacity to ensure an adequate level of personal data protection.

**Key words:** *personal data, legal regulation, data protection, consent for processing, GDPR, national legislation, international law, law enforcement, digital transformation, sensitive data, cookies.*

**Вступ.** У сучасному світі онлайн-торгівля стала невіддільною частиною повсякденного життя, створюючи нові можливості для бізнесу та споживачів. Водночас разом із цим виникають і деякі нововідкриті питання, пов'язані з обробкою та захистом персональних даних. Збирання, зберігання та використання інформації про клієнтів стали важливими аспектами діяльності будь-якої компанії, яка працює у сфері електронної комерції.

При цьому персональні дані клієнтів самі по собі стали цінним активом, що дозволяє компаніям покращувати свої сервіси, таргетувати рекламу та розвивати лояльність споживачів. Однак, разом із цими можливостями зростає ризик порушення приватності у формі неправомірного використання або витоку інформації про особу. У зв'язку з цим, юридичні рамки обробки даних стають дедалі жорсткішими, що відображається в законодавстві багатьох країн, зокрема, в Україні.

Важливу роль у формуванні законодавчих норм щодо захисту персональних даних відіграють міжнародні стандарти та рекомендації, такі як положення Конвенції Ради Європи № 108 та Директива ЄС 95/46/ЄС. Ці нормативні джерела закріплюють основні принципи обробки даних, які покликані захищати права і свободи людини в контексті ледь не повсюдного використання інформаційних технологій.

**Постановка завдання.** У пропонованій статті ми розглянемо основні юридичні вимоги до згоди на обробку даних в онлайн-торгівлі, а також кращі практики, які допоможуть



забезпечити відповідність діяльності компаній вимогам законодавства та захистити права споживачів. На матеріалах міжнародного та національного права ми проаналізуємо правові аспекти обробки даних, зокрема, принципи законності, справедливості та прозорості, а також розглянемо питання безпеки даних і управління ризиками, пов'язаними з їх обробкою.

У світлі викладеного, мета цього дослідження полягає в тому, щоб змалювати порядок та способи надання згоди на обробку персональних даних, а також правовий режим персональної інформації, на обробку якої надано згоду, а також запропонувати практичні рекомендації для бізнесу, спрямовані на покращення процедур обробки персональних даних, що сприятиме підвищенню довіри споживачів та зміцненню репутації компаній на ринку онлайн-торгівлі.

Огляд літератури з темою дослідження. З огляду на поширеність правовідносин у сфері обробки персональних даних, широка увага дослідників тут є цілком закономірною. В цьому контексті передусім потрібно згадати працю М.В. Бема та І.М. Городиського, котрі у своєму науково-практичному посібнику аналізують правові аспекти захисту персональних даних, звертаючи увагу на проблеми правозастосування та необхідність вдосконалення національного законодавства з урахуванням міжнародних стандартів [1, с. 45–67]. Ці питання перегукуються з дослідженням Т.Г. Каткової, яка розглядає адміністративну відповідальність за порушення законодавства у цій сфері, пропонуючи вдосконалення механізмів нагляду [5, с. 121].

Питання згоди на обробку даних, розглянуте В.В. Заборовським і В.В. Манзюком, акцентує на необхідності чіткого правового регулювання з метою забезпечення прав клієнтів на захист їхніх даних, що є важливим для адвокатської практики [2, с. 649–650]. Своєю чергою, А.С. Михайлик досліджує нормативно-правове регулювання захисту персональних даних працівників, вказуючи на недостатнє врахування трудових відносин у чинному законодавстві [6, с. 83–84].

К.О. Калаченкова та К.В. Бородата фокусуються на захисті персональних даних у контексті використання таргетованої реклами, наголошуючи на ризиках для конфіденційності, що виникають у процесі обробки даних для маркетингових цілей [3, с. 18–20]. Ця тематика дотично пов'язана з дослідженням Ю.Я. Самагальської, яка аналізує специфіку захисту даних в Інтернеті, акцентуючи на потребі міжнародного співробітництва у забезпеченні кібербезпеки [9, с. 261–262].

Проблематика конституційно-правового захисту інформації про особу, розглянута А.В. Кардашем, підкреслює важливість забезпечення права на приватність у різних правових системах [4, с. 105–112]. О.В. Легка також акцентує на значенні імплементації міжнародних стандартів у національне законодавство, враховуючи досвід інших країн у сфері захисту даних [8, с. 76].

А.Ю. Нашинець-Наумова у своїй монографії аналізує питання правового регулювання інформаційної безпеки, пропонуючи вдосконалення механізмів захисту даних у цифровому середовищі [7, с. 55–67]. Аналогічні аспекти підіймає і Х.Я. Терешко, досліджуючи види інформації у сфері медичного обслуговування та необхідність чіткіших правових механізмів захисту чутливих даних [10, с. 66–68].

Наостанок, Я.Г. Худолей та Н.А. Загребельна аналізують питання захисту персональних даних у період дії правового режиму воєнного стану в Україні, розглядаючи загально-теоретичні аспекти права на приватність та безпеку даних [11, с. 76–78]. Їхній аналіз підкреслює необхідність адаптації правових норм до специфічних умов, що виникають під час особливих правових режимів.

Таким чином, аналіз літератури свідчить про те, що захист персональних даних є складним і багатограним питанням, яке потребує інтегрованого підходу, що включає як вдосконалення національного законодавства, так і міжнародну співпрацю для забезпечення ефективної охорони прав на конфіденційність в умовах сучасних викликів.

**Результати дослідження.** І. Джерела міжнародного права. Міжнародно-правові джерела регулювання обігу персональних даних, безумовно, відіграють ключову роль



у формуванні правових стандартів захисту приватності та конфіденційності у глобалізованому світі. Варто наголосити, що правове регулювання персональних даних на міжнародному рівні здійснюється через систему багатосторонніх договорів, рекомендаційних документів, а також практику міжнародних судових органів, які разом створюють комплексну правову основу для забезпечення захисту персональних даних у різних юрисдикціях.

Почнімо з Конвенції Ради Європи № 108 «Про захист осіб у зв'язку з автоматизованою обробкою персональних даних» від 1981 року [12], яка є першим і, до певної міри, еталонним міжнародно-правовим документом у цій галузі. Конвенція встановлює загальні принципи щодо обробки даних (статті 5–8), які включають вимоги до законності, чесності та прозорості обробки, мінімізації даних, а також точності і збереження даних лише на період, необхідний для досягнення визначеної мети. Важливо підкреслити, що Конвенція також передбачає права суб'єктів даних, такі як право доступу до своїх персональних даних (стаття 8), право на виправлення або видалення неправомірно оброблених даних, а також право на оскарження таких дій.

Варто зазначити, що Конвенція № 108 була доповнена Протоколом CETS № 181 (від 2001 року), який уточнює та посилює вимоги щодо трансграничної передачі персональних даних. Зокрема, стаття 2 Протоколу містить положення про те, що передача персональних даних до країн, які не є членами Ради Європи, дозволяється лише за умови, що такі країни забезпечують адекватний рівень захисту персональних даних, або ж якщо існують відповідні правові гарантії. Тут же встановлюються вимоги щодо створення незалежного наглядового органу, який би здійснював контроль за дотриманням норм захисту даних (стаття 1 Протоколу).

Продовжуючи розгляд правових актів, не можна оминати увагою Загальний регламент про захист даних (GDPR) Європейського Союзу, що набув чинності у травні 2018 року [13]. GDPR замінив Директиву 95/46/ЄС і встановлює нові стандарти щодо захисту даних у Європейському Союзі. Особливої уваги заслуговують такі його положення, як стаття 6, яка детально регламентує підстави для обробки персональних даних, включаючи згоду суб'єкта даних, виконання контракту, виконання правового обов'язку, захист життєво важливих інтересів, виконання завдання, здійснюваного в суспільних інтересах або в рамках здійснення офіційних повноважень (пункти 1(a)–(f)). Водночас стаття 9 встановлює суворіші вимоги до обробки спеціальних категорій персональних даних, включаючи дані про расове або етнічне походження, політичні погляди, релігійні або філософські переконання, членство в профспілках, генетичні дані, біометричні дані для унікальної ідентифікації особи, дані про здоров'я або дані щодо сексуального життя або сексуальної орієнтації. Окрім цього, чільне місце з-поміж джерел в схарактеризованій сфері посідає Європейська конвенція про захист прав та основоположних свобод (стаття 8) [14] та практика Європейського суду з прав людини, котра розвиває та конкретизує Конвенцію в контексті права на повагу приватного та сімейного життя людини.

Що стосується міжнародно-правових актів, розроблених Організацією Об'єднаних Націй, то тут слід звернути увагу на Резолюцію Генеральної Асамблеї ООН № 45/95 від 1990 року «Керівні принципи регулювання комп'ютерних файлів, що містять персональні дані», яка рекомендує державам-членам приймати національні законодавчі акти, що встановлюють мінімальні стандарти для обробки персональних даних. Зокрема, пункти 3 і 4 цих Керівних принципів наголошують на необхідності забезпечення прав суб'єктів даних на доступ, виправлення або видалення інформації, що міститься в таких файлах, а також на важливості забезпечення безпеки даних і попередження їх несанкціонованого доступу або втрати.

Крім того, у рамках Організації економічного співробітництва та розвитку (ОЕСР) було розроблено «Керівні принципи захисту недоторканності приватного життя і трансграничних потоків персональних даних» (1980 р., переглянуті в 2013 р.), які встановлюють основні принципи обробки персональних даних, такі як обмеження збору, якість даних, обмеження мети, гарантії безпеки та прозорість. Вказані принципи, хоча і мають



рекомендаційний характер, стали основою для багатьох національних законодавчих актів і міжнародних договорів, включаючи GDPR та Конвенцію № 108.

Також варто звернути увагу на Хартію основних прав Європейського Союзу, стаття 8 якої проголошує право кожного на захист персональних даних, що його стосуються. Вона встановлює, що такі дані мають оброблятися справедливо, для визначених цілей та на основі згоди відповідної особи або на іншій законній підставі, передбаченій законом (параграф 2). Також кожна особа має право на доступ до зібраних даних, що стосуються неї, та на їх виправлення.

Отже, міжнародно-правові джерела регулювання обігу персональних даних формують комплексний нормативно-правовий простір, що включає основні принципи та стандарти для забезпечення захисту прав людини на приватність та інформаційну безпеку. Ці стандарти, хоча і різняться залежно від конкретного акта, мають спільну мету: забезпечення балансу між правами та інтересами суб'єктів даних і потребами суспільства в ефективному використанні інформації.

II. Джерела національного рівня. Національні джерела регулювання обігу персональних даних в Україні відображають прагнення держави забезпечити належний рівень захисту приватності, що відповідає міжнародним стандартам, і водночас враховують специфіку національного правового порядку та соціальних відносин. В основі нормативно-правової бази захисту персональних даних лежить Закон України «Про захист персональних даних» [15], який прийнято у 2010 році та який зазнав низки змін з метою адаптації до європейських стандартів, зокрема після підписання Угоди про асоціацію з Європейським Союзом.

Закон України «Про захист персональних даних» визначає ключові поняття, принципи, права та обов'язки сторін у сфері обробки персональних даних. Відповідно до статті 2 Закону, під «персональними даними» розуміється будь-яка інформація, що стосується фізичної особи, яка прямо або опосередковано визначається або може бути визначена. Важливим є також поняття «обробки персональних даних», яке охоплює будь-які дії або сукупність дій, здійснюваних у повністю або частково автоматизованій чи неавтоматизованій формі з персональними даними (збирання, запис, систематизація, накопичення, зберігання, адаптація, зміна, відновлення, використання, знищення тощо) (стаття 5).

Цікаво зазначити, що Закон передбачає ряд специфічних принципів обробки персональних даних, які включають законність, цільову визначеність, пропорційність, точність, обмеження строків зберігання, конфіденційність та безпеку обробки даних (статті 6, 7). Законність обробки означає, що обробка персональних даних може здійснюватися лише на підставах, чітко визначених законодавством (стаття 11), таких як згода суб'єкта даних, необхідність для виконання контракту або юридичного обов'язку, захист життєво важливих інтересів суб'єкта даних або третьої особи, а також виконання завдання, здійснюваного в суспільних інтересах або під час здійснення офіційних повноважень.

Крім того, важливою частиною національного законодавства є права суб'єктів персональних даних, які передбачені у розділі IV Закону. Ці права включають право на інформацію про обробку даних (стаття 16), право доступу до власних даних (стаття 17), право на заперечення обробки даних (стаття 18), право на виправлення, видалення чи блокування неточних або незаконно оброблених даних (стаття 19), а також право на захист своїх прав у випадку порушення законодавства (стаття 20).

Додатково, Закон України «Про захист персональних даних» встановлює обов'язки володільців та розпорядників персональних даних, включаючи вимоги до забезпечення безпеки даних (стаття 24), необхідність повідомлення Уповноваженого Верховної Ради України з прав людини про обробку даних, що становлять особливий ризик для прав і свобод суб'єктів (стаття 21), та інші заходи для захисту даних.

Окремо варто згадати про Закон України «Про Уповноваженого Верховної Ради України з прав людини», що, в аспекті розглядуваної нами тематики, визначає роль в ній Уповноваженого Верховної Ради України з прав людини як органу, відповідального за здійснення контролю за дотриманням законодавства у сфері захисту персональних даних



(стаття 22). Уповноважений має повноваження здійснювати планові та позапланові перевірки (стаття 23), видавати приписи про усунення порушень та накладати адміністративні стягнення за невиконання вимог законодавства (стаття 25). Слід зауважити, що регламентуючі акти Уповноваженого, такі як методичні рекомендації, також є важливим джерелом тлумачення і застосування положень Закону.

Крім Закону «Про захист персональних даних», захист персональних даних в Україні також регулюється іншими, більш загальними нормативно-правовими актами, такими як Цивільний кодекс України, який встановлює загальні засади захисту особистих немайнових прав, зокрема права на особисте життя (стаття 270). Окрім цього, у Законі України «Про інформацію» передбачено принципи та механізми захисту інформації про фізичну особу (стаття 11), що також стосується захисту персональних даних.

Важливо звернути увагу, що у зв'язку з процесом євроінтеграції, Україна поступово адаптує своє законодавство до вимог ЄС, зокрема, враховуючи положення GDPR. Так, законодавчі ініціативи останніх років спрямовані на удосконалення національних стандартів захисту даних, включаючи запровадження механізмів відповідальності за порушення прав суб'єктів персональних даних та встановлення суворіших вимог до обробки даних спеціальних категорій.

III. Згода на обробку персональних даних як правочин: основні вимоги. Згода на обробку персональних даних, безперечно, є одним із фундаментальних елементів сучасного правового регулювання у цій сфері. Як національне, так і міжнародне законодавство визнають згоду суб'єкта персональних даних правочином, що надає правові підстави для обробки таких даних. Розглянемо детально, чому згода розглядається як правочин, у якій формі вона має надаватися, та за яких умов обробка персональних даних може здійснюватися без такої згоди.

Національне законодавство України, а саме Закон України «Про захист персональних даних», вказує, що згода суб'єкта персональних даних є одним із правових підстав для обробки персональних даних (стаття 11). Важливо зазначити, що згідно зі статтею 2 цього Закону, згода визначається як добровільне волевиявлення фізичної особи щодо надання дозволу на обробку своїх персональних даних відповідно до визначеної мети їх обробки, висловлене у письмовій формі або у формі, що дозволяє зробити висновок про надання згоди. Таким чином, згода є правочином, що містить елементи одностороннього волевиявлення, яке створює правові наслідки для суб'єкта, що надає таку згоду.

У міжнародно-правовому контексті, Загальний регламент про захист даних (GDPR) Європейського Союзу містить подібне визначення. Стаття 4(11) GDPR визначає згоду як «будь-яке добровільно надане, конкретне, усвідомлене і однозначне виявлення волевиявлення суб'єкта даних, за допомогою якого він чи вона шляхом заяви або чіткої підтверджувальної дії погоджується на обробку персональних даних, що його чи її стосуються». Тобто, згода повинна відповідати вимогам ясності, конкретності та добровільності, що робить її правочином, який має юридичну силу та наслідки.

IV. Форма надання згоди. Згода на обробку персональних даних може надаватися у різних формах. Відповідно до українського законодавства, згода може бути надана у письмовій формі або в іншій формі, що дозволяє зробити висновок про її надання (стаття 2 Закону «Про захист персональних даних»). Така форма може включати електронну згоду, наприклад, шляхом натискання на кнопку «Приймаю» на вебсайті, або через вибір відповідної опції у цифровій формі (наприклад, у мобільному додатку). Важливо, щоб форма надання згоди дозволяла чітко зафіксувати волевиявлення суб'єкта даних і, таким чином, забезпечувала можливість підтвердження наданої згоди у майбутньому.

GDPR також встановлює вимоги до форми згоди, наголошуючи, що згода повинна бути надана у формі, яка дозволяє чітко визначити згоду суб'єкта даних. Це може бути як письмова згода, так і електронна, за умови, що вона є однозначною та підтверджує активні дії з боку суб'єкта даних (стаття 7 GDPR). Наприклад, у випадку з електронною згодою, GDPR прямо забороняє використання попередньо заповнених чекбоксів, оскільки вони не забезпечують чіткої та активної дії суб'єкта даних.



Питання про згоду на обробку персональних даних набуває особливої актуальності в контексті використання файлів cookies на вебсайтах. Cookies можуть збирати різні типи персональних даних, такі як IP-адреси, поведінка користувачів на вебсайті тощо. Відповідно до GDPR (стаття 6 та 7), для використання cookies, які не є строго необхідними для функціонування вебсайту, вебсайти повинні отримати чітку і недвозначну згоду користувача. Це означає, що користувачі повинні бути проінформовані про те, які саме дані збираються, з якою метою, та мати можливість вибору – прийняти або відхилити використання таких cookies.

V. Випадки, коли згода не вимагається. Однак, варто відзначити, що існують ситуації, коли обробка персональних даних може здійснюватися без згоди суб'єкта даних. Як українське законодавство, так і GDPR передбачають такі винятки. Наприклад, відповідно до статті 11 Закону України «Про захист персональних даних», обробка персональних даних може здійснюватися без згоди у випадках, коли це необхідно для виконання договору, стороною якого є суб'єкт даних, для виконання юридичного обов'язку володільця даних, для захисту життєво важливих інтересів суб'єкта даних або іншої фізичної особи, а також для захисту державної безпеки, економічного добробуту та прав людини.

GDPR у статті 6(1)(b)–(f) встановлює подібні підстави, що дозволяють обробку даних без згоди суб'єкта, включаючи виконання контракту, виконання юридичного обов'язку контролера даних, захист життєво важливих інтересів суб'єкта даних або іншої фізичної особи, виконання завдання, здійснюваного в суспільних інтересах або під час здійснення офіційних повноважень, а також для легітимних інтересів контролера або третьої сторони, за винятком випадків, коли ці інтереси не переважають інтереси або фундаментальні права і свободи суб'єкта даних.

Таким чином, згода на обробку персональних даних є ключовим правочином у сучасному правовому регулюванні, який становить собою фактичну підставу (юридичний факт) для законної обробки даних. Водночас законодавство передбачає конкретні вимоги до форми та змісту такої згоди, що має бути добровільною, конкретною, усвідомленою та однозначною. Разом із тим, як на національному, так і міжнародному рівнях, передбачені випадки, коли обробка персональних даних може здійснюватися без згоди, що свідчить про необхідність збалансованого підходу до захисту прав суб'єктів даних і забезпечення ефективного функціонування економіки та державних інституцій.

**Висновки.** З урахуванням викладеного вище варто підкреслити, що правове регулювання захисту персональних даних, попри значний прогрес, досягнутий як на національному, так і міжнародному рівнях, все ще стикається з численними викликами та проблемами, які потребують подальшого вдосконалення і узгодження. Серед ключових проблем можна виділити недостатню узгодженість національних правових систем з міжнародними стандартами, проблеми транснаціональної обробки даних, а також ефективність правозастосування та дотримання прав суб'єктів персональних даних.

Першою і, безумовно, важливою проблемою є недостатня узгодженість національних правових систем з міжнародними стандартами захисту персональних даних. Незважаючи на те, що Україна, як і багато інших країн, активно адаптує своє законодавство до вимог Загального регламенту захисту даних (GDPR) Європейського Союзу, все ще існують значні розбіжності в трактуванні та застосуванні правових норм. Це призводить до правової невизначеності як для національних, так і для міжнародних суб'єктів, що діють у межах різних юрисдикцій.

Зокрема, кейс Schrems II, рішення у якому Суд Європейського Союзу виніс у липні 2020 року, демонструє складнощі, пов'язані з міжнародною передачею даних. Як відомо, в цій справі означений Суд визнав недійсним Рішення Європейської Комісії про адекватність захисту персональних даних у рамках програми «Privacy Shield» між ЄС і США, оскільки американське законодавство не забезпечує рівень захисту, порівнянний з тим, що надається у ЄС. Цей випадок підкреслює необхідність подальшого вдосконалення міжнародно-правового співробітництва у сфері захисту даних і узгодження стандартів.



Другою значущою проблемою є питання транснаціональної обробки даних, яке стає все більш актуальним у сучасному глобалізованому світі. Розвиток цифрових технологій і поширення Інтернету призвели до того, що обробка даних часто здійснюється поза межами країни, де ці дані були зібрані. Це створює серйозні виклики для національних регуляторів, які не завжди мають можливість контролювати обробку даних за кордоном.

Відсутність ефективних механізмів міжнародного співробітництва у цій сфері часто призводить до того, що персональні дані суб'єктів залишаються незахищеними або піддаються ризику зловживань. Наприклад, сумнозвісний кейс із «Cambridge Analytica» продемонстрував, що компанія, яка базується у Великобританії, змогла отримати доступ до персональних даних мільйонів користувачів Facebook і використовувати їх без належної згоди для політичного таргетингу. Цей випадок виявив прогалини у законодавстві та показав, що національні регулятори часто не мають ефективних інструментів для контролю обробки даних за межами своїх юрисдикцій.

Ще однією суттєвою проблемою є ефективність правозастосування. Незважаючи на існування правових механізмів для захисту прав суб'єктів даних, на практиці забезпечення дотримання цих прав часто є складним. Це може бути пов'язано як з недостатньою поінформованістю громадян про свої права, так і з обмеженими можливостями органів контролю.

У цьому контексті важливим є кейс Google Spain SL, Google Inc. проти Agencia Española de Protección de Datos (AEPD), Mario Costeja González, де Суд ЄС визнав «право на забуття», зобов'язавши пошукові системи видаляти посилання на персональні дані на вимогу користувача, якщо ці дані застарілі або більше не актуальні. Цей випадок, хоча і став важливою віхою у захисті прав суб'єктів даних, також підкреслив складнощі, пов'язані з забезпеченням дотримання прав у цифровому середовищі.

Для вирішення окреслених вище проблем слід запропонувати декілька стратегій. По-перше, необхідно продовжувати гармонізацію національного законодавства з міжнародними стандартами, включаючи повну імплементацію положень GDPR та інших міжнародних документів у національні правові системи. По-друге, слід розвивати міжнародно-правове співробітництво, включаючи укладення нових міжнародних договорів, які б встановлювали чіткі правила для транснаціональної обробки даних та ефективні механізми контролю.

По-третє, варто посилити правозастосування на національному рівні, забезпечивши більш ефективну діяльність наглядових органів, таких як Уповноважений Верховної Ради України з прав людини, та підвищити обізнаність громадян про їхні права щодо захисту персональних даних. Це можна досягти шляхом впровадження навчальних програм, інформаційних кампаній, а також створення доступних та зручних механізмів для подачі скарг і захисту своїх прав.

Насамкінець, слід зауважити, що захист персональних даних у сучасному світі – це динамічна і складна сфера, яка потребує постійного вдосконалення правових механізмів та інституційної спроможності. Лише таким чином можна забезпечити належний захист прав людини на приватність та безпеку інформації в умовах швидко мінливого цифрового середовища.

#### Список використаних джерел:

1. Бем М. В., Городиський І. М. Захист персональних даних: правове регулювання та практичні аспекти : науково-практичний посібник. Київ : К.І.С., 2015. 220 с.
2. Заборовський В. В., Манзюк В. В. Згода клієнта адвоката на обробку його персональних даних як складова реалізації права на адвокатський запит. *Аналітично-порівняльне правознавство*. 2024. № 1. С. 648–652.
3. Калаченкова К. О., Бородата К. В. Захист персональних даних у процесі використання таргетованої реклами. *Аналітично-порівняльне правознавство*. 2023. № 3. С. 17–21.
4. Кардаш А. В. Конституційно-правовий захист інформації про особу (порівняльно-правовий аспект) : дис. канд. юрид. наук: 12.00.02. Харків, 2019. 228 с.





5. Каткова Т. Г. Адміністративна відповідальність за порушення законодавства у сфері захисту персональних даних. *Економічна та інформаційна безпека: актуальні питання та інновації* : матеріали Міжнар. наук.-практ. конф. Дніпро, 4 листоп. 2021 р. С. 120–122.
6. Михайлик А. С. До питання нормативно-правового регулювання захисту персональних даних працівників в Україні. *Науковий вісник Ужгородського національного університету*. 2022. № 72, ч. 2. С. 82–87.
7. Нашинець-Наумова А. Ю. Інформаційна безпека: питання правового регулювання : монографія. Київ : Гельветика, 2017. 168 с.
8. Легка О. В. Актуальні питання захисту персональних даних: вітчизняний та міжнародний досвід. *Правова позиція*. 2021. № 2 (31). С. 74–79.
9. Самагальська Ю. Я. Захист персональних даних в мережі Інтернет. *Науковий вісник Ужгородського національного університету*. 2024. Вип. 82, ч. 2. С. 259–264.
10. Терешко Х. Я. Види інформації як об'єкта цивільних правовідносин у сфері медичного обслуговування. *Медичне право*. 2019. № 1 (23). С. 65–73.
11. Худолей Я. Г., Загребельна Н. А. Захист персональних даних у період дії в Україні правового режиму воєнного стану: загальнотеоретичні аспекти. *Legal Bulletin*. 2023. С. 75–82.
12. Конвенція Ради Європи про захист осіб у зв'язку з автоматизованою обробкою персональних даних від 28.01.1981 року. URL: [https://zakon.rada.gov.ua/laws/show/994\\_326#Text](https://zakon.rada.gov.ua/laws/show/994_326#Text) (дата звернення: 08.04.2024).
13. 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). URL: [https://zakon.rada.gov.ua/laws/show/984\\_008-16/conv#Text](https://zakon.rada.gov.ua/laws/show/984_008-16/conv#Text) (дата звернення: 08.04.2024).
14. Конвенція про захист прав людини і основоположних свобод від 04.11.1950 року. URL: [https://zakon.rada.gov.ua/laws/show/995\\_004#Text](https://zakon.rada.gov.ua/laws/show/995_004#Text) (дата звернення: 08.04.2024).
15. Закон України «Про захист персональних даних» від 01.06.2010 року № 2297-VI. URL: <https://zakon.rada.gov.ua/laws/show/2297-17&#8203>

