DOI: 10.34015/2523-4552.2025.4.16
УДК 342.95

Трунілін М. О.,
аспірант кафедри галузевого права та загальноправових дисциплін Інституту права та суспільних відносин ЗВО «Відкритий міжнародний університет розвитку людини «Україна»
ORCID: 0009-0007-5956-9874

СТАНОВЛЕННЯ І ПОДАЛЬШИЙ РОЗВИТОК СИСТЕМИ ЗАКОНОДАВСТВА У СФЕРІ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ (МІЖНАРОДНІ АСПЕКТИ)

У статті досліджується питання стрімкого розвитку технологій та архітектура побудови системи захисту персональних даних (міжнародні аспекти) у законодавстві Європейського Союзу (далі – ЄС). Розглянуто історію розвитку інформаційних ресурсів та змін у правовому регулюванні відносин між країнами учасницями міжнародних конвенцій, трансформацію інформації про людину в окрему галузь персональних даних, яка у сучасних умовах набуває ще найбільшу цінність, потребує надійного захисту та окремої уваги при удосконаленні архітектури її правового регулювання.

У статті проаналізовано, що технологічні дослідження та відкриття, а також історичні зміни норм міжнародного права у сфері захисту персональних даних, дали підґрунтя для розвитку та удосконалення національних законодавств у цій сфері у окремих країнах ЄС, а напрацювання кейсів судової практики Європейського суду по правам людини та Суду справедливості Європейського союзу, довели висновок авторів, що у Європейській економічній зоні (скорочено - ЄЕЗ) динамічно зростає тенденція до накладення штрафів за порушення вимог Загального регламенту про захист даних (англ. General Data Protection Regulation (скорочено – GDPR).

У міжнародних конвенціях, що діють на даний час, зокрема у GDPR, визначаються основоположні принципи, яких дотримуються країни-учасники при прийнятті своїх локальних законодавчих актів, тому що розвиток та зміни у технологіях автоматизованої обробки персональних даних відбувається занадто швидко.

Запровадження у деяких країнах ЄС прозорих механізмів регулювання та контролю у системі захисту персональних даних: від фундаменту – наглядового органу, до даху - контролера даних, у взаємозв'язку з якісною цеглою – професійними фаховими спеціалістами із захисту даних, «створили якісний архітектурний об'єкт», де розмежовуються та захищаються права суб'єктів персональних даних, права та обов'язки органів адміністрування, контролерів, володільців та розпорядників персональних даних. Вивчення досвіду таких країн, їх законодавства у цій сфері та практичних рекомендацій його за-

стосування, може значно скоротити час у процесі гармонізації законодавства України з GDPR.

У статі використані історичний, діалектичний, системно-структурний, формально-логічний, соціологічний, порівняльно-правовий методи пізнання.

Автори роблять висновок, що в сучасних умовах зростання кількості воєнних конфліктів у світі, стало очевидним, що сфера захисту персональних даних стала надзвичайно важливою складовою питання національної безпеки будь-якої країни світу.

За результатами проведеного дослідження запропоновано удосконалення архітектури національного законодавства країни у сфері персональних даних та їх захисту згідно міжнародних конвенцій ЄС, європейського курсу розвитку України.

Ключові слова: *. Технологічні процеси, історія архітектури, міжнародні конвенції ЄС, персональні данні, захист персональних даних, ідентифікація осіб, передання даних, міжнародний ринок праці, ринок IT.*

Постановка проблеми. У сучасному світі майже кожна людина користується електронними пристроями, стикаючись з постійним оновленням їх технічних, технологічних та програмних продуктів, файлів. Зазвичай це супроводжується повідомленнями про оновлення політики конфіденційності, та/або згодою на використання «Cookie» (наприклад, на платформі https://meta.ua/uk/about/privacy-policy/) де було зазначено: «Ми та наші партнери (868 IAB партнери, 309 Google партнери) зберігаємо та/або отримуємо доступ до інформації на пристрої, який ви використовуєте, наприклад унікальних ідентифікаторів у файлах cookie для обробки ваших персональних даних.».

Усьому причина, необхідність приведення та дотримання законодавства про захист персональних даних, зокрема РЕГЛАМЕНТ Європейського Парламенту і Ради (ЄС) 2016/679 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) (англ. General Data Protection Regulation) від 27 квітня 2016 року (далі – GDPR або Регламент) [1].

Регламент це результат трансформації та удосконалення законодавства ЄС у сфері захисту фізичних осіб у зв'язку з опрацюванням персональних даних та вільним рухом таких даних. Регламент було ухвалене на заміну Директиви 95/46/ЄС Європейського Парламенту і Ради «Про захист фізичних осіб при обробці персональних даних і про вільне переміщення таких даних» від 24.10.1995 р. (далі - Директива) [2].

Сучасні провідні юристи практики GDPR та захисту персональних даних О. Колченогова та О. Слободянюк охарактеризували відмінності GDPR та Директиви так: «На відміну від GDPR, Директивою було встановлено право кожного з 28 членів ЄС ухвалити й адаптувати законодавство відповідно до потреб своїх громадян. Натомість Регламент вимагає його повного ухвалення усіма 28 країнами без будь-якої свободи дій. Тоб-

то GDPR вимагає від усіх 28 країн ЄС відповідати положенням Регламенту. Директиву було скасовано через те, що її положення не охоплювали того, як дані потрібно зберігати, збирати й передавати в сьогоднішніх реаліях цифрової епохи. Як і багато інших нормативно-правових актів, ці нормативні акти не встигають за темпами технологічного прогресу.» [3].

На відміну від технологій кінця XX століття, на сьогодні, фактично персоналізація (електронна ідентифікація) вже відбувається завдяки застосуванню сукупності новітніх технологій розпізнання індивідуальних ознак персональних речей, належних персонально особі електронних пристроїв та персональних даних, при цьому деякі з яких ще не визначено законодавством, як окремі об'єкти персональних даних громадян (посмішка губ, роговиця ока, голос та ін..).

Дослідження історичних аспектів побудови та формування міжнародної системи охорони персональних даних у XX-XXI столітті є предметом досліджень багатьох науковців та є важливими для аналізу сучасного стану архітектури законодавства щодо передачі, обробки і захисту персоніфікованих даних фізичних осіб.

В сучасних умовах зростання кількості воєнних конфліктів у світі, стало очевидним, що сфера захисту персональних даних є надзвичайно важливою складовою питання національної безпеки будь-якої країни світу у цьому столітті, а отже існує необхідність постійного удосконалення та гармонізації національного законодавства кожної окремої країни ЄС з міжнародними конвенціями, зокрема з GDPR.

Українське законодавство, яке ґрунтується на нині скасованій Директиві, значно відстає від сучасних тенденцій у регулюванні захисту даних.

Тому, зміна архітектури та гармонізація національного законодавства країни з міжнародними нормами GDPR є нагальною потребою в Україні, є актуальним завдання для багатьох країн ЄС та світу, можливістю в майбутньому уникнути накладання штрафів за порушення GDPR, становить не лише науковий інтерес, а й практичний сенс.

Аналіз останніх досліджень і публікацій. Вказаним питанням у тій чи іншій мірі приділяли увагу О. Тимошенко, М. Бем, І. Городиський, Г. Саттон, О. Родіоненко, І. Сопілко, К. Врублевська-Місюна, В. Тичина, В. Брижко, М. Різак, Р. Стефанчук, А. Авраменко та багато ін. Разом із цим, зважаючи на велику кількість нормативно-правових актів та їх розбіжностей у визначенні понятійно-категоріального апарату, механізмів застосування стандартів захисту інформації про особу, велике коло питань у цій сфері відносин на сьогодні є не вирішеними, у зв'язку із чим актуальним є їх розгляд, дослідження та систематизація.

Постановка завдання. Метою статті є з'ясування сутності таких понять, як «інформація про особу», «персональні дані», «ідентифікація», «персоналізація», аналіз дії у часі та прийняття нових міжнародних норм у сфері захисту, обробки та передання персональних даних про фізичну особу та забезпечення захисту прав людини, аналіз змін у часі вимог міжнародного законодавства та повноважень національних наглядових органів, судових справ щодо практи-

чних кейсів, виявлення динаміки, сутності та специфіки сучасного правового регулювання у галузі захисту персональних даних, зокрема GDPR.

Виклад основного матеріалу. Формування системи охорони персональних даних бере свій початок із середини XX ст. Так, Загальна декларація про права людини 1948 р. у ст. 12 закріпила захист персональної інформації як невід'ємного права людини на захист особистого життя, у свою чергу, Європейська конвенція про захист прав людини і основоположних свобод 1953 р. у ст. 8 зазначила, що кожен має право на повагу до свого приватного і сімейного життя, до свого житла і кореспонденції. Наразі, беручи до уваги стрімкі процеси глобалізації, розвиток високих технологій, та як наслідок появи нової форми міжнародного тероризму – кібертероризму, суспільство потребує формування нових підходів та визначення нових стандартів сучасної системи персональних даних. [4]

Серед нормативно-правових актів європейської системи законодавств, що регулюють питання пов'язані із захистом персональних даних необхідно виокремити наступні: Конвенція Ради Європи «Про захист осіб у зв'язку з автоматизованою обробкою персональних даних» від 28.01.1981 р. (далі – Конвенція № 108); Додатковий протокол до Конвенції про захист осіб у зв'язку з автоматизованою обробкою персональних даних щодо органів нагляду та транскордонних потоків даних від 08.11.2001 р.; Директива 97/66/ЄС «Про обробку персональних даних і захист прав осіб у телекомунікаційному просторі» від 15.12.1997 р. та ін. [4]

Конвенція № 108 Ради Європи передбачає дуже важливий момент, згідно з яким збирання, накопичення, зберігання і поширення персональних даних може здійснюватися лише з дозволу особи, дані про яку обробляються. Крім того, на думку Сопілко І. М., позитивним моментом даного акту є його спрямованість на об'єднання країн світу для визначення основних вимог до передачі індивідуальної інформації про людину у всесвітньому електронному просторі, тобто створення ряду процедур і правил, які стають обов'язковими при обробці персональних даних та відповідно забезпечує захист від їх порушень [5; с. 72].

Врублевська-Місюна К. М., Тичина В. П. у статті «Міжнародно-правові стандарти захисту інформації про особу», зазначили що Регламент Європейського Парламенту і Ради (ЄС) 2016/679 від 27.04.2016 р. про захист фізичних осіб у зв'язку з опрацюванням персональних даних і про вільний рух таких даних (GDPR), що прийшов на заміну рамкової Директиви про захист персональних даних 95/46/ЄС від 1995 р. (Директива) став одним з найбільш жорстких та довгоочікуваних нормативно-правових актів у сфері захисту приватності особи за останні 20 років. Прийняття вказаного документу викликало неабиякий інтерес та обговорення у суспільстві, адже він встановлює більш сувору відповідальність за порушення у сфері дотримання законності обробки персональних даних та орієнтує на необхідність запровадження якомога більшого обсягу персональних даних, що підлягають захисту.

GDPR визначає «персональні дані як будь-яку інформацію, що 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 місце перебування, онлайн-ідентифікатор або за одним чи декількома факторами, що є визначальними для фізичної, фізіологічної, генетичної, розумової, економічної, культурної чи соціальної сутності такої фізичної особи. [4]

Окрім того, GDPR встановлює нові європейські стандарти, серед яких можна виокремити наступні:

1) щодо територіальної сфери застосування. На відміну від положень Директиви, положення якої стосувались тільки суб'єктів, що перебувають в інших країнах, Правила GDPR відповідно до ст. 3 застосовують також до суб'єктів, що знаходяться в інших країнах світу. Разом з тим, кожен хто перебуває на території Європейського Союзу автоматично отримує право на захист своїх даних по GDPR;

2) щодо отримання згоди. п. 2 ст. 7 визначає, що якщо суб'єкт даних надає згоду в контексті письмової декларації, що також стосується інших питань, запит на надання згоди необхідно подавати у формі, що чітко відрізняється від інших питань, у зрозумілій та доступній формі, з використанням чітких і простих формулювань. Будь-яка частина такої декларації, що становить порушення цього Регламенту, не є зобов'язальною. Тобто, відтепер запит на отримання згоди на передавання персональних даних має бути чіткий за змістом та доступним для розуміння кожного;

3) щодо прав суб'єктів даних. У цьому аспекті GDPR значно розширив права тих осіб, чиї дані обробляються, що детально визначено у ст. 13-22. Відповідно до вказаних положень за суб'єктом закріплено право отримувати інформацію щодо особи та контактних даних контролера; цілі опрацювання, для досягнення яких призначено персональні дані; інформацію щодо періоду зберігання персональних даних; право на запит від контролера щодо доступу до персональних даних та її виправлення, стирання, обмеження опрацювання щодо суб'єкта даних тощо. Таким чином, можна зробити висновок, що основою концепції згоди на обробку даних є те, що вона має бути вільною та існування реальної можливості її вільного відкликання;

4) п. 85 Преамбули Регламенту встановлює, що як тільки контролеру стає відомо про порушення захисту персональних даних, він повинен повідомити наглядовий орган про порушення захисту персональних даних без неналежної затримки та, за можливості, не пізніше ніж за 72 годин після того, як йому стало про це відомо, за винятком якщо контролер може довести, згідно з принципом підзвітності, що порушення захисту персональних даних малоймовірно створить ризик для прав і свобод фізичних осіб;

5) щодо відповідальності. Відповідно до статті 83 Регламенту за порушення положень Регламенту сума штрафу може становити до 4% річного обороту або до 20000000 євро. Окрім зазначених вище пунктів, новели стосуються питань пов'язаних з питаннями політики конфіденційності, оцінкою ризиків, встановлення відповідальних осіб. [4].

Сучасні провідні юристи практики GDPR та захисту персональних

даних О. Колченогова та О. Слободянюк, аналізуючи практику Європейського суду з прав людини в питаннях захисту персональних даних дослідили декілька цікавих прикладів застосування санкцій наглядовим органом Польщі до порушників GDPR є ситуація з компанією "Bisnode", яка надає рішення з цифрового бізнесу, маркетингу та кредитної інформації, з головним офісом у Стокгольмі. Навесні 2019 року польський орган із захисту даних призначив свій перший штраф для цієї фірми в розмірі 220 тисяч євро за невиконання її зобов'язань щодо прав суб'єкта даних, передбачених ст. 14 GDPR. Справа в тому, що Bisnode збирала дані про осіб із відкритих джерел, не повідомляючи їх про мету та строк обробки. Наглядовий орган зобов'язав компанію зв'язатися з шістьма мільйонами людей, чию інформацію компанія зберігає чи іншим чином обробляє, щоб виконати вимоги щодо інформаційного повідомлення згідно з Регламентом.

Своєю чергою Bisnode аргументувала відмову тим, що вона не володіє електронними адресами більшості суб'єктів даних, а направляти поштою – це значні витрати для компанії. Зрештою за відмову виконати припис наглядового органу та, як наслідок, порушення Регламенту компанія дістала фінансове покарання [3].

Згадаємо, що 1 січня 2011 року набрав чинність Закон України «Про захист персональних даних» № 2297-VI від 1 червня 2010 року [6], який регулює правові відносини, пов'язані із захистом і обробкою персональних даних, і спрямований на захист основоположних прав і свобод людини і громадянина, зокрема права на невтручання в особисте життя, у зв'язку з обробкою персональних даних. Цей Закон ґрунтується на нині скасованій Директиві, тому не відповідає сучасному законодавству ЄС, зокрема GDPR.

Задля виконання умов Договору про Асоціацію України з ЄС щодо належного рівня захисту персональних даних, у Верховній Раді зареєстровані проєкти Закону України "Про захист персональних даних" за номерами № 5628 від 02.06.2021 [7] та № 8153 від 25.10.2022 [8], а також проект Закону України «Про Національну комісію з питань захисту персональних даних та доступу до публічної інформації» № 6177 від 18.10.2021 [9], що розроблені відповідно до норм та вимог GDPR, для приведення у відповідність до стандартів ЄС, які до цього часу розглядаються у парламенті.

Протилежний позитивний приклад роботи наглядового органу Франції досліджував та аналізував Мирослав Хмарський, партнер юридичною фірми Avitar, зазначивши, що 16 листопада 2021 року французький наглядовий орган із захисту даних Франції (CNIL) опублікував практичне керівництво для спеціаліст із захисту даних (DPO). Керівництво надає додаткову інформацію та практичні рекомендації організаціям, що призначають DPO, стосовно вимог GDPR і Закону про захист даних Франції. [10]. Цей досвід цікавий тим, що справді незалежний спеціаліст із захисту даних (DPO), виконуючи свої обов’язки повинен звітувати керівництву організації, де DPO працює та відповідає за організацію роботи із захисту персональних даних, але DPO не несе відповідальності в разі недотримання Закону про захист даних, а відповідальність продовжує нести організація. DPO є

ключовою контактною особою для регулювального органу (CNIL) та суб'єктів даних. DPO може допомогти представникові організації відповісти на запитання, спираючись на свій досвід. Крім того, CNIL не відповідає на запити організацій, які не проконсультувалися зі своїм DPO щодо цього конкретного питання.

Висновки. На даний час всі країни ЄС, зобов'язані мати окремий незалежний наглядовий орган, який наділений функціями формування та реалізації внутрішньої державної політики країни в сфері захисту персональних даних, має повноваження контролю за дотриманням національного Закону про захист персональних даних та GDPR.

Кожний наглядовий орган повинен володіти компетенцією на території своєї держави-члена для реалізації повноважень та виконання завдань, покладених на нього згідно з Регламентом [Преамбула (122); 1].

Про необхідність утворення та функціонування нового органу – Національної комісії з питань захисту персональних даних та доступу до публічної інформації, як центрального органу виконавчої влади зі спеціальним статусом, було також визначено у законопроекті № 6177 [9].

Тому автори приходять до висновку, що архітектура законодавства України у сфері захисту персональних даних, доступу до них, їх передачі та обробки - не є структурованою в розумінні GDPR.

Національне правове регулювання країн-членів ЄС та України, повинно відповідати GDPR, враховувати досвід та судову практику, забезпечити дотримання предмету та цілей Регламенту, що установлює норми щодо захисту фізичних осіб у зв'язку з опрацюванням персональних даних і норми про вільний рух персональних даних, а також захищає фундаментальні права і свободи фізичних осіб, зокрема їхнє право на захист персональних даних.

Список використаних джерел

1. Про захист фізичних осіб у зв'язку з опрацюванням персональних даних і про вільний рух таких даних : Регламент 2016/679 Європейського Парламенту і Ради від 27.04.2016 р. (GDPR). *Офіційний вісник Європейського Союзу*, UA L 119/1, 04.05.2016. URL: https://zakon.rada.gov.ua/laws/show/984_008-16#Text (дата звернення 01.08.2025).

2. Про захист фізичних осіб при обробці персональних даних і про вільне переміщення таких даних : Директива 95/46/ЄС Європейського Парламенту і Ради від 24.10.1995 р. *Official Journal*, L 281, 23/11/1995. URL: https://zakon.rada.gov.ua/laws/show/994_242#Text (дата звернення 01.08.2025).

3. Колченогова О., Слободянюк О. Практика вирішення спорів щодо захисту даних у контексті GDPR (порівняльний аналіз). *Електронне видання Ліга:Закон, "Юрист & Закон".* 2021. № 49. URL: https://zakon-pro.ligazakon.net/ document/EA015304?land=UA&context=UA (дата звернення 01.08.2025).

4. Врублевська-Місюна К. М., Тичина В. П. Міжнародно-правові стандарти захисту інформації. *Науковий вісник Ужгородського Національного Університету. Серія: Право.* 2022. № 74. Ч. 2. С. 149-154. DOI https://doi.org/10.24144/2307-3322.2022.74.58

5. Сопілко І. М. Міжнародно-правовий досвід захисту персональних даних: напрямки вдосконалення для України. *Юридичний вісник*. 2014. №4 (33). С. 70–75.

6. Про захист персональних даних : Закон України VI від 1.06.2010 року № 2297-VI (з останніми змінами та доповненнями, станом на 15.02.2025). *Відомості Верховної Ради України* (ВВР), 2010, № 34, ст. 481.

7. Про захист персональних даних : Проект Закону України від 07.06.2021 № 5628. URL: https://zakon-pro.ligazakon.net/document/JI05379I?ed=2021_06_02&land=UA&context=UA&an=3 (дата звернення 01.08.2025).

8. Про захист персональних даних : Проект Закону України від 25.10.2022 р. № 8153. URL: https://zakon-pro.ligazakon.net/document/JI08275I?utm_source=jurliga.ligazakon.net&utm_medium=news&utm_content=jl03&_ga=2.30614719.1427238797.1754334496-769865409.1708683360&land=UA&context=UA&an=1 (дата звернення 01.08.2025).

9. Про Національну комісію з питань захисту персональних даних та доступу до публічної інформації : Проект Закону України від 18.10.2021 № 6177. URL: https://zakon-pro.ligazakon.net/document/JI06201I?ed=2021_10_11&land=UA&context=UA&an=3 (дата звернення 01.08.2025).

10. Хмарский М. DPO: як упровадити цю функцію в Україні на основі європейського досвіду. Електронне видання Ліга:Закон, "Юрист & Закон". 2021. № 50. URL: https://zakon-pro.ligazakon.net/document/EA015326?land=UA&context=UA (дата звернення 01.08.2025).

Trunilin Mykhailo, *Postgraduate student of the Department of industry law and general legal disciplines, Institute of Law and Public Relations Open International University of Human Development "Ukraine"*

ORCID: 0009-0007-5956-9874

Establishment and Further Development of the System of Legislation in the Field of Personal Data Protection (International Aspects)

This article examines the rapid development of technology and the architecture of personal data protection systems (international aspects) in European Union (EU) legislation. It considers the history of the development of information resources and changes in the legal regulation of relations between countries participating in international conventions, the transformation of information about individuals into a separate field of personal data, which in modern conditions is becoming increasingly valuable, requires reliable protection, and deserves special attention in improving the architecture of its legal regulation.

The article analyzes how technological research and discoveries, as well as historical changes in international law norms in the field of personal data protection, have provided the basis for the development and improvement of national legislation in this area in individual EU countries. and the development of case law by the European Court of Human Rights and the Court of Justice of the European Union has led the authors to conclude that in the European Economic Area (abbreviated as EEA), there is a dynamically growing trend towards imposing fines for violations of the requirements of the General Data Protection Regulation (abbreviated as GDPR).

International conventions currently in force, in particular the GDPR, define the fundamental principles that participating countries adhere to when adopting their local legislation, because developments and changes in automated personal data processing technologies are happening too quickly.

The introduction of transparent regulatory and control mechanisms in the personal data protection system in some EU countries: from the foundation – the supervisory authority – to the roof – the data controller, in conjunction with high-quality bricks – professional data protection specialists – have created a high-quality architectural object where the rights of personal data subjects, the rights and obligations of administrative bodies, controllers, owners, and managers of personal data are delineated and protected. Studying the experience of such countries, their legislation in this area, and practical recommendations for its application can significantly reduce the time required to harmonize Ukrainian legislation with the GDPR.

The article uses historical, dialectical, systemic-structural, formal-logical, sociological, and comparative-legal methods of cognition.

The authors conclude that, given the current increase in the number of military conflicts around the world, it has become clear that personal data protection has become an extremely important component of national security for any country.

Based on the results of the study, it was proposed to improve the architecture of the country's national legislation in the field of personal data and their protection in accordance with EU international conventions and Ukraine's European development course.

***Keywords**: Technological processes, history of architecture, EU international conventions, personal data, personal data protection, identification of individuals, data transfer, international labor market, IT market.*

