УДК 342.721:004.738.5].009.1(4-672ЄС+73+71+477)
DOI https://doi.org/10.24144/2307-3322.2024.85.2.42

ПРАВОВЕ РЕГУЛЮВАННЯ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ: GDPR ТА ЗАКОНОДАВСТВО США, КАНАДИ Й УКРАЇНИ

Головацький Н.Т.,
старший викладач
кафедри адміністративного, фінансового
та інформаційного права
юридичного факультету ДВНЗ «УжНУ»

Головацький Н.Т. Правове регулювання захисту персональних даних: GDPR та законодавство США, Канади й України.

У статті проведено детальний аналіз правового регулювання захисту персональних даних у різних юрисдикціях, зокрема в Європейському Союзі, США, Канаді та Україні. Особливу увагу приділено Загальному регламенту захисту даних (GDPR), який є одним із найсуворіших міжнародних стандартів у цій сфері. Розглянуто основні положення GDPR, такі як принципи законності, чесності, прозорості, обмеження мети та мінімізації даних, а також права суб'єктів даних, включно з правом на доступ, виправлення та видалення даних. Проаналізовано вплив GDPR на міжнародний бізнес, що змусило компанії по всьому світу адаптувати свої системи обробки даних для дотримання вимог європейського законодавства.

У розділі про США акцент зроблено на законодавстві штату Каліфорнія, зокрема на California Consumer Privacy Act (CCPA), який надає громадянам права на контроль над їхніми персональними даними. Хоча законодавча база в США є фрагментарною, порівняно з GDPR, CCPA є важливим кроком у захисті приватності американських громадян.

Канадське законодавство представлено через Personal Information Protection and Electronic Documents Act (PIPEDA), який забезпечує захист персональних даних у комерційних відносинах. PIPEDA передбачає збалансованість між інтересами бізнесу та правами громадян, забезпечуючи гнучкість у використанні персональних даних, з одночасним дотриманням принципів прозорості та згоди.

Окремо проаналізовано процес гармонізації законодавства України із GDPR, що є важливим етапом у контексті інтеграції країни до європейського правового простору. Реформування українського законодавства зосереджено на посиленні захисту прав громадян та вдосконаленні механізмів контролю за обробкою персональних даних.

Стаття пропонує порівняльний аналіз розглянутих законодавств, виявляючи ключові відмінності у підходах до захисту даних. На відміну від ЄС, де регулювання є всеохоплюючим і суворим, у США спостерігається фрагментація законів. У Канаді, завдяки PIPEDA, існує більш гнучка система, орієнтована на комерційний сектор. Україна, натомість, знаходиться на шляху до повної гармонізації з європейськими стандартами, що дозволить зміцнити правовий захист громадян в умовах цифрової економіки.

Ключові слова: захист персональних даних, GDPR, CCPA, PIPEDA, законодавство України, конфіденційність, права суб'єктів даних, порівняльне право.

Holovatskiy N.T. Legal regulation of personal data protection: GDPR and the legislation of the USA, Canada, and Ukraine.

The article provides a detailed analysis of the legal regulation of personal data protection in various jurisdictions, including the European Union, the United States, Canada, and Ukraine. Special attention is given to the General Data Protection Regulation (GDPR), which is one of the strictest international standards in this field. The main provisions of the GDPR are examined, such as the principles of lawfulness, fairness, transparency, purpose limitation, and data minimization, as well as the rights of data subjects, including the right to access, rectification, and erasure of data. The impact of GDPR on

international businesses is analyzed, showing how it has forced companies worldwide to adapt their data processing systems to comply with European legal requirements.

The section on the United States focuses on California state law, particularly the California Consumer Privacy Act (CCPA), which grants citizens rights over their personal data. Although the U.S. legislative framework is fragmented compared to GDPR, the CCPA is a significant step toward protecting the privacy of American citizens.

Canadian legislation is represented by the Personal Information Protection and Electronic Documents Act (PIPEDA), which ensures the protection of personal data in commercial relationships. PIPEDA strikes a balance between business interests and citizens' rights, providing flexibility in the use of personal data while adhering to principles of transparency and consent.

The article also analyzes the process of harmonizing Ukraine's legislation with the GDPR, which is a crucial step in the context of the country's integration into the European legal space. Ukrainian legal reforms focus on strengthening citizens' rights and improving mechanisms for controlling personal data processing.

The article offers a comparative analysis of the discussed legal systems, highlighting key differences in data protection approaches. Unlike the EU, where regulation is comprehensive and stringent, U.S. laws are fragmented. In Canada, PIPEDA creates a more flexible system oriented toward the commercial sector. Ukraine, meanwhile, is on its way to full harmonization with European standards, which will enhance the legal protection of citizens in the digital economy.

Key words: personal data protection, GDPR, CCPA, PIPEDA, Ukrainian legislation, privacy, data subject rights, comparative law.

Постановка проблеми. Захист персональних даних став однією з ключових тем сучасної правової системи у зв'язку з глобалізацією, цифровізацією та розвитком новітніх технологій. У багатьох країнах приймаються нові закони або адаптуються існуючі для захисту персональних даних громадян. Зокрема, Європейський Союз ухвалив Загальний регламент захисту даних (GDPR), який встановлює жорсткі стандарти для захисту персональних даних, не лише в межах ЄС, але й для інших держав, що обробляють персональні дані громадян ЄС. Водночас такі країни, як США, Канада та Україна, мають різні підходи до регулювання цієї сфери.

Аналіз останніх досліджень і публікацій. Питанням правового регулювання захисту персональних даних сьогодні приділяється багато уваги, адже вони носять значущий характер як із теоретичної, так і з практичної точки зору для суб'єктів, які беруть участь в обробці персональних даних. Тому, багато науковців приділяють значну увагу визначеним питанням.

До висвітлення окресленої проблематики варто відзначити таких науковців, як: І.С. Похиленко, К.М. Врублевська-Місюна, В.П. Тичина, М.В. Бем, В.М. Брижко, Т.О. Гуржій, А.Л. Петрицький, В.Л. Костюк, С.С. Лукаш, Н.О. Мельничук, М.О. Міщук, О.В. Москаленко, О.М. Обушенко та багато інших.

У наукових працях зазначених науковців приділено значну увагу правового регулювання захисту персональних даних. Проте, існує проблема відсутності механізму, який дав би змогу виключити оприлюднення конфіденційної інформації в джерелах, не передбачених чинними законодавчими нормами.

Мета статті. Порівняння підходів до захисту персональних даних в Європейському Союзі (на основі GDPR), США (включно з California Consumer Privacy Act – CCPA), Канаді (Personal Information Protection and Electronic Documents Act – PIPEDA) та Україні (законодавство щодо персональних даних та гармонізація із GDPR).

Виклад основного матеріалу. Для початку проведення дослідження варто окреслити структуру та ключові положення Загального регламенту захисту даних (GDPR). GDPR був ухвалений Європейським Союзом та набув чинності у 2016 році та повноцінно почав застосовуватись лише у травні 2018 року. Його метою є посилення прав громадян на захист своїх даних та встановлення суворих вимог при опрацюванні їх персональних даних. Основними принципами GDPR є:

– Законність, правомірність і прозорість;
– Цільове обмеження;
– Мінімізація даних;
– Точність;
– Обмеження зберігання;

– Цілісність і конфіденційність;
– Підзвітність.

Ці принципи є основоположними для будь-якої організації, що обробляє персональні дані громадян ЄС, незалежно від її географічного розташування.

В розумінні Загального регламенту захисту даних (GDPR) «персональні дані» це будь-яка інформація, яка стосується фізичної особи, яку ідентифіковано чи можна ідентифікувати («суб'єкт даних»); фізична особа, яку можна ідентифікувати, є такою особою, яку можна ідентифікувати, прямо чи опосередковано, зокрема, за такими ідентифікаторами як ім'я, ідентифікаційний номер, дані про місцеперебування, онлайн-ідентифікатор або за одним чи декількома факторами, що є визначальними для фізичної, фізіологічної, генетичної, розумової, економічної, культурної чи соціальної сутності такої фізичної особи. Тут варто відзначити, що на відміну від Закону України «Про захист персональних даних», перераховані чіткі критерії, які визначають дані, що віднесені до конкретної ідентифікації особи.

А опрацюванням персональних даних GDPR розуміє будь-яку операцію або низку операцій з персональними даними або наборами персональних даних з використанням автоматизованих засобів або без них, такі як збирання, реєстрація, організація, структурування, зберігання, адаптація чи зміна, пошук, ознайомлення, використання, розкриття через передавання, розповсюдження чи надання іншим чином, упорядкування чи комбінування, обмеження, стирання чи знищення [1].

GDPR має глобальний вплив на міжнародний бізнес, оскільки він зобов'язує компанії з інших країн, які працюють із громадянами ЄС, дотримуватися його норм. Після його впровадження багато великих корпорацій, таких як Google і Facebook, зіткнулися зі значними штрафами за порушення цих норм. GDPR встановив високі стандарти щодо обробки даних і відповідальності за порушення, що сприяло активній адаптації компаній до нових вимог.

В перший же день після набрання чинності нормами Регламенту, надійшли перші ж скарги за порушення GDPR. Необхідність чіткого правового регулювання питань щодо порушення права особи на конфіденційність показує не лише теорія, а й судова практика. Контролери та процесори несуть відповідальність не лише за витік даних, але і за будь-яку невідповідність стандартам GDPR. В історії GDPR.

Два з п'яти найбільших штрафів було накладено за невідповідність положенням GDPR. 1) у «Справі Google LLC» французький DPA (CNIL) за скаргами приватних позивачів (суб'єктів даних) наклав штраф у розмірі 50 млн євро за невиконання зобов'язання щодо прозорості та поінформованості і нездатність отримати дійсну правову основу для обробки даних. Штраф у «Справі Google LLC» є найбільшим штрафом GDPR із досі накладених; та 2) у «Справі Deutsche Wohnen SE» німецький DPA наклав штраф у розмірі 14,5 млн євро за неможливість встановити систему зберігання даних, яка б могла стерти дані, які вже не потрібні для цілей обробки. Такий значний штраф був зменшений (DPA міг накласти до 28 млн євро), тому що порушник намагався виправити порушення і DPA не зміг довести, що порушення призвело до витоку чи іншого несанкціонованого розголошення. «Справа Deutsche Wohnen SE» залишається четвертим за величиною штрафом в історії GDPR [7].

У США немає єдиного національного закону щодо захисту персональних даних, подібного до GDPR. Проте на штатному рівні діють різні акти, найвідомішим з яких є California Consumer Privacy Act (CCPA), ухвалений у 2018 році. CCPA надає жителям Каліфорнії право знати, які їхні дані збирають компанії, вимагати видалення цих даних та забороняти їх продаж [2].

Основними характеристиками CCPA можна відзначити:

1. Право на доступ до інформації: Споживачі мають право дізнатися, які саме їхні персональні дані збираються компаніями, як вони використовуються і кому передаються.
2. Право на видалення даних: Споживачі можуть вимагати від компаній видалити їхні персональні дані, якщо ці дані більше не потрібні для бізнесових цілей.
3. Право на відмову від продажу даних: Закон дає можливість споживачам забороняти продаж їхніх персональних даних третім сторонам. Компанії повинні надавати легкий доступ до цієї функції, часто через посилання «Do Not Sell My Personal Information» на своїх сайтах.
4. Захист неповнолітніх: CCPA забороняє компаніям продавати персональні дані осіб молодших 16 років без явної згоди, причому для дітей молодших 13 років потрібна згода батьків.
5. Зобов'язання компаній: Компанії, що обробляють дані більш ніж 50 000 користувачів на рік або мають річний дохід більше ніж $25 мільйонів, зобов'язані дотримуватися цього закону.

6. Штрафи та відповідальність: CCPA передбачає штрафи за порушення закону, а також можливість подачі позовів від споживачів у разі витоку даних. Штрафи можуть досягати $7,500 за умисні порушення.

CCPA став першим значним кроком у США для посилення захисту приватності та даних, подібно до європейського GDPR, і надав резидентам Каліфорнії нові можливості для захисту своїх цифрових прав.

Окрім CCPA, у США діють також інші закони, що регулюють обробку персональних даних у певних секторах, такі як Health Insurance Portability and Accountability Act (HIPAA), що регулює медичні дані, та Gramm-Leach-Bliley Act (GLBA), який регулює дані у фінансовому секторі.

Канада регулює захист персональних даних через Personal Information Protection and Electronic Documents Act (PIPEDA), який був ухвалений у 2000 році. PIPEDA стосується захисту персональних даних, зібраних комерційними організаціями, і надає громадянам Канади право доступу до своїх даних та їх корекції.[3]

Personal Information Protection and Electronic Documents Act (PIPEDA), ухвалений у 2000 році, є основним канадським законом, що регулює захист персональних даних у комерційних відносинах. Він застосовується до приватного сектору, забезпечуючи баланс між правами громадян на захист своїх даних і потребами бізнесу. Ось головні характеристики цього закону:

1. Згода на обробку даних: PIPEDA вимагає, щоб компанії отримували явну або неявну згоду на збір, використання та розкриття персональних даних. Споживачі повинні бути чітко поінформовані про те, як будуть використовуватись їхні дані.
2. Прозорість: Компанії зобов'язані повідомляти громадянам про цілі збору даних і про те, як ці дані будуть використовуватись. Споживачі мають право знати, хто володіє їхніми даними і як вони будуть оброблятись.
3. Право на доступ і корекцію: PIPEDA надає громадянам право доступу до своїх персональних даних, які зберігаються компаніями, та можливість виправити неточності у своїй інформації.
4. Обмеження збирання даних: Закон зобов'язує компанії збирати лише необхідні персональні дані для виконання конкретних цілей, які визначаються на етапі отримання згоди.
5. Відповідальність компаній: PIPEDA зобов'язує компанії відповідально поводитися з даними та забезпечувати належний рівень захисту під час їх зберігання, передачі та використання.
6. Комісар з питань конфіденційності: Закон забезпечує нагляд за його виконанням через Офіс комісара з питань конфіденційності Канади. Комісар може розглядати скарги та проводити розслідування щодо можливих порушень закону.
7. Електронні документи: Окрім захисту персональних даних, PIPEDA також регулює використання електронних документів у комерційних операціях, підтримуючи перехід бізнесу на цифрові технології.

PIPEDA спрямований на створення справедливого і прозорого процесу обробки даних, дозволяючи підприємствам працювати ефективно, з одночасним захистом прав споживачів. Закон надає гнучкість у використанні даних, проте під суворим наглядом і контролем за дотриманням згоди та прозорості.

На відміну від GDPR, PIPEDA більше зосереджується на балансі між захистом персональних даних і свободою бізнесу, надаючи більше гнучкості у використанні даних. Водночас PIPEDA також підкреслює важливість згоди громадян на обробку їхніх даних.

Україна активно працює над гармонізацією свого законодавства щодо захисту персональних даних із європейськими стандартами. Основним нормативно-правовим актом є Закон України «Про захист персональних даних», який був прийнятий у 2010 році [4]. У 2021 році розпочалася активна робота над приведенням цього закону у відповідність до GDPR. Так, 25 жовтня 2022 року у Верховній Раді України було зареєстровано Проект Закону про захист персональних даних [5]. У пояснювальній записці цього законопроекту визначено, що необхідність прийняття цього проекту Закону обумовлена тим, що стан законодавства не в повній мірі забезпечує захист персональних даних в Україні, що зумовлено значним розвитком міжнародних стандартів у цій сфері, та постійне впровадження європейських стандартів і процес до повного членства в ЄС вимагають оновлення українського регулювання захисту персональних даних до європейських стандартів. Такої ж думки притримується і науковець Похиленко І.С. [6].

Останні наукові праці, свідчать про важливість гармонізації українського законодавства із європейськими стандартами. Це дозволяє Україні інтегруватися в європейський правовий простір і забезпечити належний захист даних громадян.

Незважаючи на різницю у правових системах, усі розглянуті юрисдикції мають на меті забезпечення базових прав громадян щодо обробки їхніх персональних даних. Усі системи передбачають право на доступ до даних, їх виправлення та видалення.

Висновки. Отже, основною відмінністю між GDPR та іншими юрисдикціями є суворість санкцій та контроль за дотриманням законодавства. Водночас, у США, окрім CCPA, немає єдиного загального закону, що регулює персональні дані на федеральному рівні. У Канаді ж відсутня сувора регламентація щодо згоди на обробку даних, порівняно з GDPR.

Захист персональних даних є надзвичайно важливою частиною сучасного правового регулювання. Порівняльний аналіз різних підходів показує, що GDPR став глобальним стандартом, на який орієнтуються багато країн. У той же час США та Канада розробляють власні моделі, що більше враховують інтереси бізнесу. Україна ж продовжує гармонізувати своє законодавство з європейськими стандартами, що відкриває нові можливості для захисту прав громадян та розвитку цифрової економіки.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. 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#Text.
2. California Consumer Privacy Act (CCPA), 2018. URL: https://cdp.cooley.com/ccpa-2018.
3. Personal Information Protection and Electronic Documents Act (PIPEDA), Canada, 2000. URL: https://laws-lois.justice.gc.ca/eng/acts/p-8.6/index.html.
4. Закон України «Про захист персональних даних». URL: https://zakon.rada.gov.ua/laws/show/2297-17#Text.
5. Проект Закону про захист персональних даних. URL: https://itd.rada.gov.ua/ billInfo/Bills/Card/40707.
6. Похиленко І.С. Правове регулювання захисту персональних даних/ *Юридичний вісник*, № 4 (69), 2023. URL: https://repositary.knuba.edu.ua/server/api/core/bitstreams/c8d1205c-81c6-4eb9-b57d-e5b6fd363a43/content.
7. Врублевська-Місюна К.М., Тичина В.П. Міжнародно-правові стандарти захисту інформації про особу. *Науковий вісник УжНУ*. Серія: Право. Том 2. № 74 (2022). URL: https://visnyk-juris-uzhnu.com/wp-content/uploads/2023/01/28-1.pdf.
8. Бєлова М.В., Бєлов Д.М., Виклики та загрози захисту персональних даних у ро- боті зі штучним інтелектом. *Науковий віс- ник УжНУ. Серія «Право».* Випуск 79(5). 2023. С. 289–294.
9. Бєлов Д.М., Бєлова М.В., Штучний інтелект в судочинстві та судових рішеннях, потенціал та ризики. *Науковий вісник УжНУ. Серія «Право».* Випуск 78(4). Ч. 3. 2023. С. 122–129.
10. Лазур Я.В. Забезпечення прав і свобод громадян України у сфері публічного управління: адміністративно-правовий механізм: монографія. К.: Четверта хвиля. 2010. 240 с.
11. Лазур Я.В. Поняття, сутність та елементи адміністративно-правового механізму забезпечення прав і свобод громадян у державному управлінні. *Форум права*. 2009. № 3. С. 392–398.