УДК 341.1/.8:004.8
DOI https://doi.org/10.32782/1813-338X-2025.3.29

В. І. Пішта
доктор філософії,
доцент кафедри адміністративного, фінансового
та інформаційного права
ДВНЗ «Ужгородський національний університет»,
ORCID ID: 0000-0003-2769-7189

С. С. Драбюк
здобувачка ступеня доктора філософії
ДВНЗ «Ужгородський національний університет»
ORCID ID: 0009-0005-9564-2376

М. Г. Рожкова
кандидат юридичних наук, доцент,
доцент кафедри іноземних мов
Навчально-наукового інституту міжнародних відносин
Київського національного університету імені Тараса Шевченка,
ORCID ID: 0000-0002-0891-8225

МІЖНАРОДНЕ ІНСТИТУЦІЙНЕ СПІВРОБІТНИЦТВО У СФЕРІ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ В УМОВАХ РОЗВИТКУ ШТУЧНОГО ІНТЕЛЕКТУ ТА ІНТЕРНЕТУ РЕЧЕЙ

У статті представлено комплексний аналіз інституційних моделей міжнародного співробітництва у сфері захисту персональних даних в умовах активного розвитку технологій штучного інтелекту та Інтернету речей. Розкрито особливості взаємодії міжнародних організацій, наднаціональних органів, державних інституцій та приватного сектору у контексті формування нормативних, технічних та етичних механізмів регулювання. Окрему увагу приділено універсальним і регіональним актам, зокрема Конвенції 108+, Загальному регламенту про захист даних, Принципам приватності Організації економічного співробітництва та розвитку, а також сучасним стандартам ISO/IEC, що визначають технічні вимоги до управління ризиками та конфіденційністю.

Визначено ключові виклики транскордонного обміну інформацією, проблеми гармонізації підходів і роль технічних стандартів як інструмента забезпечення довіри, прозорості й сумісності систем обробки персональних даних у міжнародному цифровому просторі.

Окрему увагу приділено тому як між собою співвідносять норми жорсткого та м'якого права. Визначено, що нормативно-правові акти можуть забезпечувати високий рівень юридичних гарантій для суб'єктів правовідносин у сфері транскордонного обміну даних, але при цьому вони також можуть створювати певні бар'єри для такого обміну. У той же час норми м'якого права, як-от рекомендації, інструкції та керівні принципи міжнародних організацій, дозволяють скоріше реагувати на виклики, які виникають у зв'язку зі стрімким розвитком цифрових технологій. Автори звертають увагу на роль Європейської ради із захисту даних та Організації економічного співробітництва та розвитку та окремих ініціатив.

У статті також приділяється увага питанню важливості технічного аспекту регулювання, що проявляється крізь призму аналізу таких міжнародних стандартів як ISO/IEC 27701, 23894 та 38507.

Зрештою звертається увага на ті моменти, які стосуються успішної інтеграції України у глобальний цифровий простір. Робиться висновок про необхідність гармонізації українського законодавства з нормами Загального регламенту про захист даних та іншими міжнародними стандартами.

Ключові слова: *міжнародне співробітництво, персональні дані, штучний інтелект, Інтернет речей, GDPR.*

© В. І. Пішта, С. С. Драбюк, М. Г. Рожкова, 2025

Постановка проблеми. У контексті глобалізації сучасних цифрових комунікацій обмін інформацією має транснаціональний характер, що призводить до втрати територіальної прив'язаності у контексті обміну інформацією. У такому разі належний захист персональних даних є першочерговим викликом перед міжнародною спільнотою. Зрештою прогрес у сферах штучного інтелекту та Інтернету речей ускладнює існуючі моделі регулювання, що спонукає до необхідності вдосконалення правових та технічних інструментів регулювання.

У зв'язку з цим необхідно звернути увагу на міжнародне інституційне співробітництво у сфері захисту персональних даних.

Аналіз останніх досліджень і публікацій. Окремі елементи міжнародного співробітництва розглядалися рядом авторів, включаючи С. О. Білу, Д. Г. Гавриченка, Х. І. Гордійчук-Бурдіну, Т. В. Іванову, І. О. Лесь та іншими. Разом з тим питання ролі технічних регламентів міжнародних організацій було об'єктом досліджень М. Бєлікової, К. Маас та А. Маяр. Водночас комплексних або фрагментарних досліджень щодо міжнародного інституційного співробітництва у сфері захисту персональних даних в умовах розвитку штучного інтелекту та Інтернету речей до цього моменту не здійснювалося.

Мета статті – здійснити аналіз інституційних моделей міжнародного співробітництва у сфері захисту персональних даних в умовах розвитку штучного інтелекту та Інтернету речей.

Виклад основного матеріалу. Сьогодні міжнародне інституційне співробітництво може розумітися як сукупність відносин і взаємодій між державами, міжнародними організаціями, бізнес-структурами та громадянським суспільством, здійснена через узгоджені економічні, правові та інституційні механізми для досягнення спільних цілей, реалізації проєктів або вирішення глобальних проблем [1, с. 30].

У контексті захисту персональних даних міжнародне інституційне співробітництво може розглядатися як системна взаємодія між міжнародними організаціями, органами державної влади, а також підприємствами, установами, та організаціями, яка спрямована на формування й імплементацію узгоджених правових норм, технічних стандартів та етичних принципів з метою забезпечення належного рівня захисту персональних даних у процесі їх обробки та транскордонної передачі.

Одним із перших міжнародних актів у сфері захисту персональних даних були Керівні принципи щодо міжнародної політики щодо захисту конфіденційності та транскордонних потоків персональних даних, розроблені Організацією економічного співробітництва та розвитку у 1980 році, оформлені як Рекомендація Організації економічного співробітництва та розвитку (далі – ОЕСР). В їх основу лягли три основні принципи, які об'єднують країни-члени ОЕСР, а саме: плюралістична демократія, повага до прав людини та відкрита ринкова економіка [2].

Міжнародне регулювання у сфері захисту персональних даних ґрунтується на поєднанні універсальних, регіональних і національних актів, що створюють основу для гармонізації підходів до захисту інформації в умовах глобальної цифровізації. Основною метою таких актів є забезпечення захисту права людини на приватність у контексті обробки даних, незалежно від їх територіальної чи юрисдикційної прив'язки.

Ключовим документом європейського права, який суттєво впливає на міжнародну практику захисту даних, є Загальний регламент про захист даних (далі – GDPR). Він визначає принципи законності, прозорості, мінімізації та обмеження мети обробки даних, а також запроваджує інститут підзвітності. Важливим є положення статті 50 GDPR, яка закріплює зобов'язання Європейської Комісії та наглядових органів сприяти розвитку міжнародних механізмів співробітництва для ефективного забезпечення дотримання законодавства про захист персональних даних [3].

Другим європейським документом є Конвенція Ради Європи № 108 (та її модернізований варіант – Конвенція 108+), яка визначає мінімальні стандарти обробки персональних даних державами-учасницями. На відміну від GDPR, ця Конвенція має відкритий характер і може бути ратифікована не лише європейськими державами, що робить її універсальним інструментом глобальної гармонізації стандартів захисту приватності [4; 5].

На глобальному рівні основу концептуального розвитку міжнародних норм становлять вже згадані нами Керівні принципи приватності ОЕСР, ухвалені ще 1980 року і оновлені в 2013 році. Вони стали першими правилами, які були угоджені міжнародною спільнотою та визначали такі принципи обробки даних як обмеження збору, якість даних, цілі використання, безпеку, відкритість і підзвітність [2].

Таким чином, міжнародне правове регулювання вибудовується за багаторівневою

моделлю, де універсальні стандарти поєднуються з регіональними. З іншого боку доповнюють їх національні акти, забезпечує можливість ефективного обміну даними в умовах використання штучного інтелекту (далі – ШІ) та Інтернету речей (далі – IoT).

Правове регулювання у сфері приватності ефективне лише тоді, коли воно підкріплене відповідними технічними стандартами, які забезпечують практичне виконання правових вимог. У зв'язку з розвитком ШІ та IoT саме стандарти стандарти набувають ключового значення, дозволяючи узгодити правові та технологічні механізми. Найважливішим міжнародним стандартом, що деталізує вимоги до управління конфіденційністю, є ISO/IEC 27701:2025 «Information security, cybersecurity and privacy protection – Privacy information management systems – Requirements and guidance». Цей стандарт розширює систему управління інформаційною безпекою і вводить поняття Privacy Information Management System [6].

Метою цього стандарту є сприяння організаціям, які є контролерами або процесорами персональних даних, у забезпеченні відповідності вимогам GDPR та інших актів. Стандарт визначає процедури для визначення ризиків, контролю доступу, ведення журналів обробки, а також взаємодії між учасниками транскордонного обміну даними. Завдяки своїй універсальності він розглядається одним із найефективніших інструментів практичного забезпечення міжнародної сумісності систем захисту даних.

Іншими важливими документами є:

− ISO/IEC 23894:2023 «Artificial Intelligence – Risk Management», який визначає методологію оцінювання ризиків, пов'язаних із використанням ШІ, зокрема у сфері обробки персональних даних [7];

− ISO/IEC 38507:2022 «Governance of IT – Governance implications of artificial intelligence», що встановлює вимоги до корпоративного управління ШІ, зокрема підзвітність, прозорість і відповідальність [8].

Міжнародне співробітництво у сфері захисту персональних даних формується на перетині політичних інтересів держав, економічних стратегій цифрового розвитку та глобальної конкуренції технологічних платформ. Держави прагнуть узгодити стандарти обробки даних для взаємного визнання рівня захисту, що є передумовою для безпечної транскордонної передачі даних.

Зважаючи на вищенаведене, очевидно, що міжнародне співробітництво у досліджуваній сфері відзначатиметься ефективністю у разі, якщо правові аспекти будуть поєднуватися із формуванням м'якого права для координації спільних зусиль, а також з технічними аспектами, які передбачають безпосередні інструменти впровадження. Саме на перетині кожного з цих аспектів зрештою й мають формуватися практичні підходи щодо забезпечення сумісності, прозорості та безпеки обробки персональних даних у контексті використання ШІ та IoT.

Далі ми звернемо увагу на кожен з аспектів та розкриємо їх роль у контексті досліджуваної теми.

Перш за все вартим уваги є саме правовий аспект, який ґрунтується на нормах права та інституційних механізмах, що встановлюють обов'язки для володільців, розпорядників та третіх осіб, а також гарантії для суб'єктів персональних даних та засадничі положення, які стосуються юридичної відповідальності у вказаній сфері. У межах ЄС центральне місце займає, як ми вже зазначали, займає Загальний регламент про захист даних, який закріплює принципи опрацювання даних (стаття 5), вимоги щодо законності опрацювання (стаття 6), права суб'єктів даних (статті 12-22), механізми передавання персональних даних до третіх країн або міжнародних організацій (глава V) та умови для накладання адміністративних штрафів (стаття 83) [3].

Регуляторна рамка натомість доповнюється діяльністю наглядових органів, тобто Data Protection Authorities, а також Європейської ради з питань захисту даних, яка забезпечує узгодженість практики шляхом ухвалення інструкції, рекомендації та найкращі практики [9, с. 65] (наприклад, Керівні принципи 05/2021 щодо взаємодії між застосуванням статті 3 та положень про міжнародну передачу даних згідно з розділом V GDPR [10]).

Зрештою правовий аспект характеризується наявністю високого рівня юридичних гарантій, підзвітністю, наявністю адміністративних штрафів та процедур захисту прав.

Попри це, також існує позиція відповідно до якої жорсткість регуляцій може призводити до зростання сукупних витрат, складності імплементації та негативного впливу на конкурентоспроможність ЄС в економічній сфері [11]. У контексті транскордонної передачі даних це може призвести до створення бар'єру не тільки для передачі даних, а для впровадження інновацій.

Формування м'якого права передбачає, наприклад, створення рекомендацій, інструк-

цій, керівних принципів тощо, які розробляються через багатосторонні платформи та робочі групи. Тут варто відзначити Керівні принципи ОЕСР щодо конфіденційності від 2013 року [12] та Рамки ОЕСР для класифікації систем ШІ від 2022 року [13].

У контексті норм м'якого права сильною стороною є швидкість розробки та широка участь стейкголдерів, але попри це добровільний характер Керівних принципів ОЕСР обмежує їхню ефективність порівняно з інструментами жорсткого права [14, с. 497]. Відтак результативність цього інструменту має добровільний характер, оскільки він позбавлений обов'язкової сили, і, відповідно, корелює з правовою спроможністю держави забезпечити імплементацію розроблених настанов в національне законодавство.

Технічний аспект передбачає необхідність підкріплення правового регулювання відповідними технічними стандартами, які забезпечують практичне виконання правових вимог. Зважаючи на швидкий розвиток штучного інтелекту та Інтернету речей саме такі стандарти знаходяться на перетині між правовими нормами та технологічними процесами. Власне стандарти самі по собі не мають примусової юридичної сили та потребують синхронізації із правовими нормами та нормами м'якого права.

Висновки. Зрештою для здійснення ефективної імплементації найкращих європейських практик у сфері захисту персональних даних в умовах розвитку штучного інтелекту та Інтернету речей Україні потрібно здійснити модернізацію правового регулювання: від гармонізації законодавства про захист персональних даних із положеннями Загального регламенту про захист даних до необхідності врегулювати питання пов'язані зі штучним інтелектом, наприклад, запровадивши класифікацію ризиків та вимоги до прозорості та мінімізації збору даних. Технічною опорою для України має стати адаптація та впровадження міжнародних стандартів як-от ISO/IEC 27701 для належного управління ризиками штучного інтелекту.

Як наслідок поєднання жорсткого права з механізмами м'якого права, регуляторних пісочниць та різноманітних стимулів для бізнесу має дозволити зберегти баланс між захистом прав людини та технологічним розвитком, а також полегшить транскордонний обмін даними в інтересах національної безпеки та інновацій.

Список використаної літератури:

1. Гордійчук-Бурдіна Х.І., Іванова Т.В. Концептуальні засади міжнародного економічного співробітництва. *Міжнародне науково-технічне співробітництво: принципи, механізми, ефективність*: зб. наук. пр. XXI (XXXIII) Міжнар. наук.-практ. конф., 17-18 квітня. 2025р. Київ : КПІ ім. Ігоря Сікорського, 2025. С. 30-32.
2. OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data. URL: https://www.oecd.org/content/dam/oecd/en/publications/reports/2002/02/oecd-guidelines-on-the-protection-of-privacy-and-transborder-flows-of-personal-data_g1gh255f/9789264196391-en.pdf?utm
3. 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#top
4. Конвенція про захист осіб у зв'язку з автоматизованою обробкою персональних даних, прийнята, 28 січня 1981 року у м. Страсбург. URL: https://zakon.rada.gov.ua/laws/show/994_326#Text.
5. Convention 108 +. Convention for the protection of individuals with regard to the processing of personal data. URL: https://www.europarl.europa.eu/meetdocs/2014_2019/plmrep/COMMITTEES/LIBE/DV/2018/09-10/Convention_108_EN.pdf
6. ISO/IEC 27701:2025 «Information security, cybersecurity and privacy protection – Privacy information management systems – Requirements and guidance. URL: https://www.iso.org/obp/ui/en/#iso:std:iso-iec:27701:ed-2:v1:en
7. ISO/IEC 23894:2023 – Information technology – Artificial intelligence - Risk management. URL: https://oecd.ai/en/catalogue/tools/isoiec-238942023-information-technology-artificial-intelligence-risk-management
8. ISO/IEC 38507:2022 – Information technology – Governance of IT – Governance implications of the use of artificial intelligence by organizations
9. Bielikova M. Recommendations and guidelines of the European Data Protection Board as a tool to prevent transnational and international disputes. Míľniky práva v stredoeurópskom priestore 2023 / Veronika Ťažká (zost.). Bratislava: Právnická fakulta Univerzity Komenského v Bratislave., 2023. 600 s.
10. Guidelines 05/2021 on the Interplay between the application of Article 3 and the provisions on international transfers as per Chapter V of the GDPR. URL: https://www.edpb.

europa.eu/our-work-tools/documents/public-consultations/2021/guidelines-052021-interplay-between-application_en
11. Reducing regulatory burden to restore the EU's competitive edge. 68 proposals for the reduction of regulatory burden in 2025. URL: https://www.businesseurope.eu/wp-content/uploads/2025/02/2025-01-22_businesseurope_mapping_of_regulatory_burden-d55-1.pdf
12. The OECD Privacy Framework. 2013. URL: https://www.afapdp.org/wp-content/uploads/2018/06/oecd_privacy_framework.pdf
13. OECD Framework for the Classification of AI Systems. 2022. URL: https://www.oecd.org/content/dam/oecd/en/publications/reports/2022/02/oecd-framework-for-the-classification-of-ai-systems_336a8b57/cb6d9eca-en.pdf
14. Mayar A., Maas K. The effectiveness of the OECD Guidelines' NCP procedure. *Business and Society Review*. 2024. № 129 (3). P. 479-501. https://doi.org/10.1111/basr.12368

Pishta V. I., Drabiuk S. S., Rozhkova M. G. International institutional cooperation in the field of personal data protection in the conditions of the development of artificial intelligence and the Internet of Things

The article provides a comprehensive analysis of institutional models of international cooperation in the field of personal data protection amid the rapid development of artificial intelligence and the Internet of Things. It examines the interaction between international organizations, supranational bodies, national authorities, and the private sector in shaping harmonized legal, technical, and ethical mechanisms of governance. Particular attention is given to universal and regional instruments, including Convention 108+, the General Data Protection Regulation, the OECD Privacy Guidelines, and modern ISO/IEC standards that define technical requirements for risk management and privacy governance.

The article identifies key challenges related to cross-border data flows, the harmonization of regulatory approaches, and the role of technical standards as tools that foster trust, transparency, and interoperability between data processing systems in the international digital environment.

Special attention is given to how the norms of hard law and soft law relate to each other. It is explained that legal acts can provide a high level of protection and clear guarantees for individuals involved in cross-border data exchange. However, they may also create certain barriers for such data flows. At the same time, soft law instruments – such as recommendations, guidelines, and principles developed by international organizations – allow for a faster response to challenges caused by the rapid development of digital technologies. The authors highlight the role of the EDPB, OECD, and several related initiatives.

The article also focuses on the importance of the technical aspect of regulation, which is shown through the analysis of international standards such as ISO/IEC 27701, 23894, and 38507.

Finally, attention is paid to the factors important for Ukraine's successful integration into the global digital environment. The authors conclude that it is necessary to harmonize Ukrainian legislation with the General Data Protection Regulation and other international standards.

Key words: *international cooperation, personal data, artificial intelligence, Internet of Things, GDPR.*

Дата першого надходження рукопису до видання: 21.07.2025
Дата прийнятого до друку рукопису після рецензування: 25.08.2025
Дата публікації: 30.09.2025