

ПРАВОВИЙ МЕХАНІЗМ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ В КІБЕРПРОСТОРИ

LEGAL MECHANISM FOR PROTECTION OF PERSONAL DATA IN CYBERSPACE

Тарасенко В.О., магістр права

У сучасному цифровому світі, що характеризується стрімким розвитком інформаційних технологій і повсюдною цифровізацією, питання захисту персональних даних набуває особливої актуальності. Це зумовлено не лише зростанням обсягів інформації, що обробляється в кіберпросторі, а й появою нових, більш витончених загроз для приватності особистості. Персональні дані, від фінансової інформації до біометричних ідентифікаторів, перетворилися на один із найцінніших ресурсів сучасної економіки. Водночас їхня висока цінність робить їх мішенню для неправомірного використання, включаючи кібершахрайство та крадіжку особистих даних. Захист персональних даних є невіддільним елементом системи цифрових прав громадян та ключовою передумовою для формування безпечного інформаційного суспільства.

Актуальність теми зумовлена низкою об'єктивних чинників, що вимагають негайного реагування з боку правової системи. Транскордонний характер кіберпростору створює значні виклики для традиційних принципів юрисдикції. Дані можуть оброблятися та передаватися через кордони різних держав, що ускладнює застосування національного законодавства та притягнення порушників до відповідальності, а це вимагає розробки уніфікованих міжнародних стандартів. Крім того, постійний розвиток технологій обробки даних (наприклад, Big Data, штучний інтелект) та поява нових моделей бізнесу вимагають перегляду наявних правових норм. Недостатня правова визначеність щодо того, хто є відповідальним за захист даних у складних ланцюжках обробки, створює правові прогалини, якими можуть скористатися зловмисники. Не менш важливим є питання забезпечення балансу між захистом персональних даних та іншими суспільними інтересами, такими як розвиток інновацій. Недостатньо гнучке законодавство може стати перешкодою для розвитку цифрової економіки, тоді як слабке – не зможе ефективно захистити права громадян.

Ключові слова: персональні дані, кіберпростір, кібербезпека, правове регулювання, GDPR, приватність.

In the modern digital world, characterized by the rapid development of information technologies and widespread digitalization, the issue of personal data protection is gaining particular relevance. This is due not only to the growth in the volume of information processed in cyberspace, but also to the emergence of new, more sophisticated threats to personal privacy. Personal data, from financial information to biometric identifiers, has become one of the most valuable resources in the modern economy. At the same time, their high value makes them a target for misuse, including cyber fraud and identity theft. Personal data protection is an integral element of the system of digital rights of citizens and a key prerequisite for the formation of a secure information society.

The relevance of the topic is due to a number of objective factors that require an immediate response from the legal system. The cross-border nature of cyberspace creates significant challenges to traditional principles of jurisdiction. Data can be processed and transferred across borders, making it difficult to apply national legislation and hold offenders accountable, which requires the development of uniform international standards. In addition, the constant development of data processing technologies (e.g. Big Data, artificial intelligence) and the emergence of new business models require a review of existing legal norms. Insufficient legal certainty as to who is responsible for data protection in complex processing chains creates legal gaps that can be exploited by criminals. Equally important is the issue of ensuring a balance between the protection of personal data and other public interests, such as the development of innovation. Insufficiently flexible legislation can become an obstacle to the development of the digital economy, while weak legislation cannot effectively protect citizens' rights.

Key words: personal data, cyberspace, cybersecurity, legal regulation, GDPR, privacy.

Постановка проблеми. Стрімкий розвиток цифрових технологій та глобалізація інформаційних процесів призвели до масового збору, обробки та зберігання персональних даних у кіберпросторі. Це створило нові виклики та загрози для фундаментального права особи на приватність. Незважаючи на вдосконалення технологій безпеки, зростаюча складність кібератак та методів зловживання інформацією вимагає адекватного та ефективного правового реагування. Наявність прогалин у законодавстві та недостатня обізнаність громадян щодо своїх прав роблять питання захисту персональних даних у кіберпросторі надзвичайно актуальним.

Метою статті є дослідження правових засад захисту персональних даних в кіберпросторі.

Стан дослідження. Проблема правового регулювання захисту персональних даних у кіберпросторі є предметом активного обговорення в юридичній науці. Дослідження українських та міжнародних фахівців спрямовані на аналіз нормативно-правової бази, виявлення прогалин у законодавстві та розробку рекомендацій щодо його вдосконалення. Зокрема, у своїх працях Самагальська Ю. Я. та Аніщук В. В. розглядають загальні аспекти захисту даних в мережі Інтернет, акцентуючи увагу на зростаючій складності кіберзагроз. Важливість адаптації українського законодавства до стандартів ЄС, зокрема GDPR, досліджується в роботах Головацького Н. Т. Науковець аналізує принципи прозорості та згоди, а також порівнює українські норми із законодавством США та Канади. Бондаренко О. С. зосереджує увагу на захисті цифрової

особистості, що є невід'ємною частиною захисту персональних даних в цифрову епоху. Загалом, науковці підкреслюють, що, незважаючи на існування законодавства, його реалізація стикається з низкою проблем, пов'язаних із недостатнім усвідомленням ризиків та низьким рівнем обізнаності громадян.

Виклад основного матеріалу. Відповідно до статті 31 Конституції України кожному гарантується таємниця листування, телефонних розмов, телеграфної та іншої кореспонденції. Згідно із положеннями статті 32 Основного Закону ніхто не може зазнавати втручання в його особисте і сімейне життя. Не допускається збирання, зберігання, використання та поширення конфіденційної інформації про особу без її згоди, крім випадків, визначених законом, і лише в інтересах національної безпеки, економічного добробуту та прав людини [1].

Персональні дані – це будь-яка інформація, що стосується ідентифікованої фізичної особи. У кіберпросторі цей термін включає не лише очевидні дані, такі як ім'я, адреса та номер телефону, але й менш явні, зокрема IP-адреси, файли cookie, геолокаційні дані та поведінкові патерни користувачів. Згідно із Законом України «Про захист персональних даних», обробка персональних даних включає будь-яку дію або сукупність дій, таких як збирання, реєстрація, накопичення, зберігання, адаптування, зміна, поновлення, використання і поширення [2]. У контексті кіберпростору це поняття поширюється на всі цифрові транзакції та взаємодії, від звичайного відвідування веб-сайту до купівлі товарів [4, с. 254].

Одним з найважливіших аспектів є захист цифрової особистості, яка є сукупністю цифрових даних, що представляють індивідуальні характеристики, риси та поведінку особи. Ефективний захист цифрової ідентичності є запорукою безпеки та добробуту особи в цифрову епоху.

Особистість, безсумнівно, є однією з найбільш інтригуючих граней людських істот. Цифрова особистість представляє собою складову індивідуальності, що існує в онлайн середовищі. Вона включає в себе різноманітні соціальні, інституційні, правові, наукові та технологічні аспекти, які необхідно розглядати для повного розуміння особистості в цілому. S. Vogel виділяє п'ять видів цифрової особистості:

- відкрита цифрова особистість, яка переконана, що цифрові технології є хорошим способом взаємодії з друзями, клієнтами та партнерами;

- сумлінна цифрова особистість – це та, що навряд чи спробує нову технологію, доки не буде продемонстровано її переваги;

- екстраверт – сприймає нові технології та різноманітні методи спілкування з людьми, часто майже не замислюючись про наслідки, швидше за все, буде мікроблогером через Twitter або користувачем Facebook;

- погодливі цифрові особистості використовуватимуть нові технології, оскільки вони оцінять переваги, які вони можуть принести, але можуть не максимізувати потенціал, оскільки вони хвилюються про те, щоб не набридати чи не заважати людям;

- невротична цифрова особистість цинічно ставиться до нових технологій і схильна відкидати їх; їй навряд чи буде комфортно застосовувати соціальні мережі для ділових відносин [6, с. 335].

Найбільш значущим міжнародним документом у сфері захисту даних є Загальний регламент про захист даних (General Data Protection Regulation, GDPR) Європейського Союзу. GDPR набув чинності у 2018 році. Зазначений нормативно-правовий акт, встановлює високі стандарти захисту для всіх, хто обробляє дані громадян ЄС, незалежно від їхнього місцезнаходження. Серед основних принципів GDPR:

- **Законність, справедливість і прозорість:** дані мають оброблятися на законних підставах, із забезпеченням прозорості для суб'єкта даних.

- **Обмеження мети:** дані повинні збиратися для чітко визначених, законних цілей і не повинні оброблятися в спосіб, несумісний із цими цілями.

- **Мінімізація даних:** збір даних має обмежуватися необхідним мінімумом.

- **Точність:** дані мають бути точними і, за потреби, оновлюватися.

- **Обмеження зберігання:** дані не повинні зберігатися довше, ніж це необхідно для досягнення мети.

- **Цілісність і конфіденційність:** дані повинні бути захищені від несанкціонованої або незаконної обробки. Крім того, GDPR надає суб'єктам даних широкі права, включаючи право на доступ до своїх даних, право на їх виправлення, видалення («право на забуття»), обмеження обробки та перенесення даних [7, с. 289-290].

Законодавство США та Канади також має свої особливості. У США правове регулювання є фрагментованим і залежить від сектора. Зокрема, існують федеральні закони, такі як Закон про переносимість та підзвітність медичного страхування (HIPAA), та державні акти, як-от Закон Каліфорнії про конфіденційність споживачів (CCPA). У Канаді діє Закон про захист особистої інформації та електронних документів (PIPEDA), який також встановлює принципи збирання, використання та розголошення персональних даних у комерційній діяльності [7, с. 291].

Україна активно адаптує своє законодавство до міжнародних, зокрема європейських, стандартів. Основним

нормативним актом є Закон України «Про захист персональних даних». Однак, з огляду на євроінтеграційні процеси, Україна рухається до гармонізації з GDPR, що вимагає внесення суттєвих змін. Законодавство України базується на Конституції України, яка гарантує право на невтручання в особисте життя.

Національне законодавство, як і GDPR, базується на принципах прозорості та згоди. Прозорість забезпечує, що суб'єкти даних розуміють, як їхні дані використовуються, а згода гарантує, що обробка даних відбувається на добровільній основі. Однак, на практиці існують проблеми, пов'язані з невідповідністю положень Закону України реаліям цифрового середовища, а також низьким рівнем обізнаності громадян щодо своїх прав [9, с. 180-181].

Актуальним питанням є також адміністративно-правовий механізм захисту прав інтелектуальної власності, що тісно пов'язаний із захистом персональних даних. Ефективність цього механізму залежить від повноти законодавства та ефективності правозастосування. Особливо варто відзначити роль Закону України «Про основні засади забезпечення кібербезпеки України», який створює основи для захисту інформації в державних та приватних системах.

Основні загрози, з якими стикаються персональні дані в кіберпросторі, включають:

- **Кібератаки:** хакерські атаки, фішинг, шкідливе програмне забезпечення.

- **Витоки даних:** несанкціонований доступ до баз даних, що містять конфіденційну інформацію.

- **Неправомірні обробка:** використання даних без згоди особи, зловживання ними.

- **Технологічні ризики:** розвиток штучного інтелекту створює нові загрози, що вимагають інноваційних підходів до захисту.

Для мінімізації цих ризиків необхідно вживати комплексних заходів, включаючи технічні (шифрування, аутентифікація), організаційні (політики приватності, оцінка впливу на приватність) та правові. Важливою передумовою для підвищення довіри громадян до цифрових сервісів є забезпечення належного захисту їхніх даних [11, с. 70-71].

Слід зауважити, що законодавство України передбачає відповідальність компаній та організацій, які збирають персональні дані, щодо забезпечення належного захисту таких даних від несанкціонованого доступу, втрати чи знищення. Контроль за дотриманням законодавства здійснюється Уповноваженим Верховної Ради України з прав людини. Вказаний орган розглядає скарги громадян, проводить перевірки та може накладати адміністративні стягнення. Громадяни мають право знати, хто і з якою метою обробляє їхні дані, вимагати їх виправлення або видалення, а також відкликати свою згоду на обробку. У разі порушення прав на захист персональних даних, особа може звернутися до суду для відновлення своїх прав і відшкодування шкоди.

Слід підкреслити роль Уповноваженого Верховної Ради України з прав людини у сфері захисту персональних даних, адже право на приватність є одним із основоположних прав людини. Відповідно до норм статті 23 Закону України «Про захист персональних даних» до основних повноважень щодо захисту персональних даних Уповноваженого Верховної Ради України з прав людини, зокрема, належать:

- отримувати пропозиції, скарги та інші звернення фізичних і юридичних осіб з питань захисту персональних даних та приймати рішення за результатами їх розгляду;

- проводити на підставі звернень або за власною ініціативою виїзні та безвиїзні, планові, позапланові перевірки володільців або розпорядників персональних даних в порядку, визначеному Уповноваженим, із забезпеченням відповідно до закону доступу до приміщень, де здійснюється обробка персональних даних;

– за підсумками перевірки, розгляду звернення видавати обов’язкові для виконання вимоги (приписи) про запобігання або усунення порушень законодавства про захист персональних даних, у тому числі щодо зміни, видалення або знищення персональних даних, забезпечення доступу до них, надання чи заборони їх надання третій особі, зупинення або припинення обробки персональних даних;

– звертатися з пропозиціями до Верховної Ради України, Президента України, Кабінету Міністрів України, інших державних органів, органів місцевого самоврядування, їх посадових осіб щодо прийняття або внесення змін до нормативно-правових актів з питань захисту персональних даних;

– складати протоколи про притягнення до адміністративної відповідальності та направляти їх до суду у випадках, передбачених законом;

– інформувати про законодавство з питань захисту персональних даних, проблеми його практичного застосування, права і обов’язки суб’єктів відносин, пов’язаних із персональними даними;

– здійснювати моніторинг нових практик, тенденцій та технологій захисту персональних даних [2].

Варто зазначити, що за порушення законодавства про захист персональних даних передбачена адміністративна, цивільно-правова та кримінальна відповідальність.

Порушення законодавства про захист персональних даних можуть мати серйозні наслідки як для осіб, чії дані були скомпрометовані, так і для компаній або організацій, відповідальних за їх обробку. Одним з основних наслідків є фінансові санкції. Органи регулювання можуть накладати значні штрафи на компанії за порушення законодавства. Наприклад, відповідно до Загального регламенту про захист даних (GDPR) в ЄС, штрафи можуть досягати 4% від річного обсягу бізнесу або 20 мільйонів євро, залежно від того, що більше. В Україні, відповідно до статті 188-39 Кодексу України про адміністративні правопорушення, за порушення законодавства у сфері захисту персональних даних можуть накладатися адміністративні штрафи. Крім того, відшкодування збитків також є важливим аспектом. Постраждалі особи можуть подати позови на відшкодування збитків, завданих витоком або нена належним обробленням їхніх даних. Це може включати як матеріальні, так і нематеріальні збитки, відповідно до статті 1166 Цивільного кодексу України. Згідно зі статтею 182 Кримінального кодексу, незаконні дії щодо збору, зберігання, використання, знищення, поширення або зміни

конфіденційної інформації про особу, якщо це не підпадає під регулювання інших статей Кодексу, тягнуть за собою покарання у вигляді штрафу від п’ятисот до тисячі неоподатковуваних мінімумів доходів громадян, виправних робіт до двох років, арешту до шести місяців або обмеження волі до трьох років [11, с. 70].

Удосконалення законодавчої бази є одним з ключових напрямків у забезпеченні захисту персональних даних. Це передбачає регулярний перегляд та оновлення законодавства з урахуванням нових технологій та викликів. Посилення відповідальності за порушення законодавства шляхом збільшення штрафних санкцій та введення кримінальної відповідальності за найсерйозніші правопорушення також є важливим кроком. Крім того, необхідно створити чіткі та зрозумілі визначення ключових понять, щоб уникнути неоднозначностей у застосуванні закону. Окрему увагу слід приділити регулюванню нових технологій, таких як штучний інтелект та блокчейн, які відкривають нові можливості для обробки персональних даних, але водночас створюють нові ризики [11, с. 70-71].

Висновки. Правовий механізм захисту персональних даних в кіберпросторі є складним і динамічним процесом. В Україні вже діє певний алгоритм захисту персональних даних у кіберпросторі. Зазначений алгоритм базується як на основі норм національного права, так і на основі норм міжнародних актів, зокрема актів Європейського Союзу.

Попри значний прогрес у покращенні механізмів захисту персональних даних у кіберпросторі, українське законодавство, що регулює захист персональних даних, все ще потребує гармонізації з європейськими стандартами, зокрема з GDPR. Ефективність правового регулювання залежить не лише від наявності відповідних законів, а й від рівня обізнаності громадян та усвідомлення володільцями даних своєї відповідальності. Захист персональних даних має розглядатися в комплексі, поєднуючи правові, технічні та організаційні заходи. З огляду на стрімкий розвиток технологій, правові норми повинні бути гнучкими та адаптивними, щоб відповідати новим викликам.

У майбутньому необхідно зосередитися на розробці та впровадженні більш суворих законодавчих норм, посиленні державного контролю, а також підвищенні рівня цифрової грамотності населення. Лише комплексний підхід дозволить забезпечити надійний захист персональних даних та гарантувати право на приватність у цифрову епоху.

ЛІТЕРАТУРА

1. Конституція України : від 28.06.1996 № 254к/96-ВР : станом на 1 січ. 2020 р. URL: <https://zakon.rada.gov.ua/laws/show/254k/96-vr#Text>
2. 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>
3. Про основні засади забезпечення кібербезпеки України : Закон України від 05.10.2017 № 2163-VIII : станом на 20 квіт. 2025 р. URL: <https://zakon.rada.gov.ua/laws/show/2163-19#Text>
4. Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року «Про Стратегію кібербезпеки України» : Указ Президента України від 26.08.2021 № 447/2021. URL: <https://zakon.rada.gov.ua/laws/show/447/2021#Text>
5. 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
6. Бондаренко О. С., Думчиков М. О. Захист цифрової особистості: вивчення досвіду Європейського Союзу та України // № 1. 2024. URL: <https://doi.org/10.32782/2524-0374/2024-1/75>
7. Головацький Н. Т. Правове регулювання захисту персональних даних: GDPR та законодавство США, Канади й України // Серія ПРАВО. Вип. 85, ч. 2. 2024. URL: <https://doi.org/10.24144/2307-3322.2024.85.2.42>
8. Анішук В. В. Проблема захисту персональних даних в кіберпросторі // Серія ПРАВО. Вип. 84, ч. 3. 2024. С. 62-64. URL: <https://doi.org/10.24144/2307-3322.2024.84.3.38>
9. Головацький Н. Т. Прозорість та згода як основні принципи захисту персональних даних в Україні // Серія ПРАВО. Вип. 83, ч. 2. 2024. URL: <https://doi.org/10.24144/2307-3322.2024.83.2.25>
10. Самагальська Ю. Я. Захист персональних даних в мережі Інтернет // Науковий вісник Ужгородського Національного Університету. 2024. URL: <https://doi.org/10.24144/2307-3322.2024.82.2.41>
11. Биков О. М., Савченко В. В. Захист персональних даних у сучасному законодавстві // Legal Bulletin. № 4 (14). 2024. С. 7-11. URL: <https://doi.org/10.31732/2708-339X-2024-14-A9>
12. Закон про захист особистої інформації та електронних документів (PIPEDA), Канада, 2000. URL: <https://laws-lois.justice.gc.ca/eng/acts/p-8.6/index.html>