УДК 342.738:614.2:004.89
DOI https://doi.org/10.24144/2788-6018.2025.06.3.73

ЗАХИСТ ПЕРСОНАЛЬНИХ МЕДИЧНИХ ДАНИХ У СИСТЕМАХ ШТУЧНОГО ІНТЕЛЕКТУ: МІЖНАРОДНО-ПРАВОВІ МЕХАНІЗМИ ТА ПРОБЛЕМИ ЇХ ІМПЛЕМЕНТАЦІЇ

Скалецька З.С.,
доцент, доктор правових наук,
Республіка Польща,
доцент,
Національний університет
«Києво-Могилянська академія»
ORCID: 0000-0001-9162-4836

Скалецька З.С. Захист персональних медичних даних у системах штучного інтелекту: міжнародно-правові механізми та проблеми їх імплементації.

Цифрова трансформація систем охорони здоров'я, зокрема стрімке впровадження технологій штучного інтелекту (ШІ), спричиняє глибоку зміну традиційних підходів до збирання, аналізу та зберігання персональних медичних даних. Розширені можливості алгоритмів машинного навчання, здатних працювати з багатовимірними та високочутливими інформаційними масивами, одночасно відкривають потенціал для підвищення ефективності медичних послуг і формують нові загрози конфіденційності. Зростає ризик несанкціонованого доступу, повторної ідентифікації пацієнтів, упровадження алгоритмічних упереджень, що можуть призвести до дискримінації окремих груп, а також небезпека цілеспрямованих кібератак на медичну інфраструктуру. За таких умов пріоритетного значення набуває розроблення та впровадження дієвих міжнародно-правових механізмів регулювання використання ШІ в галузі охорони здоров'я.

Метою статті є всебічний аналіз провідних міжнародних нормативних інструментів захисту медичних даних, зокрема GDPR (ЄС), HIPAA (США), APPI (Японія), та визначення їх ефективності щодо гарантування конфіденційності в середовищі, де домінують інтелектуальні технології. Особливу увагу приділено порівнянню вимог до мінімізації даних, забезпечення прозорості алгоритмів, дотримання принципів справедливості та юридичної відповідальності у процесі автоматизованого прийняття рішень. Проаналізовано специфіку імплементації цих стандартів у медичних інформаційних системах різних країн, виокремлено фактори, що ускладнюють узгодження регуляторних вимог у глобальному цифровому середовищі: технологічну складність моделей ШІ, відсутність уніфікованих підходів до управління ризиками, недостатню адаптацію етичних норм до реалій автоматизованої медицини.

На основі студій прикладних кейсів застосування ШІ у лікарняних інформаційних системах наголошено, що ефективний захист персональних медичних даних можливий лише за умови взаємодії технологічних рішень (шифрування, федеративне навчання, диференційна конфіденційність), правових інструментів та етичних принципів медичної практики. Зроблено висновок про необхідність подальшої гармонізації міжнародних стандартів, розроблення узгодженої міждержавної політики й формування глобальної системи нагляду, здатної забезпечити безпечний, прозорий і підзвітний розвиток ШІ у сфері охорони здоров'я.

Ключові слова: штучний інтелект, медичні дані, GDPR, HIPAA, APPI, кібербезпека, медичне право.

Skaletska Z.S. Protection of personal medical data in artificial intelligence systems: international legal mechanisms and problems of their implementation.

The digital transformation of healthcare systems, particularly the rapid integration of artificial intelligence (AI) technologies, is fundamentally reshaping traditional approaches to the collection, analysis, and storage of personal medical data. The growing capabilities of machine-learning algorithms, which can process multidimensional and highly sensitive information arrays, simultaneously expand the potential for improving the efficiency of medical services and create new threats to privacy. Risks of unauthorized access, patient re-identification, algorithmic bias leading to discrimination, and targeted cyberattacks on medical infrastructure are steadily increasing. Under these conditions, the development and implementation of effective international legal mechanisms regulating the use of AI in healthcare becomes a critical priority.

The aim of the article is to provide a comprehensive analysis of leading international regulatory instruments for protecting medical data– specifically the GDPR (EU), HIPAA (USA), and APPI (Japan)– and to evaluate their effectiveness in ensuring confidentiality in an environment dominated by intelligent technologies. Particular attention is paid to comparing requirements related to data minimization, algorithmic transparency, adherence to fairness principles, and legal responsibility in automated decision-making processes. The article examines the specifics of implementing these standards in medical information systems across different countries and identifies key factors that hinder regulatory harmonization in a global digital environment, such as the technological complexity of AI models, the absence of unified risk-management approaches, and the insufficient adaptation of ethical norms to the realities of automated medicine.

Based on an analysis of applied cases of AI deployment in hospital information systems, the study emphasizes that effective protection of personal medical data is possible only through the combined use of technological solutions (encryption, federated learning, differential privacy), legal tools, and the ethical principles of medical practice. The article concludes by highlighting the need for further harmonization of international standards, the development of coordinated intergovernmental policies, and the creation of a global oversight system capable of ensuring safe, transparent, and accountable AI development in the healthcare sector.

Key words: artificial intelligence, medical data, privacy, GDPR, HIPAA, APPI, cyber security.

Постановка проблеми. Сучасна людина постійно генерує дані – від показників фітнес-браслета до запитів у медичних застосунках. Сфера охорони здоров'я особливо вразлива, адже саме в ній концентруються найцінніші, надчутливі відомості про стан здоров'я, генетичні характеристики та медичні втручання. Упровадження систем ШІ розширює можливості обробки таких даних, але водночас створює ризики втручання у приватність, алгоритмічної дискримінації та кіберзагроз. Це зумовлює потребу в ефективних міжнародних правових механізмах, які б гарантували безпеку персональних медичних даних у цифрову епоху.

Аналіз останніх досліджень і публікацій. Проблематика захисту персональних даних у сфері медицини активно досліджується як українськими, так і міжнародними науковцями. Значний внесок зроблено в роботах І. Діордіци та О. Коваля щодо інтеграції систем ШІ у системи безпеки медичних даних; у працях М. Міци та О. Рябощука про перспективи систем ШІ в охороні здоров'я; у дослідженнях Roy S., Wang C., Morley J. та інших авторів, які аналізують етичні та правові аспекти алгоритмічної обробки медичної інформації. У міжнародному вимірі важливими є рекомендації ВООЗ, документи ЄС, наукові огляди з питань governance AI у healthcare.

Метою статті є сформулювати та обґрунтувати системний підхід до міжнародно-правового регулювання захисту персональних медичних даних у процесі використання систем ШІ, визначити ключові проблеми та окреслити можливі напрями вдосконалення правових механізмів.

Виклад основного матеріалу. В умовах стрімкої цифрової трансформації систем охорони здоров'я питання обробки персональних медичних даних набуває все більшої актуальності, оскільки саме ці дані становлять базу для роботи сучасних алгоритмів штучного інтелекту, систем підтримки клінічних рішень, медичних інформаційних платформ та аналітичних сервісів. Медичні дані є однією з найбільш чутливих категорій персональної інформації через їхній глибоко приватний характер, тривалий життєвий цикл та високий потенціал негативних наслідків у разі порушення конфіденційності. Вони включають не лише традиційні клінічні відомості – історію хвороб, результати лабораторних досліджень, діагностичні зображення, – але й нові типи біомедичних даних, такі як геномні, протеомні та біометричні показники, які дедалі частіше використовуються у персоналізованій медицині та моделях прогнозування.

З появою штучного інтелекту значно розширилися можливості застосування таких даних для діагностики, прогнозування перебігу захворювань, скринінгу патологій та оптимізації лікувальних стратегій. Водночас використання великих наборів даних (Big Data) створює додаткові загрози – від ризику ідентифікації особи навіть у нібито анонімізованих масивах до потенційних маніпуляцій алгоритмами, які можуть спричинити дискримінаційні рішення. Наукові дослідження вказують, що навіть добре оброблені знеособлені дані можуть бути повторно ідентифіковані шляхом перехресного аналізу з іншими доступними наборами, що ставить під сумнів ефективність традиційних методів анонімізації [12, с. 87].

Міжнародно-правове регулювання обробки медичних даних перебуває на етапі активного формування. Загальний регламент про захист даних Європейського Союзу (далі General Data Protection Regulation – GDPR) (Regulation (EU) 2016/679), який сьогодні є однією з найбільш ефективних та комплексних систем захисту даних в Європейському Союзі, визначає медичні дані як спеціальну категорію, що потребує підвищеного рівня захисту та обґрунтування правових підстав для оброб-

ки. Значну увагу приділено принципам мінімізації, пропорційності, прозорості та цільового використання інформації, а також необхідності проведення оцінки впливу на захист даних (DPIA), коли впроваджуються високоризикові технології, включаючи алгоритми машинного навчання [16]. У США система HIPAA забезпечує галузевий характер регулювання та встановлює конкретні технічні й адміністративні стандарти безпеки, зокрема вимоги до шифрування, контролю доступу та ведення обліку всіх дій користувачів. Японська APPI демонструє гнучкіший підхід і поєднує можливості для інновацій зі строгими правилами щодо обмеження збору та передачі даних третім сторонам, зокрема у хмарних інфраструктурах [13].

Окремої уваги потребують технологічні аспекти захисту медичних даних, оскільки правові норми можуть бути ефективними лише за умов належного технічного забезпечення їх реалізації. Сучасні технології включають криптографічні механізми (симетричне та асиметричне шифрування, криптографію на основі гомоморфних функцій, багатосторонні обчислення), методи псевдонімізації та анонімізації, диференційну приватність, федеративне навчання, технології доступу без розкриття даних (zero knowledge proofs), а також системи моніторингу та виявлення аномальної поведінки користувачів. Зокрема, диференційна приватність активно використовується в системах популяційних медичних досліджень для мінімізації ризику витоку інформації про конкретну особу під час агрегованого аналізу. Так зване федеративне навчання дає змогу зберігати дані в локальних медичних установах, уникаючи централізації великих масивів інформації, що зменшує ризик масштабних витоків, але водночас ускладнює перевірку якості моделі [12, с. 90].

Етичні виклики у сфері застосування штучного інтелекту в медицині є не менш значущими, ніж правові чи технічні. Проблема «чорної скриньки» ускладнює визначення критеріїв, за якими алгоритм ухвалює рішення, і може створювати перешкоди для реалізації права пацієнта на отримання пояснення. Алгоритмічні упередження часто виникають також через нерепрезентативність вибірки, неправильний підбір параметрів або неконтрольовані кореляції, що призводить до дискримінації за расовими, віковими, статевими чи соціально-економічними та іншими ознаками. У сфері охорони здоров'я це може мати критичні наслідки – наприклад, занижену точність діагностики для певних груп пацієнтів чи обмеження доступу до ефективного лікування. Дослідження свідчать, що складні алгоритми машинного навчання можуть відтворювати або підсилювати наявні соціальні нерівності, якщо їх тренують на історичних медичних записах, які вже містять системні упередження [10].

Практичний досвід провідних медичних центрів підтверджує необхідність комплексного підходу до захисту даних. Університетський госпіталь Гамбург-Еппендорф упровадив систему штучного інтелекту для виявлення аномальної поведінки у доступі до медичних записів, що суттєво зменшило кількість інцидентів порушення конфіденційності [15]. Аналіз застосування Watson Health IBM показує, що хоча ШІ може підвищити якість діагностики та пришвидшити прийняття клінічних рішень, проблеми валідації моделей та можливість упереджених результатів залишаються значними. Досвід Національної служби охорони здоров'я Великої Британії демонструє важливість стандартизації протоколів обробки даних, оскільки взаємодія між системами, що працюють за різними нормативами, ускладнює аналіз та використання інформації [5, 6]

Таким чином, ефективна система правового регулювання обробки медичних даних у системі ШІ повинна поєднувати вимоги міжнародного права щодо захисту приватного життя, технічні засоби захисту, етичні стандарти, організаційні механізми контролю та міждисциплінарний підхід до впровадження технологій. Наявні в світі моделі регулювання, хоч і відрізняються між собою, демонструють прагнення до забезпечення балансу між розвитком інновацій та захистом прав людини. Водночас відсутність єдиної глобальної нормативної системи створює бар'єри для міжнародного обміну даними і стримує розвиток транснаціональних медичних проектів. Подальша правова гармонізація стандартів, створення однакових вимог до прозорості алгоритмів, удосконалення методів технічного захисту та формування універсальних підходів до етичних аспектів використання систем ШІ є необхідними кроками для забезпечення сталого майбутнього цифрової медицини з дотримання поваги прав людини.

Додатковий аналіз міжнародних тенденцій свідчить, що застосування систем штучного інтелекту в медичній сфері потребує значно ширших правових та організаційних підходів, ніж ті, що нині існують. Багато країн знаходяться на етапі формування власних нормативних моделей, і хоча вони часто спираються на базові принципи захисту даних, їхні практичні рішення суттєво різняться 21 . Це зумовлює ризики нормативної фрагментації та ускладнює транскордонний обмін медичними даними, особливо у великих дослідницьких консорціумах, які активно працюють з алгоритмами машинного навчання. Важливим викликом є те, що сучасні моделі систем ШІ здатні працювати з даними, отриманими з різних юрисдикцій, і водночас не всі нормативні системи забезпечують однаковий рівень захисту, що створює ситуації так званих "регуляторних прогалин".

Країни Європейського Союзу вже стикаються з труднощами узгодження GDPR з новим Регламентом ЄС про штучний інтелект (далі – AI Act), який запроваджує категоризацію ризиків для застосувань ШІ, включаючи медичні системи [17]. Наприклад, системи діагностичного аналізу зображень відносяться до високоризикових, а отже потребують суворої сертифікації, аудитів та доведення прозорості алгоритмів. Однак, практична реалізація вимог AI Act залишається складною, оскільки медичні моделі часто використовують глибокі нейронні мережі, внутрішня логіка яких не піддається легкому тлумаченню. У деяких дослідженнях відзначається, що абсолютна прозорість так званих «моделей чорних скриньок» («black box models») принципово неможлива, тому регулятори мають змінити підходи до вимог Explainable AI (XAI), збалансувавши наукову реальність і потреби етичного контролю [18].

У США регуляція в галузі систем ШІ та медичних даних розвивається шляхом адаптації чинних механізмів, зокрема HIPAA, та впровадження рекомендацій Управління з контролю за продуктами і ліками (далі – FDA). FDA вже створило окрему концепцію регуляції алгоритмів, що оновлюються ("Software as a Medical Device" та "Adaptive AI"), відповідно до якої модель повинна проходити постійний моніторинг після розгортання, адже дані, на яких вона працює, змінюються в реальному часі. Цей підхід деякі дослідники називають "циклічною регуляторною моделлю", оскільки він передбачає безперервний контроль, а не одноразову сертифікацію продукту [1, 2].

У сфері технічного захисту даних важливо відзначити, що просте застосування стандартних засобів шифрування не гарантує безпеки медичних даних, оскільки багато загроз пов'язані не з перехопленням інформації, а з атаками на структуру використовуваних моделей. Зокрема, дедалі частіше застосовуються методи атак "membership inference", коли зловмисник може визначити, чи входили дані конкретного пацієнта до тренувальної вибірки моделі. Інший тип загроз – "model inversion attacks", які дозволяють відновлювати характеристики оригінальних даних на основі вихідних параметрів моделі. Такі атаки особливо небезпечні для геномних даних, оскільки вони є унікальними і практично не піддаються справжній анонімізації [20]. Це вимагає впровадження додаткових технічних засобів – від диференційної приватності до контролю вхідних і вихідних запитів моделі, створення захищених апаратних середовищ та використання федеративних платформ.

Зростає також роль етичних та біоетичних комітетів, міждисциплінарних груп, які здійснюють оцінку впливу систем ШІ на права людини. Експерти з біоетики наполягають на необхідності включення до процедури оцінювання моделей медичних систем ШІ таких критеріїв, як ризик дискримінації, можливість помилкової класифікації, здатність алгоритму підтримувати автономію пацієнта та забезпечувати інформовану згоду. Університетська лікарня Цюриха вже використовує спеціальні етичні аудитні протоколи для проєктів систем ШІ, де оцінюються не лише технічні параметри моделі, але й її вплив на організаційні процеси та взаємодію між лікарем і пацієнтом [3].

Варто звернути увагу, що питання інформованої згоди значно ускладнюється у випадку використання систем ШІ. Традиційні форми згоди, які передбачають розуміння пацієнтом конкретної мети обробки даних, можуть бути недостатніми, оскільки використання систем ШІ включає можливість подальшого навчання моделі, застосування вторинного аналізу та потенційної передачі даних у зовнішні дослідницькі групи. Саме тому в багатьох країнах розвивається концепція "динамічної згоди" – коли пацієнт може поступово ухвалювати рішення щодо різних аспектів використання своїх даних і змінювати ці рішення у будь-який момент [19]. Проте реалізація цієї концепції потребує складних цифрових платформ і підвищення цифрової грамотності населення, що є додатковим викликом особливо для країн з обмеженими технічними ресурсами.

Ще одним глобальним питанням є нерівність доступу до технологій штучного інтелекту. Країни з високим рівнем цифровізації охорони здоров'я уже переходять до використання автономних діагностичних систем, тоді як інші регіони лише починають цифровізувати базові медичні процеси. Це створює ризик "цифрової асиметрії", коли якість медичної допомоги, доступ до сучасних методів лікування та обсяг даних для досліджень значною мірою залежатимуть від рівня технологічного розвитку країни. Деякі науковці попереджають про можливість "епідеміологічного упередження", коли моделі, треновані на даних розвинених країн, не будуть адекватно працювати в суспільствах із іншими демографічними характеристиками, патернами захворюваності та умовами життя [14].

Таким чином, сучасні тенденції засвідчують, що створення ефективної системи правового регулювання обробки медичних даних у системах штучного інтелекту потребує комплексного підходу, що включає оновлення законодавства, розвиток технічних інструментів, підвищення біоетичної відповідальності, удосконалення механізмів інформованої згоди та забезпечення рівності доступу до технологій. Розвиток систем ШІ в медицині неможливий без узгоджених міжнародних стандартів, довіри пацієнтів і гарантованого захисту їхніх персональних даних. Наукова спільнота підкреслює, що формування глобального правового регулювання є не лише рекомендованим, а й необхідним етапом для зменшення ризиків і реалізації потенціалу технологій у сфері охорони здоров'я.

Висновки. Захист персональних медичних даних у системах штучного інтелекту є одним з ключових викликів сучасної цифрової медицини. Проведене дослідження засвідчило, що правові режими різних держав – ЄС, США, Великої Британії, Канади, Японії – демонструють спільну тенденцію до посилення вимог щодо конфіденційності, прозорості та безпеки алгоритмів. Водночас між ними існують значні відмінності, що ускладнюють транскордонний обмін даними та інтеграцію глобальних медичних систем.

GDPR задає найжорсткіші стандарти у сфері медичних даних, зокрема через обов'язковість DPIA, суворі обмеження доступу та вимогу алгоритмічної прозорості. HIPAA фокусується на галузевих вимогах до безпеки даних та відповідальності суб'єктів медичної інфраструктури, а APPI забезпечує збалансоване регулювання приватності в умовах швидкого технологічного розвитку Японії.

Виявлено, що основні загрози, пов'язані з використанням систем ШІ у медичній сфері, включають непрозорість алгоритмів, потенційні упередження, ризики кібератак, технічну несумісність старих медичних систем із новітніми рішеннями та біоетичні дилеми щодо відповідальності. Для мінімізації цих ризиків необхідні комплексні підходи: удосконалення міжнародних стандартів, створення механізмів незалежного аудиту та сертифікації алгоритмів систем ШІ, впровадження багаторівневих систем кіберзахисту та підвищення компетентності медичного персоналу.

Окреме значення має розвиток спільної міжнародної політики у сфері захисту персональних та медичних даних, що забезпечить сумісність правових режимів і сприятиме безпечному обміну даними для наукових досліджень, телемедицини та розробки інноваційних систем штучного інтелекту. У кінцевому підсумку ефективний захист персональних медичних даних можливий лише за умов балансу між технологічним прогресом, правовим контролем і фундаментальним дотриманням прав людини на приватність.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. AI in Medicine: Pros & Cons. Go Online Law School. URL: https://www.goonlinelawschool.com/post/ai-in-medicine-pros-cons (дата звернення: 15.11.2025).
2. Aldoseri A., Al-Khalifa K.N., Hamouda A.M. Re-thinking data strategy and integration for artificial intelligence: concepts, opportunities, and challenges. *Applied Sciences*. 2023. № 13. С. 7082. URL: https://www.mdpi.com/2076-3417/13/12/7082.
3. Ellahham S., Ellahham N. Application of artificial intelligence in the health care safety context: opportunities and challenges. American Journal of Medical Quality. 2020. URL: https://journals.sagepub.com/doi/abs/10.1177/1062860619878515.
4. Forcier M.B., Gallois H., Mullan S. Integrating artificial intelligence into health care through data access: can the GDPR act as a beacon for policymakers? *Journal of Law and the Biosciences*. 2019. № 1. С. 317. URL: https://academic.oup.com/jlb/ article-abstract/6/1/317/5570026.
5. Gerke S., Minssen T., Cohen G. Ethical and legal challenges of artificial intelligencedriven healthcare. Artificial Intelligence in Healthcare. 2020. URL: https://www.sciencedirect.com/science/article/pii/B9780128184387000125.
6. Kasula B.Y. Framework Development for Artificial Intelligence Integration in Healthcare: Optimizing Patient Care and Operational Efficiency. Transactions on Latest Trends in IoT. 2023. URL: https://www.ijsdcs.com/index.php/TLIoT/article/ view/406.
7. Liaw S.T., Liyanage H., Kuziemsky C. Ethical use of electronic health record data and artificial intelligence: recommendations of the primary care informatics working group. Yearbook of Medical Informatics. 2020. URL: https://www.thieme-connect.com/products/ejournals/html/10.1055/s-0040-1701980.
8. Morley J., Murphy L., Mishra A., Joshi I. Governing data and artificial intelligence for health care: developing an international understanding. JMIR Formative Research. 2022. URL: https://formative.jmir.org/2022/1/e31623.
9. Pablo R.G.J., Roberto D.P., Victor S.U. Big data in the healthcare system: a synergy with artificial intelligence and blockchain technology. *Journal of Integrative Bioinformatics*. 2022. URL: https://www.degruyter.com/document/doi/ 10.1515/jib-2020-0035/html.
10. Roy S. Privacy Prevention of Health Care Data Using AI. *Journal of Data Acquisition and Processing*. 2022. URL: https://www.researchgate.net/profile/Soumit-Roy-3/publication/375957548_PRIVACY_PREVENTION_OF_HEALTH_CARE_DATA_USING_AI/links/6564e0b8ce88b87031197ecc/PRIVACY-PREVENTION-OF-HEALTHCARE-DATA-USING-AI.pdf.
11. Wang C., Zhang J., Lassi N., Zhang X. Privacy protection in using artificial intelligence for healthcare: Chinese regulation in comparative perspective. *Healthcare*. 2022. № 10. С. 1878. URL: https://www.mdpi.com/2227-9032/10/10/1878.

12. Діордіца І.В. Інтеграція штучного інтелекту в системи захисту персональних даних у сфері охорони здоров'я. *Наука і техніка сьогодні* (Серія «Педагогіка», Серія «Право», Серія «Економіка», Серія «Техніка», Серія «Фізико-математичні науки»). 2024. № 5 (33). С. 87–97. URL: http://perspectives.pp.ua/index.php/nts/article/view/11764.
13. Міца О. Дослідження перспектив використання засобів штучного інтелекту в галузі охорони здоров'я. URL: https://dspace.uzhnu.edu.ua/jspui/bitstream/lib/37126/1/0.pdf
14. ЦЕДЕМ. Захист персональних даних у добу штучного інтелекту: міжнародні підходи та виклики. URL: https://cedem.org.ua/consultations/zahyst-personalnyh-danyh-u-dobu-shtuchnogo-intelektu-mizhnarodni-pidhody-ta-vyklyky/ (дата звернення: 15.11.2025).
15. Erste KI-Anwendung zur Erstellung von Arztbriefen im UKE im Einsatz. URL : https://www.uke.de/allgemein/presse/pressemitteilungen/detailseite_154368.html (дата звернення: 15.11.2025).
16. Регламент ЄС 2016/679 «Загальний регламент про захист даних». URL: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679 (дата звернення: 15.11.2025).
17. Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828. URL: https://eur-lex.europa.eu/eli/reg/2024/1689/oj/eng (дата звернення: 15.11.2025).
18. Cynthia Rudin, Stop Explaining Black Box Machine Learning Models for High Stakes Decisions and Use Interpretable Models Instead// *Nature Machine Intelligence*, Vol 1, May 2019, 206–215 2018. URL: https://explainableairesearch.github.io/publications/rudin2018stop/ (дата звернення: 15.11.2025).
19. Lee, A.R., Koo, D., Kim, I.K. *et al.* Identifying facilitators of and barriers to the adoption of dynamic consent in digital health ecosystems: a scoping review. *BMC Med Ethics* 24, 107 (2023). https://doi.org/10.1186/s12910-023-00988-9.
20. Zhang C, Bonomi L. Mitigating Membership Inference in Deep Learning Applications with High Dimensional Genomic Data. Proc (IEEE Int Conf Healthc Inform). 2022 Jun; 2022:10.1109/ichi54592.2022.00101. doi: 10.1109/ichi54592.2022.00101. Epub 2022 Sep 8. PMID: 36120416; PMCID: PMC9473339. URL: https://pmc.ncbi.nlm.nih.gov/articles/PMC9473339/?utm_source=chatgpt.com (дата звернення: 15.11.2025).
21. Greenleaf, Graham, Global Data Privacy Laws 2023: 162 National Laws and 20 Bills (February 10, 2023). (2023) 181 Privacy Laws and Business International Report (PLBIR) 1, 2-4, UNSW Law Research Paper No. 23–48. URL : http://dx.doi.org/10.2139/ssrn.4426146 (дата звернення: 15.11.2025).