DOI: 10.33498/louu-2024-09-064

Ольга Россильна

кандидатка юридичних наук,
старша наукова співробітниця відділу проблем модернізації господарського права та законодавства
Державної установи "Інститут економіко-правових досліджень імені В. К. Мамутова Національної академії наук України"
(Київ, Україна)
Researcher ID LLM-7344-2024
ORCID ID: https://orcid.org/0000-0002-1648-6063
rossylna@gmail.com

УДК 346.7:342.721:614.2

АДАПТАЦІЯ ЗАКОНОДАВСТВА УКРАЇНИ У СФЕРІ ЕЛЕКТРОННИХ ДАНИХ ПРО ЗДОРОВ'Я ДО ПРАВА ЄВРОПЕЙСЬКОГО СОЮЗУ

Анотація. Актуальність питання захисту електронних даних про здоров'я значно зросла в умовах розвитку цифрових технологій та інтеграції України до Європейського Союзу. Попри низку законодавчих ініціатив, у сфері охорони здоров'я досі спостерігається фрагментація даних, відсутність єдиної стратегії розвитку інформаційних систем і недостатній рівень захисту персональних даних. Такі виклики зумовлюють необхідність адаптації законодавства України до європейських стандартів, зокрема до положень Загального регламенту про захист даних (GDPR), а також впровадження ефективних механізмів вторинного використання електронних медичних даних.

Метою статті є аналіз законодавчих підходів до захисту електронних даних про здоров'я в Україні та ЄС, оцінка поточного стану адаптації українського законодавства до європейських вимог і визначення ключових напрямів його удосконалення з урахуванням міжнародних стандартів.

У дослідженні застосовано методи порівняльного правознавства для аналізу європейського та українського законодавства у сфері електронних даних про здоров'я. Використано також формально-юридичний та системно-структурний методи для оцінки законодавчих ініціатив та їхньої відповідності міжнародним стандартам.

Проведений аналіз свідчить про те, що електронні дані про здоров'я, зокрема дезагреговані та неперсональні дані, є важливим інструментом для розвитку системи охорони здоров'я. Проте в Україні законодавство у цій сфері залишається фрагментованим і потребує удосконалення. Основні проблеми полягають у відсутності єдиної стратегії розвитку електронної системи охорони здоров'я, недостатньому захисті персональних даних і слабкій нормативно-правовій базі для вторинного використання електронних даних. Пропонується впровадження механізмів для покращення управління електронними медичними даними, адаптація нормативних актів до положень GDPR і створення єдиної цифрової платформи для ефективної обробки таких даних.

Отже, Україна потребує ґрунтовної адаптації свого законодавства до європейських вимог у сфері захисту електронних даних про здоров'я. Це дасть змогу забезпечити не лише захист персональних даних, а й створити можливості для ефективного використання неперсональних даних у наукових дослідженнях та медичній практиці. Також важливою є розбудова інфраструктури цифрових послуг у сфері охорони здоров'я, що сприятиме інтеграції України до європейського простору охорони здоров'я.

Ключові слова: електронні дані про здоров'я; персональні дані; неперсональні дані; дезагреговані дані; захист даних; право ЄС; вторинне використання даних; охорона здоров'я.

Попри численні наукові дослідження у сфері захисту електронних даних про здоров'я, тема не втрачає актуальності. Це пов'язано з низкою факторів, зокрема: постійним оновленням законодавства та труднощами в імплементації положень права ЄС; підвищенням обізнаності громадськості про власні права у зазначеному напрямі та усвідомленням важливості захисту своїх даних; порушенням прав осіб на захист персональних даних, у тому числі через витоки інформації та зловживання використання даних; розвитком інформаційних технологій, штучного інтелекту та цифровізації, що сприяє зростанню обсягу даних, які збираються та обробляються; в умовах розвитку інформаційного суспільства зростає значення не лише правового, а й етичного та соціального виміру конфіденційності та довіри.

Проблемі захисту персональних даних свою увагу присвятили такі вчені, як: А. Біла-Кисельова, Т. Гуржій, А. Петрицький, О. Тимошенко, С. Гусаров, К. Мельник, С. Лаптєв, І. Похиленко, Т. Попович, О. Кізлова, В. Бойко, М. Василенко, М. Бем, І. Городинський, Г. Саттон, О. Родіоненко, М. Бєлова, Д. Бєлов та ін. Питання захисту медичних даних досліджували І. Сенюта, К. Токарєва, С. Вахненко, А. Мусієнко, В. Мусієнко та ін.

Метою дослідження є визначення правових аспектів обробки та захисту електронних даних про стан здоров'я відповідно до норм європейського права, аналіз відповідності національного законодавства України європейським вимогам щодо обробки електронних медичних даних, а також вивчення необхідності вдосконалення нормативно-правової бази для забезпечення конфіденційності, безпеки та прозорості обробки електронних даних у сфері охорони здоров'я.

Передусім варто з'ясувати загалом, що являють собою дані про здоров'я. Відповідно до положень Загального регламенту про захист даних (GDPR)[1] під "даними щодо стану здоров'я" розуміються персональні дані, що стосуються стану фізичного чи психічного здоров'я фізичної особи, зокрема надання медичних послуг, що відображають інформацію про її стан здоров'я. Персональні дані щодо стану здоров'я повинні містити всі дані, що пов'язані зі станом здоров'я суб'єкта даних і розкривають інформацію про минулий, поточний або майбутній стан фізичного або психічного здоров'я суб'єкта даних. Це включає інформацію про фізичну особу, зібрану під час реєстрації на надання послуг або надання послуг, у сфері охорони здоров'я, як вказано у Директиві Європейського Парламенту і Ради 2011/24/ЄС. Водночас необхідно звернути увагу на більш системний підхід, запропонований у Проєкті Регламенту Європейського Парламенту та Ради про Європейський простір даних про стан здоров'я (далі – Проєкт Регламенту), у якому відповідно до визначеної мети та предмета регулювання базовим терміном

[1] Regulation (EU) 2016/679 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 and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) <https://eur-lex.europa.eu/eli/reg/2016/679/oj> (accessed 10.10.2024).

визначено "електронні медичні дані". Останні, своєю чергою, поділяються на персональні та неперсональні електронні медичні дані:

> *персональні електронні дані про стан здоров'я* – дані про стан здоров'я та генетичні дані, як вони визначені в Регламенті (ЄС) 2016/679, а також дані, що стосуються детермінант здоров'я, або дані, що обробляються у зв'язку з наданням медичних послуг, які обробляються в електронній формі;
> *неперсональні електронні дані про здоров'я* – дані, що стосуються здоров'я та генетичні дані в електронному форматі, які не підпадають під визначення персональних даних, наведене в ст. 4(1) Регламенту (ЄС) 2016/679[2].

Українське законодавство в галузі персональних даних порівняно недавно розпочало свій рух у напрямі адаптації до положень європейського законодавства, саме тому перебуває ще в активній фазі створення відповідних умов для забезпечення сталого й високого рівня захисту фізичних осіб та усунення перешкод для потоків персональних даних, з одного боку, та належного рівня захисту – з другого[3]. Загальним нормативно-правовим актом України у сфері персональних даних, порядку їх збирання, обробки, передачі тощо є Закон України "Про захист персональних даних"[4]. Варто зауважити, що натепер більшість законодавчих актів, а також проєктів нормативно-правових актів містять відсилочні норми до згаданого Закону. Особливої актуальності це набуло в епоху діджиталізації, а також з активним розвитком і впровадженням електронних реєстрів різного спрямування. Саме тому кожен законопроєкт оцінюється на відповідність його положень у сфері захисту персональних даних міжнародно-правовим зобов'язанням у сфері європейської інтеграції та праву ЄС.

Оцінка відповідності нормативно-правових актів України міжнародно-правовим зобов'язанням у сфері європейської інтеграції щодо забезпечення належного рівня захисту електронних даних про здоров'я здійснюється з урахуванням передусім таких положень Угоди про асоціацію між Україною з однієї сторони, та Європейським Союзом, Європейським Співтовариством з атомної енергії і їхніми державами-членами, з іншої сторони (надалі – Угода про асоціацію)[5]:

– загальною для всіх сфер правового регулювання є ст. 15 Угоди про асоціацію, згідно з якою Сторони домовились співробітничати з метою *забезпечення належного рівня захисту персональних даних відповідно до найвищих європейських та міжнародних стандартів, зокрема відповідних документів*

[2] Proposal for a Regulation of The European Parliament and of the Council on the European Health Data Space COM/2022/197 final <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52022PC0197> (accessed 10.10.2024).
[3] О Россильна, 'Європейський вимір персоналізованої медицини та великих даних' [2023] 2 Науковий вісник ДДУВС 51–56. DOI: 10.31733/2078-3566-2023-6-51-56.
[4] Про захист персональних даних: Закон України від 1 червня 2010 р. № 2297-VI <https://zakon.rada.gov.ua/laws/show/2297-17#Text> (дата звернення 10.10.2024).
[5] Association Agreement between the European Union and its Member States, of the one part, and Ukraine, of the other part <https://eur-lex.europa.eu/eli/agree_internation/2014/295/oj> (accessed 10.10.2024).

Ради Європи. Співробітництво у сфері захисту персональних даних може включати, inter alia, обмін інформацією та експертами;

– відповідно до ст. 426 Угоди про асоціацію Сторони розвивають співробітництво в галузі охорони здоров'я з метою підвищення рівня його безпеки та захисту здоров'я людини як передумови сталого розвитку та економічного зростання;

– з метою забезпечення співробітництва у сферах зміцнення системи охорони здоров'я, запобігання і контролю за інфекційними та неінфекційними захворюваннями, обміну інформацією та знаннями в галузі охорони здоров'я Сторони здійснюють спільні заходи в рамках підходу *"охорона здоров'я у всіх політиках"* та поступової інтеграції України в європейські мережі охорони здоров'я (ст. 427 Угоди про асоціацію);

– згідно зі ст. 389 Угоди про асоціацію Сторони зміцнюють своє співробітництво щодо розвитку інформаційного суспільства на користь приватних осіб і бізнесу через забезпечення загальнодоступності інформаційно-комунікаційних технологій (ІКТ) та через кращу якість послуг за доступними цінами. Водночас відповідно до ст. 391(1a) Угоди про асоціацію таке співробітництво охоплює сферу сприяння широкосмуговому доступу, поліпшення безпеки мереж та широкому використанню ІКТ приватними особами, бізнесом та адміністративними органами шляхом розвитку локальних ресурсів Інтернет і впровадження онлайн-послуг, зокрема електронного бізнесу, електронного уряду, *електронної охорони здоров'я* та електронного навчання.

Крім того, важливість захисту даних, у тому числі щодо здоров'я, підкреслено у низці міжнародних документів Європейського Союзу та Ради Європи. Безпосередньо цьому питанню присвячені ст. 8 Хартії Європейського Союзу про основоположні права, ст. 16 Договору про функціонування Європейського Союзу, ст. 8 Конвенції про захист прав людини і основоположних свобод (та відповідна практика Європейського суду з прав людини), ст. 6 Конвенції № 108 про захист осіб у зв'язку з автоматизованою обробкою персональних даних та ін.

Питання захисту даних у сфері охорони здоров'я нерозривно пов'язане з відповідним рівнем формування *системи електронної охорони здоров'я.* Попри всі успіхи в зазначеній царині, Україна наразі перебуває ще на початковому етапі формування та удосконалення відповідної системи.

У Звіті Європейської Комісії щодо України[6] відзначено, що, незважаючи на запуск системи електронної охорони здоров'я, включаючи електронні рецепти, продовжує існувати фрагментація та дублювання даних у сфері охорони здоров'я. В Україні не існує стратегії розвитку інформаційної системи

[6] Ukraine 2023 Report Accompanying the document Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions 2023 Communication on EU Enlargement policy <https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=SWD:2023:699:FIN> (accessed 10.10.2024).

охорони здоров'я, а нормативно-правова база потребує доопрацювання. *Відсутність або низька якість дезагрегованих даних у сфері охорони здоров'я є однією з ключових системних проблем,* яка впливає на процеси планування та формування політики, а також на реалізацію програм у сфері охорони здоров'я.

Система електронної охорони здоров'я має формуватися в контексті загальних підходів ЄС "Здоров'я в усіх політиках" та "Єдине здоров'я". Технології кібербезпеки, такі як цифрова ідентифікація, криптографія та виявлення вторгнень, а також їх застосування в такій сфері, як охорона здоров'я мають важливе значення для забезпечення безпеки та довіри до діяльності з боку громадян, державних адміністрацій та бізнесу (п. 39 преамбули Регламенту (ЄС) 2021/694[7]). Розбудова інфраструктури цифрових послуг системи електронної охорони здоров'я, розширення її новими цифровими послугами щодо профілактики захворювань, забезпечення доступу до більш якісних даних для досліджень, профілактики захворювань і персоналізованої охорони здоров'я та медичної допомоги належить до переліку проєктів, які становлять спільний інтерес і слугують розгортанню і найкращому використанню цифрових можливостей або інтероперабельності (Додаток I до Регламенту (ЄС) 2021/694[8]). Не викликає сумнівів також теза про те, що активний розвиток телекомунікаційних і глобальних комп'ютерних мережевих технологій привів до появи такого виду злочинного посягання кіберзлочинності, як транскордонна комп'ютерна злочинність[9], що становить безпосередню загрозу також і для безпеки медичних даних.

Відповідно до ст. 14 Директиви 2011/24/ЄС від 9 березня 2011 р. про застосування прав пацієнтів на транскордонні послуги в галузі охорони здоров'я (далі – Директива 2011/24/ЄС)[10] Європейський Союз підтримує та сприяє співробітництву та обміну інформацією між державами-членами, які працюють у рамках добровільної мережі, що об'єднує національні органи, відповідальні за електронну охорону здоров'я, призначені державами-членами. Серед завдань мережі системи електронної охорони здоров'я, зокрема, є розробка та впровадження ефективних методів для забезпечення використання медичної інформації в інтересах громадського здоров'я та наукових досліджень. Однак, як зазначається, положення Директиви 2011/24/ЄС є добровільними за своєю природою, що частково пояснює, чому цей аспект Директиви продемонстрував обмежену ефективність у підтримці

[7] Regulation (EU) 2021/694 of the European Parliament and of the Council of 29 April 2021 establishing the Digital Europe Programme and repealing Decision (EU) 2015/2240 <https://eur-lex.europa.eu/eli/reg/2021/694/oj> (accessed 10.10.2024).

[8] Ibid.

[9] А Мусієнко, В Мусієнко, 'Актуальні аспекти нормативно-правових механізмів захисту персональних даних в електронних медичних реєстрах в Україні' [2022] 1 (11) DICTUM FACTUM 17–22.

[10] Directive 2011/24/EU of the European Parliament and of the Council of 9 March 2011 on the application of patients' rights in cross-border healthcare <https://eur-lex.europa.eu/eli/dir/2011/24/oj> (accessed 10.10.2024).

контролю фізичних осіб над їхніми персональними електронними даними про здоров'я на національному та транскордонному рівнях і дуже низьку ефективність щодо вторинного використання електронних даних про здоров'я[11].

Щодо опрацювання (обробки) персональних електронних даних про здоров'я, то відповідні операції (збирання, реєстрація, організація, структурування, зберігання, адаптація чи зміна, пошук, ознайомлення, використання, розкриття через передавання, розповсюдження чи надання іншим чином, упорядкування чи комбінування, обмеження, стирання чи знищення) наразі у Європейському Союзі регулюються положеннями Регламенту (ЄС) 2016/679 Європейського Парламенту та Ради, а для інституцій та органів Союзу – Регламентом (ЄС) 2018/1725 Європейського Парламенту та Ради[12].

Питання персональних даних щодо здоров'я є надзвичайно чутливим для кожної особи. Саме з цієї причини відповідні дані є одним із пунктів переліку, що визначені ст. 6 Конвенції № 108 як особлива категорія даних, які не можуть піддаватися автоматизованій обробці, якщо внутрішнє законодавство не забезпечує відповідних гарантій. Обробка конфіденційних даних, як правило, заборонена, за винятком деяких конкретних випадків. Зокрема, обробка конфіденційних даних допускається, коли це необхідно для забезпечення громадського здоров'я на основі законодавства ЄС або національного законодавства.

За загальним правилом, відповідно до ст. 9(1) Загального регламенту про захист даних обробка генетичних даних, біометричних даних з метою однозначної ідентифікації фізичної особи, даних про стан здоров'я заборонена. Водночас це положення не застосовується за умови, що така обробка необхідна з міркувань суспільного інтересу у сфері громадського здоров'я (ст. 9(2i) Загального регламенту про захист даних). Крім того, законодавство Союзу або держави-члена може обмежувати за допомогою законодавчих заходів обсяг обов'язків і прав, передбачених Загальним регламентом про захист даних, якщо це є необхідним і пропорційним заходом, зокрема, для цілей забезпечення громадського здоров'я (ст. 23(e) Загального регламенту про захист даних). Необхідно також враховувати, що неоднакове впровадження та тлумачення Загального регламенту про захист даних державами-членами створює значні правові невизначеності, що призводить до перешкод для вторинного використання електронних даних про здоров'я[13].

[11] Proposal for a Regulation on the European Health Data Space COM/2022/197 (n 2).
[12] Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC <https://eur-lex.europa.eu/eli/reg/2018/1725/oj> (accessed 10.10.2024).
[13] Proposal for a Regulation on the European Health Data Space COM/2022/197 (n 2).

Варто зазначити, що прийняття Проєкту Регламенту про Європейський простір даних про здоров'я у поєднанні з GDPR значно кристалізує права фізичних осіб, зокрема, на: отримання доступу до своїх медичних даних в електронній формі негайно, безкоштовно і в легко читабельному, доступному й загальноприйнятому форматі; поширення своїх даних у електронній формі іншим медичним працівникам при переході в іншу лікарню без перешкод з боку попередніх постачальників медичних послуг або виробників; внесення даних до своєї електронної медичної картки про себе або про своїх дітей; внесення змін до помилкових даних онлайн; обмеження доступу до своїх електронних медичних даних (або їх частини); отримання інформації про фахівців, які мають доступ до їхніх даних[14].

Водночас інформаційна платформа громадського здоров'я призначена для збирання та зберігання агрегованої знеособленої інформації. З точки зору формування політики у сфері громадського здоров'я вторинне використання даних є надзвичайно важливим. Персональні дані повинні бути агреговані або анонімізовані в первинному джерелі, мінімізуючи ризики для захисту даних і зберігаючи контроль з боку первинного контролера даних. Набори персональних даних та агреговані або анонімізовані дані повинні зберігатися окремо, принаймні за допомогою логічного розділення, а в ідеалі – у фізично відокремлених IT-системах. Інфраструктура повинна бути створена за необхідності на основі концепції псевдонімізації (а не анонімізації), що дає змогу контролерам даних громадського здоров'я повертатися до окремого суб'єкта даних тією мірою, якою це приносить безпосередню користь суб'єкту даних[15]. На думку К. Токарєвої, закріплення в законодавстві обов'язку володільців і розпорядників персональних медичних даних здійснювати псевдонімізацію таких даних значно покращить інформаційну безпеку та дотримання права на таємницю про стан здоров'я особи[16].

Європейський простір даних охорони здоров'я встановлює загальні рамки ЄС, що дають змогу використовувати дані охорони здоров'я для досліджень, інновацій, громадського здоров'я, формування політики, регуляторної діяльності та персоналізованої медицини. Він спиратиметься на створення нової децентралізованої інфраструктури ЄС для вторинного використання даних охорони здоров'я (HealthData@EU), яка об'єднає органи доступу до даних охорони здоров'я, що мають бути створені у всіх державах-членах[17].

[14] The European Health Data Space (EHDS) <https://www.european-health-data-space.com> (accessed 10.10.2024).

[15] The protection of personal data in health information systems – principles and processes for public health (World Health Organization, 2021) <https://iris.who.int/bitstream/handle/10665/341374/WHO-EURO-2021-1994-41749-57154-eng.pdf?sequence=1&isAllowed=y> (accessed 10.10.2024).

[16] К Токарєва, 'Проблема захисту персональних даних у сфері охорони здоров'я в умовах інформатизації' [2022] 11 Юридичний науковий електронний журнал 496–499. DOI https://doi.org/10.32782/2524-0374/2022-11/120.

[17] The European Health Data Space (n 14).

А отже, враховуючи євроінтеграційний курс України, це стане новим юридичним, етичним та технологічним викликом.

Додатково варто зауважити, що право на здоров'я є інклюзивним правом, яке поширюється не лише на своєчасну та належну медичну допомогу, а й на основні детермінанти здоров'я, такі як доступ до безпечної питної води та належних санітарних умов, здорові умови праці та навколишнього середовища, а також доступ до медичної освіти та інформації, зокрема з питань сексуального та репродуктивного здоров'я[18]. Отже, створення та ведення інформаційних систем у сфері охорони здоров'я, яка підтримує доступ до медичної інформації та управління системами охорони здоров'я, є юридично визнаним інтересом, який повинен бути збалансований із захистом даних. Досягнення відповідності прав потребує належного документування та прозорості по відношенню до всіх зацікавлених сторін, включаючи широку громадськість і суб'єктів даних, на яких впливає діяльність. Цей процес також важливий для визначення того, чи може діяльність з обробки даних вимагати згоди суб'єкта даних або чи законний, переважаючий правовий інтерес виправдовує обробку персональних даних.

Очікується, що більш чіткі правила та механізми, що підтримують вторинне використання електронних медичних даних, а також обов'язкову транскордонну інфраструктуру для вторинного використання електронних медичних даних буде встановлено з прийняттям Регламенту Європейського Парламенту та Ради про Європейський простір даних у сфері охорони здоров'я. Саме цей Регламент має закласти основу для вторинного використання електронних медичних даних, запроваджуючи більш конкретні правила для сектору охорони здоров'я, що охоплюють обмін електронними медичними даними і можуть впливати на постачальників послуг з обміну даними, формати, що забезпечують портативність медичних даних, правила співпраці для альтруїзму даних у сфері охорони здоров'я та взаємодоповнюваність щодо доступу до приватних даних для вторинного використання.

Висновки. За результатами проведеного дослідження можна виокремити декілька ключових аспектів. Передусім адаптація законодавства України у сфері електронних даних про здоров'я до права ЄС забезпечить більш ефективний захист персональних даних громадян України та сприятиме розвитку інформаційних систем у сфері охорони здоров'я. Основні проблеми законодавства України в цій сфері пов'язані з фрагментацією нормативно-правової бази та відсутністю комплексної стратегії розвитку інформаційних систем охорони здоров'я, що призводить до дублювання даних та недостатнього захисту персональних даних.

Правове регулювання електронних даних про здоров'я в ЄС наразі базується на положеннях Загального регламенту про захист даних (GDPR),

[18] The protection of personal data in health information systems – principles and processes for public health (n 15).

який визначає чіткі вимоги щодо обробки персональних медичних даних та впровадження систем захисту конфіденційності. Необхідність імплементації положень acquis ЄС щодо електронної охорони здоров'я та захисту персональних даних зумовлена тим, що це сприятиме покращенню якості надання медичних послуг в Україні та підвищенню рівня захисту прав пацієнтів.

Встановлено, що важливу роль у формуванні ефективної системи охорони здоров'я відіграють дезагреговані та неперсональні електронні дані про здоров'я. Використання неперсональних електронних даних про здоров'я, що не підпадають під визначення персональних, дає змогу забезпечити проведення наукових досліджень, аналіз епідеміологічних даних і покращення управління системою охорони здоров'я без порушення конфіденційності пацієнтів.

Вторинне використання електронних даних про здоров'я є одним із ключових напрямів розвитку системи електронної охорони здоров'я, особливо в контексті наукових досліджень і громадського здоров'я. Це включає використання знеособлених і неперсональних даних для аналізу, прогнозування та покращення якості медичних послуг. Водночас існує необхідність упровадження чітких правових механізмів, що гарантують безпеку і захист цих даних під час їх повторного використання.

Важливими кроками для забезпечення безпеки та довіри до системи електронних даних про здоров'я, а також предметом подальших досліджень слугуватимуть особливості нормативно-правового забезпечення створення Єдиного цифрового простору охорони здоров'я та впровадження новітніх технологій, таких як криптографія, цифрова ідентифікація тощо.

REFERENCES

Bibliography

Journal articles

1. Musiienko A, Musiienko V, 'Aktualni aspekty normatyvno-pravovykh mekhanizmiv zakhystu personalnykh danykh v elektronnykh medychnykh reiestrakh v Ukraini' [2022] 1 (11) DICTUM FACTUM 17–22.
2. Rossylna O, 'Ievropeiskyi vymir personalizovanoi medytsyny ta velykykh danykh' [2023] 2 Naukovyi visnyk DDUVS 51–56. DOI: 10.31733/2078-3566-2023-6-51-56.
3. Tokarieva K, 'Problema zakhystu personalnykh danykh u sferi okhorony zdorovia v umovakh informatyzatsii' [2022] 11 Yurydychnyi naukovyi elektronnyi zhurnal 496–499. DOI https://doi.org/10.32782/2524-0374/2022-11/120.

Websites

4. The European Health Data Space (EHDS) <https://www.european-health-data-space.com/> (accessed 10.10.2024).
5. The protection of personal data in health information systems – principles and processes for public health (World Health Organization, 2021) <https://iris.who.int/bitstream/handle/10665/341374/WHO-EURO-2021-1994-41749-57154-eng.pdf?sequence=1&isAllowed=y> (accessed 10.10.2024).

Olha Rossylna

ADAPTATION OF UKRAINIAN LEGISLATION IN THE FIELD OF ELECTRONIC HEALTH DATA TO THE LAW OF THE EUROPEAN UNION

Abstract. The relevance of the issue of electronic health data protection has increased significantly in the context of the development of digital technologies and Ukraine's integration into the European Union. Despite some legislative initiatives, the healthcare sector is still characterised by data fragmentation, lack of a unified strategy for the development of information systems and insufficient protection of personal data. Such challenges require the adaptation of Ukrainian legislation to European standards, in particular to the provisions of the General Data Protection Regulation (GDPR), as well as the introduction of effective mechanisms for the secondary use of electronic health data.

The purpose of the article is to analyse the legislative approaches to the protection of electronic health data in Ukraine and the EU, to assess the current state of adaptation of Ukrainian legislation to European requirements and to identify the key areas for its improvement with due regard to international standards.

The study uses comparative law methods to analyse European and Ukrainian legislation in the field of electronic health data. Formal legal and system-structural methods were also used to assess legislative initiatives and their compliance with international standards.

The analysis shows that electronic health data, including disaggregated and non-personal data, is an important tool for healthcare system development. However, in Ukraine, legislation in this area remains fragmented and needs to be improved. The main challenges include the lack of a unified strategy for the development of the eHealth system, insufficient protection of personal data, and a weak legal framework for the secondary use of electronic data. It is proposed to introduce mechanisms to improve the management of electronic health data, adapt regulations to the GDPR and create a single digital platform for the efficient processing of such data.

Thus, Ukraine needs to thoroughly adapt its legislation to European requirements in the field of electronic health data protection. This will not only ensure the protection of personal data, but also create opportunities for the effective use of non-personal data in research and medical practice. It is also important to develop the infrastructure of digital healthcare services, which will facilitate Ukraine's integration into the European healthcare area.

Keywords: electronic health data; personal data; non-personal data; disaggregated data; data protection; EU law; secondary use of data; healthcare.