

## ІСТОРИКО-ПРАВОВИЙ АСПЕКТ РОЗВИТКУ ПІДХОДІВ ДО ФОРМУВАННЯ ПЕРСОНАЛЬНИХ ДАНИХ

### HISTORICAL AND LEGAL ASPECT OF THE DEVELOPMENT OF APPROACHES TO THE FORMATION OF PERSONAL DATA

Дяковський О.С., к.ю.н.,

викладач кафедри інформаційного, господарського та адміністративного права

*Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського»*

У статті досліджується історико-правовий аспект розвитку підходів до формування персональних даних. Активне впровадження технологій та цифровізація суспільства призвели до значного зростання обсягів персональних даних, що збираються, зберігаються та обробляються державними органами та приватними компаніями. У цьому контексті важливим є аналіз історичних етапів та правових норм, які вплинули на формування сучасного підходу до захисту персональних даних.

Автор роботи приділяє увагу еволюції правового регулювання персональних даних у різних правових системах світу. В статті розглянуто історичні передумови виникнення і розвитку концепції захисту персональних даних, починаючи від перших спроб правового регулювання цього питання у XX столітті до сучасних нормативно-правових актів, таких як Загальний регламент про захист даних (GDPR) в Європейському Союзі та інші директиви. Розкрито також особливості становлення інституту персональних даних на рівні окремих країн (Франція, Німеччина, США).

Значна увага приділена порівняльному аналізу розвитку правового регулювання в різних країнах, що дозволяє виокремити спільні риси та відмінності у підходах до формування і захисту персональних даних. Також у роботі розглядаються ключові виклики, з якими стикаються законодавці у процесі адаптації правових норм до сучасних реалій, таких як глобалізація, розвиток інтернету та соціальних мереж, штучний інтелект та великі дані. На основі проведеного аналізу розкрито генезу розвитку інституту персональних даних та визначено ключові аспекти, що вплинули на поточний стан правового регулювання. У висновках підкреслюється важливість інтеграції правових норм різних держав для ефективного захисту персональних даних у глобалізованому світі.

**Ключові слова:** персональні дані, правове регулювання, захист даних, історичний розвиток, GDPR, міжнародне право.

The article examines the historical and legal aspect of the development of approaches to the formation of personal data. The development of technology and the digitalization of society have led to a significant increase in the amount of personal data collected, stored and processed by public authorities and private companies. In this context, it is important to analyze the historical stages and legal norms that have influenced the formation of the modern approach to personal data protection.

The authors of this paper pay attention to the evolution of legal regulation of personal data in different legal systems of the world. The article examines the historical background of the emergence and development of the concept of personal data protection, starting from the first attempts to regulate this issue in the XX century to modern legal acts, such as the General Data Protection Regulation (GDPR) in the European Union and other national laws. The author also reveals the peculiarities of the formation of the personal data institute at the level of individual countries (France, Germany, and the USA).

Considerable attention is paid to a comparative analysis of the development of legal regulation in different countries, which allows to identify common features and differences in approaches to the formation and protection of personal data. The article also discusses the key challenges faced by legislators in the process of adapting legal norms to modern realities, such as globalization, development of the Internet and social networks, artificial intelligence and big data. Based on the analysis, the author reveals the genesis of the development of the personal data institute and identifies the key aspects which have influenced the current state of legal regulation. The conclusions emphasize the importance of integrating the legal norms of different countries for the effective protection of personal data in the globalized world.

**Key words:** personal data, legal regulation, data protection, historical development, GDPR, international law.

**Актуальність теми.** У XXI ст. світ переживає справжню революцію в галузі інформаційних технологій та комунікацій, що безпосередньо впливає на всі сфери людської діяльності, зокрема, на правові аспекти використання та захисту персональних даних. З розвитком цифрових технологій, питання збереження, обробки та передачі персональних даних стає однією з найактуальніших тем у сучасному суспільстві.

Не зважаючи на цілу низку проблематик, пов'язаних із доступом, поширенням, обробкою персональних даних, жодна із правових систем так і не віднайшла оптимальний підхід, який би дозволив нівелювати потенційні ризики в даному сегменті. В даному контексті, досвід минулого може бути корисним інструментом для прогнозування майбутніх змін у законодавстві та для формування більш ефективних правових механізмів захисту персональних даних.

**Актуальність теми** також визначається зростаючою увагою до захисту персональних даних на міжнародному рівні. В умовах глобалізації і збільшення транскордонних інформаційних потоків питання уніфікації правових норм набуває все більшого значення. Аналіз історико-правових підходів до регулювання персональних даних у різних країнах дозволяє створити базу для гармонізації законодавства на міжнародному рівні, що є необхідним для ефективного захисту прав і свобод людини в інформаційному просторі.

Ідентичне питання перебуває в полі наукових пошуків таких вчених як Бем М. В., Городиський І. М., Саттон Г., Родіоненко О. М., які комплексно підходять до вивчення історичного та правового аспекту розвитку інституту персональних даних як в Україні, так і на європейських просторах [1]. Цінним теоретичним доробком в контексті проведеного нами дослідження стала монографія Гуржій Т. О. [2]. Досить ґрунтовно до питання аналізу міжнародного досвіду в частині розвитку інституту захисту персональних даних підходить Золотар О. О. [3] та Сопліко І. М. [9].

**Мета дослідження** – ідентифікація основних етапів розвитку правових норм, які регулюють персональні дані та виявлення ключових чинників, що вплинули на формування сучасних стандартів захисту персональних даних.

**Виклад основного матеріалу.** Час зародження інституту захисту персональних даних, загалом, ідентифікують II пол. XX ст., коли лише починають з'являтися інформаційні технології, сприяючи при цьому обробці значної кількості даних. Рада Європи, безперечно, не може залишити поза увагою масовий вплив, який здійснює поширення і загальна доступність технологій та окремих цифрових продуктів на соціум. Таким чином, у 1968 парламентська асамблея видає один із перших офіційних документів – рекомендацію № 509 – зміст якої транслює всю стурбованість потенційним впливом сучасних тех-

нологій обробки даних на приватність [3]. За тим, комітет з прав людини розпочинає більш детальне вивчення даного питання, у зв'язку з чим відправною точкою в історії розвитку інституту персональних даних прийнято вважати саме даний момент.

На наш погляд, все не так однозначно, як трактують у більшості наукових джерел. Зокрема, слід звернути увагу на кінець XIX ст., коли у світ виходить публікація американських юристів Уорена С. Д. та Блейданса Л. Д. під назвою «Право на приватне життя». В опублікованому у HarvardLawReview дослідженні особлива увага приділена так званому «праву бути залишеним» (дослівно: «righttobeletalone») [14]. Звісно, без належного нормативно-правового закріплення, проте із досить ґрунтовним тлумаченням змісту поняття, – вже в той час воно перебувало в полі теоретико-правових дискусій.

Фактично, першість у прийнятті відповідного профільного Закону належить Федеративній Республіці Німеччина. При чому, прийнятий закон мав локальний характер, адже у 1970 році він набирає чинності на території землі Гессен. Відповідний резонанс мала і світова спільнота. Так, вже за 4 роки на території США було прийнято документ під назвою Privacy Act, де конгресом було вперше зафіксовано чітку лінію між правом на особисте життя та персональними даними. Норми зазначеного документу пронизані єдиною думкою: окремі аспекти особистого життя людини в тій чи іншій мірі можуть стати відомими (розкритими, порушеними) в процесі збору, розповсюдження, використання персональних відомостей органами державної влади [1]. Цікаво, що було конкретизовано і суб'єкта, який проводить окремі маніпуляції із такого роду даними, адже на той час законодавець не допускав ймовірність аналогічних дій зі сторони приватного сектору, до прикладу, суб'єктів господарювання. Відповідно, що у першому (німецька практика), що у другому (американський досвід) випадку, назвати прийняті законодавчі акти повноцінним документом буде не коректно, але фактично мова йде про перші етапи виходу права на захист персональних даних з-під егиди права на особисте життя.

В подальшому, Федеративна Республіка Німеччина продовжує тримати першість у питанні розвитку законодавства щодо захисту персональних даних. Так, у 1977 році набирає законної сили перший національний закон – Bundesdatenschutzgesetz.

За тим, до лав країн, які ставлять в пріоритеті питання захисту персональних даних доєднується і Франція. У 1978 році тут приймають Закон «Про інформатику і цивільні свободи», передумовою для узаконення якого стали події 70-х рр. Французька влада запускає проект SAFARI, застосовуючи при цьому цифрові технології із обробки великої кількості даних, для створення єдиного реєстру. Мета платформи полягає у формуванні бази для ідентифікації будь-якого із громадян завдяки номеру, присвоєного за соціальним страхуванням. На використання вказаних технологій гостро реагують засоби масової інформації, публікуючи лонґрид під назвою «SAFARI чи полювання на французів», тим самим провокуючи один із досить масштабних скандалів на рахунок контролю і масового відслідковування владою всіх громадян. Відповідно, саме суспільне невдоволення призвело до відміни проекту та переорієнтації курсу на обмеження в обробці персональних даних. Таким чином, французький і німецький досвід дають значний поштовх для подальшого розвитку даної сфери, як по європейській території, так і за її межами. До даної проблематики все частіше апелюють більша кількість держав та міжнародних організацій.

Із 1980 року прослідковується значна кількість досягнень і нововведень у зазначеному напрямку. Організація економічної співпраці та розвитку видає нагора Guideline із рекомендаціями по захисту персональних даних, зважаючи на стрімкий розвиток комп'ютерних технологій

та їх застосування в спектрі комерційних транзакцій. Вже наступного року було прийнято перший із числа міжнародних договорів щодо персональних даних, який ввійшов в історію права під назвою Конвенція про захист фізичних осіб при автоматизованій обробці персональних даних, що стала великим консолідованим напрацюванням у своїй сфері. До речі, велика кількість положень із вказаного документу лягла в основу вітчизняного закону про захист персональних даних.

Головна проблема в сфері захисту персональних даних кін. XX – поч. XXI ст. – поява Інтернету та його швидкісний розвиток. В результаті аналізу цілої низки потенційних загроз, ЄС у 1995 році приймає Рамкову Директиву по захисту персональних даних [12], ключова ціль якої полягає в уніфікації законодавства держав-членів на предмет захисту персональних даних. За основу, при розробці тексту документу, було взято механізми, котрі передбачені міжнародною конвенцією 1981 року [4]; окрім зазначеного, було розроблено принципово нові вимоги до операторів персональних даних, а також регламентовано права для громадян ЄС.

Ситуація докорінно змінюється із формуванням та виходом на ринок таких цифрових монополістів, які формують в мережі велику п'ятірку GAFAM (Google, Amazon, Facebook, Apple, Microsoft). Пошукові системи, за відсутністю прямих джерел капіталізації й примноження фінансів, розпочинають активно просувати на своїх платформах рекламу, що базується на засадах аналізу поведінки користувачів. Останнє фактично і відображає сутність таргетованої реклами. Розтлумачимо декілька основних технічних нюансів: кожному із користувачів умовно присвоюється так званий ID-код, який дає змогу відслідкувати потенційні покупки, переваги, побажання клієнтів (користувачів) цифрових ресурсів. В процесі накопичення необхідної кількості відомостей, вони агрегуються в єдиний профіль, тим самим дають змогу пропонувати коректну продукцію. За тим, контекстна реклама стає досить швидко затребуваною, що розуміють і використовують інші цифрові гіганти.

В першу чергу, задля релевантності реклами, котра пропонується різним групам аудиторії, перелічені суб'єкти активно збирають значну кількість персональних даних, щоб сформувати так званий портрет кожного користувача. Цифрові технології дають змогу оперативно аналізувати та перенаправляти такий масив інформації фактично до країни, яка ніколи не відрізнялася розвинутим законодавством в сфері захисту персональних даних. Європейська спільнота не могла ігнорувати подібний розвиток подій, у зв'язку з чим, 2009 року було прийнято Директиву ePrivacy. Документ по більшій мірі встановлює порядок застосування cookies-файлів та ідентифікує особливості збору цифрових даних для реклами [11].

Проте сам користувач далеко не у всіх випадках усвідомлює яка інформація, ким та з якою метою обробляється/передається, адже відсутня цифрова гігієна і звичка уважно читати згоду про обробку персональних даних. Хоча одне лише відвідування сайту надає інформацію про пристрій, з якого отримано доступ; історію покупок; критерії відбору продуктів; IP-адресу; стать; взаємодію із іншими мобільними додатками та соціальними мережами. Відповідно, потенціал цифрових технологій відкриває можливість для самостійного збору великої кількості даних із застосування складного програмного забезпечення, або в якості альтернативи дає змогу купувати ці ж дані у інших суб'єктів.

Частково можна відмітити і позитивні сторони стосовно роботи персоналізації і таргетингу. До прикладу, саме завдяки вказаним технологіям користувачі отримують вже відфільтровані пропозиції щодо продуктів чи послуг, тим самим нівелюючи необхідність додаткового пошуку альтернатив. В свою чергу, споживач має розуміти специфіку роботи алгоритмів; перелік відомостей, які збираються, оброблюються.

Досить загострюється ситуація в даному напрямку після подій із WikiLeaks. Некомерційна організація проаналізувала та опублікувала низку важливих документів, котрі стали їй відомими в результаті витоку інформації (до прикладу, статистичні дані відносно корупції в Кенії, видатки на війну в Афганістані тощо). Ресурс також давав змогу стати анонімним джерелом інформації будь-кому, хто цього забажає.

Все частішими стають хакерські атаки як результат ціленаправленої роботи зловмисників (до прикладу, сайт знайомств для осіб, які вже перебувають в шлюбі Ashley Madison із переліком персональних даних було викладено в мережу), так і в силу людської халатності та цифрової безграмотності. До речі, кейс із сайтом знайомств в історії розвитку інституту персональних даних був досить показовим, адже це призвело не лише до масової кількості розлучень по всьому світу та навіть окремих випадків суїциду, але й мало наслідком те, що у вільному доступі опинилося більше ніж 1000 персональних даних осіб із Саудівської Аравії. За законодавством мусульманської країни, у випадку зради одним із партнерів, з-поміж видів покарання може бути застосовано і смертну кару. Саме тому, не слід ігнорувати чи недооцінювати значення та роль інституту персональних даних у сучасному світі.

В світлі зазначеного, ЄС приймає цілком обґрунтоване рішення відносно потреби у модернізації законодавства та застосування всіма державами-членами ЄС однакового підходу, без суттєвих розбіжностей на рівні національного законодавства. Більше 5 років, починаючи із 2012, тривали дискусії щодо тексту нової Директиви, який міг би бути апробований кожною із держав. Як результат, було видано Детальний аналіз GDPR. Але на цьому законотворча діяльність ЄС в системі координат персональних даних не завершується. Очевидною стає проблема відсутності регламентації на рівні кримінального законодавства, адже положення документу не охоплюють даний напрямок. У зв'язку із зазначеним, у 2016 році приймають Директиву щодо захисту фізичних осіб при автоматизованій обробці персональних даних державними органами з метою попередження, розшуку, виявлення та переслідування кримінальних злочинів [13]. Цього ж року було прийнято і Директиву NIS (Network and Information Security), котра була орієнтована на забезпечення високого рівня безпеки у відношенні до провайдерів цифрових послуг і операторів критичних інфраструктур. Розширюється і спектр проблематик, які охоплює вказаний документ, шляхом врегулювання забезпечення безпеки не лише персональних даних, але й будь-яких даних в цілому.

Відповідно, європейська спільнота багато чого зробила і продовжує роботи в частині забезпечення захисту персональних даних, кібербезпеки, дотримання права на приватність, захищеності електронної комунікації [10; 9, с. 72–73].

Що стосується вітчизняної практики, як свідчить бібліографічний аналіз, до середини 90-х років ХХ ст. правових та організаційних засад захисту персональних даних у вітчизняній науці ґрунтовно не досліджували. З одного боку, це пояснюється концентрацією наукового потенціалу на розв'язання глобальних проблем розбудови національної правової системи. З іншого – проблематика захисту персональних даних тоді ще не мала великої соціальної актуальності: тогочасний рівень інформатизації суспільства був вельми низьким, обробка персональних даних здійснювалась переважно у механічний спосіб, а відповідні інформаційні бази були нечисленними й легко контролюваними. Відповідно на певному історичному відтинку техніко-технологічні аспекти накопичення, обробки та передачі даних мали значно більший науковий резонанс, аніж питання їх правового захисту [2, с. 9–10].

Чинне українське законодавство в сфері захисту персональних даних, у першу чергу репрезентоване:

- Конституцією України [5];

- Законом України «Про захист персональних даних» [6]. Прийняття даного документу, безперечно, прогресивний, хоча і відносно запізнений крок в системі розвитку законодавства про захист персональних даних. Відповідно до міжнародних підходів цей акт вперше визначив підхід до розуміння ключового концепту, тим самим обґрунтовано розширивши межі захисту особистої інформації;

- документами у сфері захисту персональних даних, прийняті Уповноваженим Верховної Ради України з прав людини.

Саме конституційні норми становлять базу національного законодавства, характеризують цінності сучасного суспільства ізумовлюють напрями їх реалізації. Взятий (цілком успішно) Україною курс на цифровізацію різних сфер суспільних відносин, що знаходить вираження і в ухвалених останніми роками нормативних правових актах, формує передумови для закріплення нових прав людини в інформаційній сфері, пріоритетне місцесеред яких належить праву на захист персональних даних.

Громадяни відповідно до свого суб'єктивного права самостійно розпоряджаються персональними даними, розміщуючи, наприклад, їх у соціальних мережах, реєму та Інтернет-магазинах, однак, вбачається, що вепоху глобальних ризиків, пов'язаних з появою все нових і нових технологій (наприклад, обробка «великих даних»), держава покликана забезпечувати мінімальні гарантії захисту персональної інформації для того, щоб не допустити порушення інших конституційних прав, особливо дискримінації.

Вагоме значення мають також низка інших законів, як наприклад, Закон України «Про доступ до публічної інформації» [8] та Закон України «Про інформацію» [7]. При цьому, в основному Законі, який регламентує правовідносини в частині захисту персональних даних знайшли своєї відображення більшість положень Директиви [12].

Аналіз юридичної літератури та зарубіжного законодавства показує, що зміст права на захист персональних даних становить можливість вимагати вчинення будь-яких дій з ними лише за згодою суб'єктів персональних даних або на іншій законній підставі у встановлених цілях і справедливо, що гарантується державою, у тому числі за допомогою здійснення контролю з боку компетентного уповноваженого органу. Новітні Основні закони окремих держав уже закріплюють право на захист персональних даних як самостійне, зокрема така практика характерна для Вірменії, Угорщини, Сербії, Швейцарії.

В умовах активних бойових дій, Україні, не зважаючи на свій потужний ресурсний і трудовий потенціал, досить складно розвиватися та удосконалювати законодавство, в тому числі в напрямку захисту персональних даних. Але наукова спільнота, законодавець та кращі представники ІТ-сегменту, безперечно, не стоять на місці і роблять важливі напрацювання в даному напрямку, щоб Україна і надалі підтримувала статус однієї із розвинутих цифрових країн світу, при цьому, завоювавши право позиціонуватися державою, в якій де-юре і де-факто дотримуються і поважають права на захист персональних даних.

**Висновки та перспективи подальших наукових пошуків.** Глобальною тенденцією останніх десятиліть стало збільшення обсягів і швидкості обробки персональної інформації та дедалі більше її поширення в мережі Інтернет, зокрема в соціальних мережах і месенджерах. Необхідність удосконалення технічного захисту персональних даних прямо кореспондує постійному розвитку інформаційно-комунікаційних технологій та їх безпечному використанню. У зв'язку з цим особливої актуальності набувають питання правового реагування та процесу, що відбуваються, з метою забезпечення безперешкодної реалізації конституційних прав і свобод людини та громадянина в різних сферах діяльності (надання електронних послуг, торгівля, охорона здоров'я, освіта, здійснення адміністративних процедур та ін.). Перспективи подальших наукових пошуків вбачаємо у розкритті сучасних і найбільш прогресивних механізмів самозахисту персональних даних.

## ЛІТЕРАТУРА

1. Бем М. В., Городиський І. М., Саттон Г., Родіоненко О. М. Захист персональних даних: Правове регулювання та практичні аспекти: науково-практичний посібник. К.: К.І.С., 2015. 220 с.
2. Гуржій Т. О. Правовий захист персональних даних: монографія. Т. О. Гуржій, А. Л. Петрицький. Київ: Київ. нац. торг.-екон. ун-т, 2019. 216 с.
3. Золотар О. О. Інформаційна безпека людини: теорія і практика : монографія. Київ: ТОВ «Видавничий дім «АртЕк», 2018. 446 с.
4. Конвенція Ради Європи про захист осіб у зв'язку з автоматизованою обробкою персональних даних від 28.01.1981. *Офіційний вісник України*. 2011. № 1. С. 1994.
5. Конституція України. *Відомості Верховної Ради України* (ВВР). 1996. № 30. с. 141. URL: <https://zakon.rada.gov.ua/laws/show/254к/96-вр#Text>
6. Про захист персональних даних: Закон України від 01.06.2010 № 2297-VI. URL: <https://zakon.rada.gov.ua/laws/show/2297-17#Text>
7. Про інформацію: Закон України від 02.10.1992 № 2657-XII. URL: <https://zakon.rada.gov.ua/laws/show/2657-12#Text>
8. Про доступ до публічної інформації: Закон України від 13.01.2011 № 2939-VI. URL: <https://zakon.rada.gov.ua/laws/show/2939-17#Text>
9. Сопілко І. М. Міжнародно-правовий досвід захисту персональних даних: напрямки вдосконалення для України. *Юридичний вісник*. Вип.4 (33). 2014. с. 70-75
10. Стандарти захисту персональних даних в соціальній сфері. М. В. Бем,, І. М. Городиський. Львів: б.в., 2018. 110 с.
11. Directive 2009/136/EC of the European Parliament and of the Council, of 25.11.2009. EUR-lex. URL:<https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32009L0136>
12. Directive 95/46/EC Of The European Parliament And Of The Council of 24 October 1995 «On the protection of individuals with regard to the processing of personal data and on the free movement of such data». Official Journal. L 281, 1995. p. 31–50
13. Directive (EU) 2016/680 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 by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA. EUR-lex. URL:<https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016L0680&from=EN>
14. Warren S. D., Brandeis L. D. The Right to Privacy. *Harvard Law Review*, 1890. . 4 (5), p. 193–220. <https://doi.org/10.2307/1321160>