

КОНФІДЕНЦІЙНІСТЬ ІНФОРМАЦІЇ ПРО РЕПРОДУКТИВНЕ ЗДОРОВ'Я ЛЮДИНИ: ЦИФРОВІ ВИКЛИКИ ТА ПРОБЛЕМИ ПРАВОВОГО РЕГУЛЮВАННЯ

DOI: <http://dx.doi.org/10.18370/2309-4117.2025.80.70-84>

А.І. СУББОТ

д. ю. н., професор, завідувач кафедри публічного та європейського права ПЗБО «Київський міжнародний університет», м. Київ
ORCID: 0000-0002-1453-9379

К.О. КАЛАЧЕНКОВА

к. ю. н., доцентка кафедри господарського та адміністративного права Донецького національного університету ім. Василя Стуса, м. Вінниця
ORCID: 0000-0003-0720-2476

В.В. БЕРЧ

д. ю. н., доцентка, професорка кафедри конституційного права та порівняльного правознавства Ужгородського національного університету, м. Ужгород
ORCID: 0000-0002-3837-4724

А.В. БАСАЛАЄВА

PhD, доцентка кафедри конституційного права Київського національного університету ім. Тараса Шевченка, м. Київ
ORCID: 0000-0001-7558-2621

Б.П. РАТУШНА

к. ю. н., доцентка кафедри права Львівського національного університету ветеринарної медицини та біотехнологій ім. Степана Гжицького, м. Львів
ORCID: 0000-0003-2645-9242

В.І. ПРОДАН

PhD, старша викладачка кафедри конституційного права та порівняльного правознавства юридичного факультету ДВНЗ «Ужгородський національний університет», м. Ужгород
ORCID: 0009-0008-3805-5150

Контакти:

Калаченкова Катерина
Олександрівна
Донецький національний університет ім. Василя Стуса,
21021, вул. 600-річчя, 21,
м. Вінниця, Україна
Email: k.kalachenkova@
dopnu.edu.ua
Тел.: +380 (432) 50 89 30
+38 (066) 082 21 29

ВСТУП

Питання конфіденційності у сфері громадського здоров'я для сучасної держави в умовах глобальних трансформацій має ключове значення, що зумовлено такими факторами: чутливість питання здоров'я громадян в умовах екологічних криз; проблеми низької народжуваності та ментальних загроз; гуманізація суспільства та потреба обстоювання власних життєвих кордонів людини із забезпеченням поваги до її приватності; кризові явища пандемічного, суспільного та політичного характеру, які деструктивно впливають на стан громадського здоров'я; розвиток віртуального середовища, цифрових технологій, електронного публічного урядування, що створює небезпеку поширення приватної інформації особи без її дозволу; поява засобів штучного інтелекту (ШІ), які дають змогу обробляти та генерувати значні бази даних, що стосуються пацієнта (так, збираючи та зіставляючи дані із соціальних мереж, ШІ може отримати особисто чутливі дані та використати їх неправомірно, зокрема в контексті дискримінації особи за станом здоров'я; недобросовісні фармацевтичні та медичні компанії можуть використовувати персональні дані про особу з метою нав'язування реклами чи комерціалізації послуг через таргетування); невизначеність правового регулювання захисту персональних даних у медичній сфері, наявність прогалин у цьому сегменті права та колізійності норм. Усе зазначене актуалізує наукову та праксеологічну увагу до проблеми унормування питань конфіденційності у сфері медицини загалом.

Питання здоров'я нації має онтологічну цінність для суспільства та розвитку цивілізації, зокрема репродуктивне здоров'я тут займає провідне місце, оскільки забезпечує можливість відтворення та продовження роду. Глобальні, віртуальні, технологічні, соціально-культурні зміни сучасного суспільства трансформують усі сфери, пов'язані із забезпеченням громадського репродуктивного здоров'я. Такі виклики мають аксіологічний вплив, пов'язаний, зокрема, з доступністю інформації, зручністю використання різних новітніх технологічних засобів для самостійного

моніторингу репродуктивних функцій організму, зниженням витрат держави та громадян на медико-організаційну діяльність тощо. Водночас репродуктивне здоров'я зазнає девальваційного впливу внаслідок цифрових загроз та інших конвенційних викликів.

Чутливість інформації у сфері репродуктивного здоров'я зумовлена не тільки правовими, етичними та медичними чинниками, але й має онтологічно-філософську природу, оскільки вищий рівень соціальної конкордії полягає в гуманізації суспільного життя через абсолютизацію прав людини, зокрема прав на приватність та відтворення. Автономна воля особистості втілюється в ідеї захисту медичної інформації, насамперед чутливої – даних про репродукцію, репродуктивний анамнез та наміри пацієнта як суб'єкта права.

Біоетичні засади суспільства перебувають у конфлікті з новими можливостями, що зумовлює біхевіористичне спрямування розвитку медицини та репродуктивних технологій, правові колізії, прогалини та інформаційні загрози. Такий конфлікт виникає внаслідок неузгодженості нових технологій, що застосовуються в медицині в галузі репродуктивного здоров'я, з правом пацієнта чи користувача на конфіденційність інформації та дотриманням принципу обов'язкової згоди на розголошення інформації.

Уся парадигма суспільних відносин формує складне комплексне поле правових, організаційних, етико-медичних та технологічних чинників, тому її зміни зумовлюють потребу в оновленні правового регулювання питань конфіденційності особи у сфері охорони та захисту інформації про її репродуктивне здоров'я, що можливо здійснити лише в результаті широкого наукового та громадського обговорення проблеми, визначення етико-медичних дискусійних аспектів та пошуку ефективного, вираженого рішення.

Предмет дослідження був проаналізований науковцями вітчизняної та зарубіжної шкіл у контексті трьох сфер – правової, технічної та медичної. Питання конфіденційності інформації про пацієнта та медичної таємниці аналізувалися фахівцями здебільшого у сфері правознавства.

Першу групу становлять наукові праці, присвячені правовому обґрунтуванню регулювання приватності медичної інформації в нових умовах. Цивільно-правовий режим охорони права на лікарську таємницю як ключовий елемент захисту приватного життя особи в умовах цифровізації медицини був предметом низки досліджень останніх років [1–3]. Крім того, І.В. Діордіца та співавт. [4] акцентували на юридичних проблемах захисту персональних даних у сфері охорони здоров'я в Україні [5].

Сфера медичної інформації та даних про пацієнта [6] була розглянута Т.В. Блашук і Д.О. Придатко в контексті функціонування Електронної системи охорони здоров'я (ЕСОЗ) в Україні, а також у зв'язку з можливістю отримання таких даних компетентними уповноваженими органами публічної влади [7].

Безпека та конфіденційність медичної інформації, насамперед стосовно можливості функціонування ШІ, були предметом ґрунтовного аналізу, проведеного науковцями ОАЕ [8], Великої Британії [9, 10], Канади [11], Греції [12], Австралії [13], Оману [14]. Така широка географія науковців, які цікавилися цим питанням, пояснюється затребуваністю оновлення та цифровізації медичної сфери у світлі нових технологічних можливостей.

Питання пошуку балансу між приватністю та державною безпекою аналізувала Eleni Filley [15]. M. Asmitha і S.M. Rajgoral у своїх роботах зосередилися на проблемі досягнення рівноваги між конфіденційністю та правом іншої особи на інформацію [16, 17]. Досліджень, що аналізують конфіденційність у медичній сфері, на сьогодні існує менше. R.J. Chung та співавт. стверджують, що пацієнти стикаються з низкою труднощів та перешкод у пошуку та отриманні конфіденційної допомоги [18]. Науковці також звертають увагу на проблеми конфіденційності електронної медичної інформації.

Другу групу становлять дослідження, що стосуються технологічних можливостей у медичній галузі, зокрема щодо забезпечення репродуктивного здоров'я. F.Y. Gbagbo та співавт. сфокусувалися на питанні забезпечення загального доступу до послуг у сфері сексуального та репродуктивного здоров'я в контексті досягнення Мети 3.7 «Цілей сталого розвитку»¹ до 2030 року, зокрема послуг із планування сім'ї, отримання інформації та освіти, а також інтеграції в національну стратегію [19]. Також N.F.M. Tohit та M. Naque розглядали медичне забезпечення у сфері прав людини в контексті кризових перепон у сталому розвитку [20].

Також досліджувалися додаткові можливості для покращення доступу до репродуктивної освіти за допомогою активного машинного навчання [21], розвитку інформаційних та медико-біологічних технологій [22], розвитку телемедицини [23].

До третьої групи досліджень належать доктринальні розробки, що стосуються репродуктивного, менструального, материнського здоров'я і сексуального благополуччя в контексті глобальних та технологічних загроз. Норвезькі та шведські дослідники аналізували рівень уваги до репродуктивного здоров'я підлітків через застосування нових цифрових інструментів [24]. N. Alfawzan та ін. досліджували безпеку жінок у зв'язку з використанням цифрових додатків, розроб-

лених для моніторингу репродуктивного здоров'я [25–27]. Вплив міграційних факторів на репродуктивне здоров'я також був предметом уваги наукової спільноти [28]. Зміни в правовій політиці щодо заборони абортів активізували проблему доступності інформації про сексуальне життя та репродуктивну діяльність. J. Sao та співавт. обґрунтовували небезпеку порушення конфіденційності сексуального та репродуктивного життя ризиком кримінального переслідування з боку органів влади США [29, 30] та Нігерії [31].

Розвиток ШІ та синергетичність його проявів актуалізували проблему технологічної неповноти у сфері забезпечення конфіденційності даних про пацієнтів і користувачів медичних послуг. L. Roudsari визначає, що у сфері акушерства та репродуктивного здоров'я такі прогалини мають гіперболізовану деструкцію, оскільки «визначаються глибокою етичною чутливістю та впливом на людину» [32].

Попри те що чимало сучасних наукових праць приділяли увагу цифровізації медичної сфери, сьогодні не існує єдиного, комплексного правового підходу, що може стати підґрунтям правової політики сучасності. Крім того, питання конфіденційності інформації в глобалізованому суспільстві технологічних можливостей саме в контексті репродуктивних прав людини ще не набуло достатнього наукового інтересу. Ця наукова стаття спрямована на заповнення цієї прогалини в сучасних суспільних відносинах та забезпечення потреби в комплексному, міжкомплементарному науковому підході до зазначеної проблеми.

Мета дослідження: аналіз екзистенційних викликів цифровізації у сфері конфіденційності інформації про репродуктивне здоров'я людини.

Для досягнення мети були поставлені такі завдання:

- виявити концептуальні засади цифровізації в репродуктивній медицині та трансформації репродуктивних і генетичних даних;
- визначити соціальні парадигми й суспільні уявлення, що формують ставлення до приватності та конфіденційної інформації у сфері репродуктивного здоров'я;
- узагальнити ключові міжнародні правові стандарти захисту репродуктивних і генетичних даних;
- проаналізувати медичну таємницю як об'єкт правового захисту в умовах цифрової трансформації;
- охарактеризувати особливу чутливість репродуктивних і генетичних даних та її значення для етики, приватності й data governance (управління даними);
- оцінити технологічні, кібербезпекові та ШІ-орієнтовані ризики в цифровій інфраструктурі репродуктивних даних і сервісів mHealth (мобільної охорони здоров'я) та FemTech (технічні розробки в галузі медицини жіночого здоров'я);
- інтерпретувати результати емпіричного онлайн-опитування щодо поінформованості, довіри та поведінкових реакцій на загрози витоку репродуктивних даних;
- сформулювати обґрунтовані пропозиції щодо вдосконалення національної правової політики та правового регулювання у сфері охорони здоров'я для забезпечення ефективного захисту репродуктивних даних в умовах цифровізації.

¹ «Цілі сталого розвитку» (або «Глобальні цілі») – ключові напрямки розвитку країн, що були ухвалені на Саміті ООН зі сталого розвитку на період із 2015 по 2030 роки.

МАТЕРІАЛИ ТА МЕТОДИ

Комплементарний підхід, який є провідним у цьому дослідженні, передбачає інтеграцію явищ, процесів та знань у сферах медицини, репродуктології, правознавства, інформатизації та техніки, оскільки лише поєднання окремих проявів у межах цілісного дослідження дає можливість отримати об'єктивні та ефективні результати.

Діалектичний метод використовується для системного філософського методологування, що дає можливість виявити суперечності в правовому регулюванні.

Етико-медичний підхід застосовувався для розуміння цінності приватності як основного вияву свободи та гідності особи й необхідності запиту добровільної згоди як на медичне втручання, так і на розголошення інформації, що є особливо чутливим у сфері репродуктивного здоров'я.

У межах застосування статистичного методу було розроблено та проведено онлайн-опитування, спрямоване на виявлення рівня обізнаності, довіри та побоювань населення щодо можливості витоку конфіденційної інформації про стан здоров'я, зокрема репродуктивного. Конструювання інструментарію ґрунтувалося на підборі чітко сформульованих питань, що охоплювали ключові компоненти цифрової поведінки та ставлення до конфіденційності, а також на використанні різних типів відповідей: рейтингових шкал (від 1 – «зовсім не згоден(-на)» до 5 – «повністю згоден(-на)»), поліваріантних, закритих і напівзакритих формулювань, що забезпечило валідність та релевантність отриманих даних.

Вибірка охоплювала 643 респонденти, середній вік яких становив 38,5 року, незалежно від статі, рівня освіти та місця проживання. Групу було сформовано методом зручної вибірки, що передбачало залучення респондентів, які мали доступ до цифрових опитувальників та виявили готовність добровільно взяти участь у дослідженні. Такий підхід є типовим для досліджень чутливих тем і дає змогу отримати валідні емпіричні дані щодо поведінкових та психологічних аспектів, пов'язаних із використанням цифрових медичних сервісів, навіть за відсутності формалізованої загальної сукупності.

Дослідження не потребувало схвалення етичного комітету, оскільки було повністю анонімним, не містило персональних даних і не передбачало будь-яких медичних втручань. Проект відповідає вимогам Гельсінської декларації (Declaration of Helsinki 1994, 2000, 2008) Всесвітньої медичної асоціації (World Medical Association) та етичним принципам, пов'язаним із медичними дослідженнями за участю людей. Усі учасники надали інформовану згоду на участь в анонімному дослідженні.

Первинна обробка та аналіз даних здійснювалися за допомогою методів описової статистики (середні значення, медіана, варіаційні характеристики), графічних методів візуалізації розподілів, а також критеріїв статистичного порівняння та виявлення асоціацій (зокрема, χ^2 Пірсона для незалежних вибірок). Для поглибленої перевірки зв'язків між шкальними змінними застосовувався ранговий коефіцієнт кореляції Спірмена. Статистичні обчислення виконувалися вручну та за допомогою спеціалізованого програмного забезпечення.

РЕЗУЛЬТАТИ ТА ОБГОВОРЕННЯ

Концептуальні основи цифровізації в репродуктивній медицині

Цифровізація стала невіддільним складником сучасних систем охорони здоров'я, трансформуючи способи отримання та зберігання медичної інформації й обміну нею. У репродуктивній медицині цифрова трансформація сягнула особливо чутливого виміру: електронні медичні карти, телемедичні консультації, програми відстеження фертильності та генетичні бази даних перетворилися на важливі інструменти клінічної практики. Ці технології дають змогу підвищити точність діагностики, забезпечити дистанційну підтримку пацієнтів та інтеграцію міждисциплінарних медичних команд. Однак вони також створюють безпрецедентні ризики для конфіденційності та захисту даних, оскільки репродуктивна медицина за своєю суттю має справу з інтимною та генетичною інформацією, яка стосується особистої ідентичності та сімейного життя.

Дані репродуктивної медицини мають подвійний характер – є одночасно медичними та генетичними, що зумовлює їхню особливу чутливість і підвищений ризик у разі цифрової обробки. Згідно зі звітами ВООЗ, дані про репродуктивне здоров'я класифікуються як одна з найбільш чутливих категорій персональних даних, неправильне використання яких може завдати незворотної шкоди окремим особам та сім'ям [33]. Загальний регламент про захист даних Європейського Союзу (General Data Protection Regulation (GDPR) [34]) чітко відносить дані про здоров'я та генетичну інформацію до «спеціальних категорій персональних даних» і, відповідно до ст. 9(1), забороняє їх обробку, якщо не дотримано суворих умов (GDPR, 2016). Українське законодавство також визнає цю чутливість та заборону обробки даних, пов'язаних зі здоров'ям, біометричних або генетичних даних, що зазначено в ст. 7 Закону України «Про захист персональних даних» [35].

Отже, цифровізація у сфері репродуктивної медицини потребує суворого балансу між інноваціями та конфіденційністю. Інструменти цифрової медицини – електронні репродуктивні реєстри, лабораторні інформаційні системи, інтегровані платформи mHealth – розширюють можливості лікування та прогнозування, але водночас збільшують ризики несанкціонованого доступу, витоку чи зловживання репродуктивними, сексуальними та генетичними даними. Чутливий характер цієї інформації створює високий потенціал для дискримінації, стигматизації та втручання в приватне життя. Саме тому надійні правові рамки, стандарти етичного нагляду та сучасні підходи до управління медичними даними (data governance) стають необхідною передумовою безпечної цифрової трансформації репродуктивної медицини.

З огляду на зазначене, подальший аналіз у статті зосереджений на виявленні конкретних технологічних загроз та правових ризиків, які виникають у процесі цифровізації репродуктивної медицини, а також на оцінці відповідності національного регулювання міжнародним стандартам захисту персональних даних.

Медична таємниця як об'єкт правового захисту в умовах цифровізації

Право пацієнта на збереження в таємниці відомостей про стан здоров'я, діагнози, результати обстеження, методи лікування та іншої інформації, отриманої під час медичного обслуговування, гарантується ст. 39-1 та ст. 40 Основ законодавства України про охорону здоров'я [36]. Ці положення конкретизуються в ст. 285 Цивільного кодексу України [37], де визначається, що пацієнт має право на таємницю щодо стану свого здоров'я, факту звернення за медичною допомогою, діагнозу та інших відомостей, отриманих під час його лікування.

Медична таємниця охоплює не лише класичні медичні записи, а й біометричні та генетичні дані, які набувають особливої цінності в сучасних е-системах охорони здоров'я (зокрема електронній системі eHealth). У контексті цифрової медицини поняття «медична таємниця» тісно пов'язане із забезпеченням конфіденційності, цілісності та безпеки персональних даних, що відповідає вимогам Європейської Конвенції про захист прав людини [38], а також положенням GDPR, який відносить інформацію про здоров'я до особливо чутливих категорій даних.

Так, ст. 8 Європейської конвенції з прав людини гарантує право на повагу до її приватного й сімейного життя, житла й кореспонденції. Хоча в ній прямо не згадуються поняття «здоров'я» чи «лікарська / медична таємниця», Європейський суд із прав людини послідовно тлумачить це положення як таке, що охоплює захист персональних даних про здоров'я та обов'язок конфіденційності в медичному контексті. У таких знакових справах, як «Z проти Фінляндії» (1997) [39] (§ 94–95), «I. проти Фінляндії» (2008) [40] та «LL проти Франції» (2006) [41], Суд підтвердив, що захист медичних даних є засадничим принципом права на приватність. Європейський суд із прав людини наголосив, що розкриття інформації, пов'язаної зі здоров'ям особи, без її згоди може суттєво вплинути на її приватне життя та підірвати довіру до системи охорони здоров'я. Отже, будь-яке втручання державних органів у конфіденційність даних про здоров'я має відповідати закону, мати законну мету та бути затребуваним у демократичному суспільстві, як того вимагає ст. 8 (2) Європейської конвенції з прав людини. Тобто, можна стверджувати, що медична таємниця – це не просто професійний обов'язок, а вимога прав людини, яка поширюється на управління електронними медичними записами та іншими цифровими системами, що містять конфіденційну медичну та генетичну інформацію.

Таке тлумачення узгоджує поняття лікарської таємниці із ширшими правами на приватність, роблячи її стандартом прав людини, а не просто професійним обов'язком. У цьому сенсі лікарська таємниця, згідно зі ст. 8 Європейської конвенції з прав людини, виходить за межі відносин між лікарем і пацієнтом і передбачає відповідальність держави за безпеку даних, захист цифрових медичних записів та нагляд за системами електронної охорони здоров'я.

Доречно узагальнити, що зазначена стаття Європейської конвенції з прав людини слугує нормативним містком між традиційними поняттями лікарської таємниці (закріпленими

в ст. 40 Основ законодавства України про охорону здоров'я та ст. 285 Цивільного кодексу України) та сучасною цифровою системою захисту даних, що регулюється такими інструментами, як GDPR та Конвенція 108+ [42]. Остання є оновленою версією Конвенції 1981 року й стосується захисту осіб у зв'язку з автоматизованою обробкою персональних даних.

Порівняльний аналіз свідчить, що українське законодавство поступово адаптується до європейських стандартів, однак відрізняється рівнем деталізації процедур обробки медичних даних. Наприклад, GDPR передбачає обов'язкове визначення відповідальної особи з питань захисту даних (Data Protection Officer (DPO)) у медичних закладах, тоді як в Україні ця функція здебільшого виконується формально або делегується працівникам IT-відділу. Крім того, європейські норми встановлюють суворі вимоги до отримання згоди на обробку генетичних та біометричних даних, що особливо важливо для діяльності закладів репродуктивної медицини. Практика показує, що саме в таких закладах найчастіше виникають порушення, пов'язані з неналежним інформуванням пацієнтів, зберіганням біоматеріалів та передачею результатів аналізів через незахищені цифрові канали.

Також слід звернути увагу, що в контексті репродуктивної медицини сфера лікарської таємниці виходить далеко за межі загальної медичної інформації та охоплює особливо чутливі категорії даних, а саме: інформацію про фертильний статус особи або діагноз безпліддя; використання допоміжних репродуктивних технологій (ДРТ), включно з екстракорпоральним заплідненням (ЕКЗ), криоконсервацією гамет або ембріонів та сурогатним материнством; ідентифікаційні дані донорів, реципієнтів та сурогатних матерів; генетичні або біометричні дані, отримані в результаті медичних або лабораторних обстежень.

Така інформація є «чутливими персональними даними», як згідно із законодавством України, так й із законодавством ЄС, і підлягає посиленому захисту. Ст. 40 Основ законодавства України про охорону здоров'я та ст. 285 Цивільного кодексу України встановлюють обов'язок медичних працівників зберігати конфіденційність будь-якої інформації, отриманої під час лікування, включно з репродуктивними та генетичними даними. Однак цифровізація репродуктивних послуг та розширення ЕКОЗ значно підвищують ризик несанкціонованого доступу, особливо там, де дані про донорів гамет або сурогатних матерів зберігаються в електронних базах даних без достатніх заходів шифрування або псевдонімізації.

Подальший правовий та етичний конфлікт виникає між правом дитини знати своє біологічне походження та правом донора на анонімність. Хоча українське законодавство наразі захищає конфіденційність донора, нещодавні законодавчі ініціативи (наприклад, Проект Закону № 13683 від 22.08.2025 р. «Про допоміжні репродуктивні технології» [43]) та судові дискусії відображають щораз більший тиск щодо визнання інтересу дитини до розкриття особистості відповідно до ст. 7 Конвенції ООН про права дитини та порівняльних європейських тенденцій (наприклад, Велика Британія, Швеція, Нідерланди). Відсутність чітких правових механізмів для балансування цих конкурентних прав створює невизначеність для клінік ЕКЗ, контролерів даних та медичних працівників,

які повинні забезпечувати дотримання вимог конфіденційності, реагуючи на потенційні заяви щодо ідентичності.

У підсумку цифровізація суттєво розширює межі традиційного інституту медичної таємниці, перетворюючи його на багатовимірний об'єкт правового захисту, що охоплює генетичні, біометричні та репродуктивні дані в електронних системах охорони здоров'я. У сфері репродуктивної медицини ці виклики постають особливо гостро, оскільки від конфіденційності залежить не лише приватність пацієнта, а й правовий статус донорів, реципієнтів, сурогатних матерів та майбутньої дитини. Саме тому подальший аналіз має бути зосереджений на технологічних та кібербезпекових загрозах, що виникають у процесі цифрової обробки репродуктивних даних, а також на структурних прогалинах у правовому регулюванні, які посилюють ці ризики.

Цифрова інфраструктура репродуктивних даних: типи загроз та соціально-правові наслідки

Сучасне суспільство, що розвивається під впливом цифрових та біотехнологічних трансформацій, характеризується невизначеним, біфуркаційним траєкторним розвитком. Технологічний прогрес у сфері медицини та даних створює одночасно сприятливі умови для розширення доступу до репродуктивних послуг, але й абсолютно нові ризики для конфіденційності. Ця дуальність відображає загальну закономірність цифрової модернізації: інновації суттєво покращують якість медичних послуг, але водночас ускладнюють захист приватної інформації, яка у сфері репродуктивного здоров'я має максимально чутливий характер.

З одного боку, можна стверджувати про значні досягнення технологічного прогресу щодо всіх сфер життя, серед яких репродуктивне здоров'я не є винятком. Наприклад, цифрові технології, як-от інтернет, текстові повідомлення та соціальні мережі використовуються як цінні інструменти поширення інформації про сексуальне та репродуктивне здоров'я. Також доводиться, що цифровізація у сфері охорони здоров'я (зокрема eHealth), що розширює використання цифрових технологій для передачі інформації, створює позитивний результат для інформування громадськості в досліджуваній сфері [44]. До суттєвих позитивних наслідків також слід додати точніше виявлення патологій або прогнозування результатів [45].

З іншого боку, технологічний та біомедичний прогрес спричиняє ряд екзистенційних дилем, які проблемно регулювати через їхню дискусійність та суперечливість щодо усталеної практики соціального буття. L.R. Ninsiima та співавт. стверджують, що сексуальне та репродуктивне здоров'я є основним складником глобального тягаря сексуальних проблем [46], які попри розвиток технологій досі не вирішені. Крім того, ці технологічні зміни породили додатково нові дискусії.

Ці проблеми лежать у двох площинах – безпечність цифрових технологій та загрози використання ШІ.

У сфері сексуального та репродуктивного здоров'я застосовується низка сучасних цифрових технологій, які успішно впроваджені в суспільну та медичну практику. Інформація про репродуктивне та сексуальне здоров'я представлена

в інформаційному ландшафті, а отже, і доступ до консультування та послуг, зокрема таких чутливих, як, наприклад, медикаментозний аборт, значною мірою опосередковується цифровими формами комунікації лікаря та пацієнта, використанням інтернету для пошуку інформації, зберігання даних на цифрових платформах, зверненням до соціальних мереж для пошуку інформації у сфері репродукції, застосуванням цифрових додатків – усе це загрожує кібербезпеці та підвищує ризик кібератак, а також недобросовісного збору даних сторонніми особами без автономної згоди пацієнта чи споживача медичної інформації. A.Z. Huq та R. Wexler зазначають, що цифрова епоха зумовлює потребу акцентувати не тільки на репродуктивних правах, але і їх захисті, зокрема як ключове постає питання, «чи наражає пошук медичної інформації на юридичну небезпеку» [47].

Особливо небезпечною є ситуація у сфері мобільних застосунків, що призначені для відстеження менструального циклу, фертильності чи вагітності. За даними аналітичного аудиту 25 популярних додатків, 84% із них мають можливість передавати персональні дані третім сторонам, а 67% пов'язані юридичними зобов'язаннями щодо такого обміну [48]. Відомі також численні випадки фактичного розголошення інформації.

Так, Федеральна торгова комісія США подала скаргу проти додатка «Flo Health Inc.» (найбільш завантажуваного додатка для відстеження менструації у світі у 2022 році [49]), звинувативши його в тривалому обміні конфіденційними даними про здоров'я користувачів із сервісами «Фейсбук», «Гугл», «Аппсфлаєр» та «Фларри». Намагаючись реагувати на звинувачення, додаток запровадив режим «Анонім», проте немає переконливих даних що такі заходи з деідентифікації є надійними. Також у 2023 році Комісія звинуватила додаток для відстеження менструації «Premom» в обмані користувачів щодо їхньої практики обробки даних шляхом розкриття інформації про здоров'я третім сторонам [50].

Додаткову небезпеку становлять так звані «темні патерни» – дезінформаційні або приховані інтерфейсні рішення, що спонукають користувачів розкривати більше даних, ніж це необхідно технічно чи етично. Вони супроводжуються прихованими механізмами передачі даних третім сторонам без дозволу власника даних [51]. Ці практики посилюють ризик не тільки комерційного таргетування, але й дискримінації за станом здоров'я, сексуальною орієнтацією або репродуктивним статусом. У деяких країнах можливість доступу до таких даних може призвести до кримінального переслідування жінок або медичних працівників у разі порушення абортних обмежень [52], що підкреслює суспільну небезпеку цифрових слідів.

Існують і доведені випадки продажу репродуктивних даних спеціалізованими брокерами інформації. Журналістські розслідування зафіксували пропозиції (понад 30 оголошень) щодо купівлі баз даних вагітних жінок, що містили інформацію про триместровість, методи планованих пологов та інші інтимні деталі. Така практика продажу даних була поширена багато років, особливу популярність вона мала в осіб, що надають послуги чи продають товари, що пов'язані з майбутнім батьківством. Це створює загрозу не лише для

приватності, але й для безпеки жінок, особливо в юрисдикціях із політично чутливими положеннями щодо репродуктивних прав. Аналітичний звіт, підготований в цій ситуації урядом, констатував, що продавалися різноманітні набори даних про мільйони майбутніх матерів – від інформації про триместр вагітності й до бажаних методів пологів [53].

Наслідки поширення таких даних виходять далеко за межі порушення приватності. Дослідження показують, що інформація про репродуктивний статус може бути використана роботодавцями, страховими компаніями та кредиторами, що збільшує ризики дискримінації, стигматизації або відмови в доступі до послуг. Особливо вразливими є особи з нетрадиційною статевою ідентичністю, жінки, які користуються технологіями допоміжної репродукції, або ті, хто має специфічні генетичні характеристики. У багатьох дослідженнях повідомлялося, що особи можуть бути дискриміновані у зв'язку з їхньою сексуальною ідентичністю чи репродуктивною поведінкою [54], а неправомірна доступність інформації щодо окремих стигматизованих груп може призводити до того, що особа набуває «досвід системного гноблення» [55].

Такі казуси дають змогу констатувати, що дані про репродуктивне здоров'я, які здебільшого вважаються інтимними та приватними, насправді широко збираються та регулярно поширюються операторами та брокерами даних. У багатьох випадках люди безпосередньо діляться інформацією про репродуктивне здоров'я, проте не надають дозволу на збір, обробку та посилення інформації. Крім того, особи не підозрюють, що такі дані можуть збиратися. Прикладами є: публікація посту чи фотографії в соціальних мережах про вагітність, приєднання до онлайн-групи підтримки для жінок, які зіткнулися з втратою вагітності, тощо. Ці публічні дії надають компаніям та, залежно від налаштувань конфіденційності користувача, широкий громадськості інформацію про репродуктивне здоров'я.

Науковці також констатують низький рівень знань громадськості про самостійне запобігання поширенню інформації, нівелюючи загрозу використання даних про їхнє репродуктивне здоров'я. Досліджуючи це питання, науковці [56, 57] констатують низький рівень розуміння проблеми – здебільшого користувачі додатків та інших цифрових інструментів навіть не підозрюють, що їхня приватна інформація доступна технологічним корпораціям та постачальникам медичних послуг у сфері репродуктивного здоров'я.

Ця проблема є актуальною і для України. За результатами проведених нами досліджень, мобільними додатками, пов'язаними зі здоров'ям, користується чимало жінок (78,1% від загальної популяції), з них 76% зазначили, що йдеться про додатки, пов'язані з репродукцією (стосуються менструації, фертильності, вагітності), 76% – з фітнесом або харчуванням, 68% – із загальними медичними аспектами (зокрема, рецептами, аналізами, вакцинацією, ліками). Отже, переважна більшість тих, хто використовує мобільні додатки, пов'язані зі здоров'ям, зацікавлені у відстежуванні своїх репродуктивних показників.

Особливо репрезентативним наш аналіз є в контексті порівняння безпеки конфіденційних даних у загальних медичних додатках та тих, що стосуються репродуктивного та

сексуального здоров'я. Отримані емпіричні дані дали можливість здійснити диференційований аналіз рівня недовіри та страху, пов'язаного із цифровою обробкою медичної інформації. З'ясувалося, що користувачі різних типів медичних застосунків демонструють різні рівні занепокоєння залежно від чутливості даних.

Користувачі лише загальних медичних додатків продемонстрували найнижчі середні показники страху (1,50–1,75). Натомість серед користувачів, які застосовують одночасно загальні та репродуктивні сервіси, спостерігався значно вищий рівень занепокоєння (2,08–2,58). Найвищий показник був серед тих, хто не використовує цифрових додатків взагалі (2,78–2,89). Остання група в типовий спосіб продемонструвала ефекти інформаційної асиметрії та страху перед невідомими технологічними процесами (рис. 1).

Отже, результати опитування підтверджують, що репродуктивні дані розглядаються респондентами як найбільш інтимні та соціально вразливі, що зумовлює суттєво вищий рівень страху через їхній можливий витік чи використання проти особи. Цей патерн відповідає глобальним трендам щодо зростання недовіри до цифрових сервісів, що обробляють інтимні або генетично релевантні дані. Тобто саме сфера репродукції / фертильності / менструального здоров'я сприймається як найчутливіша та найвразливіша.

Проведений тест χ^2 Пірсона показав, що між використанням репродуктивних цифрових додатків та рівнем занепокоєння щодо можливого витоку інтимних репродуктивних даних існує статистично значуща асоціація ($\chi^2 = 40,461$; $p < 0,001$). Це означає, що тип медичних застосунків, якими користується респондент, суттєво впливає на інтенсивність його побоювань щодо конфіденційності. Водночас порівняння показників користувачів додатків, пов'язаних із репродуктивними функціями, та тих, хто уникав використання додатків, пов'язаних із питаннями здоров'я взагалі, показало статистично більший рівень занепокоєності можливістю витоку інформації в представників другої групи, що може бути однією з причин відмови від подібних застосунків ($\chi^2 = 18,321$; $p < 0,001$).

Оскільки серед користувачів додатків із репродуктивного та сексуального здоров'я спостерігається істотно вищий рівень занепокоєння, ніж серед тих, хто застосовує лише загальні медичні сервіси, використання спеціалізованих додатків є значущим предиктором підвищеного страху витоку інтимних даних.

Отриманий результат підтверджує, що обробка даних, пов'язаних із репродуктивним здоров'ям, сприймається користувачами як особливо чутлива сфера, а тому спричиняє виражену тривожність та недовіру до цифрових систем. Це також узгоджується з міжнародними дослідженнями, які демонструють підвищений рівень вразливості й обережності користувачів у питанні безпеки саме репродуктивних даних.

Слід усвідомлювати, що поступово кількість користувачів незмінно буде збільшуватися, оскільки додатки є зручними та репрезентують дедалі більше технологічних можливостей для контролю сексуального та репродуктивного здоров'я користувачів. Тому проблема для України також буде актуалізуватися.

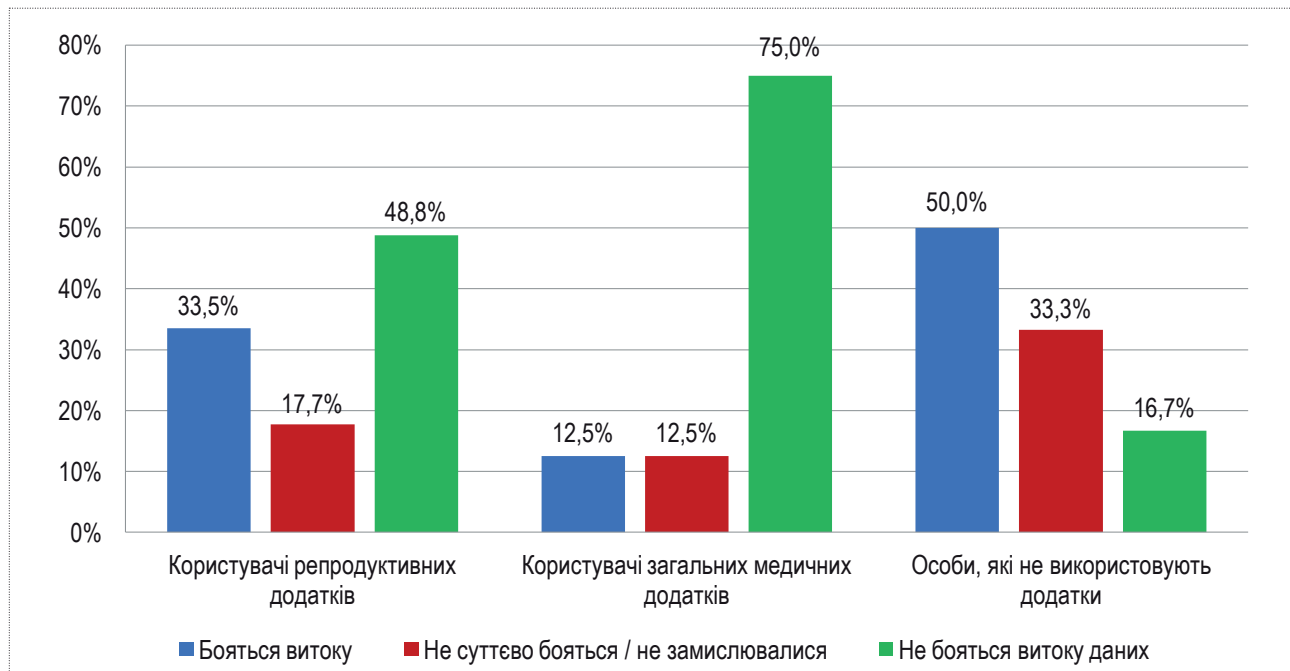


Рисунок 1. Результати статистичного спостереження за рівнем побоювання користувачів мобільних додатків щодо витоку даних

Водночас результати опитування свідчать про загальний низький рівень обізнаності щодо ризиків цифрового поширення медичних даних. Лише 3,1% респондентів повідомили, що добре ознайомлені з політикою конфіденційності й усвідомлюють можливі небезпеки її порушення. Натомість 56,2% опитаних мають лише часткове уявлення про потенційні загрози, а 40,7% – ніколи серйозно не замислювалися над цією проблемою. Це свідчить про системний дефіцит цифрової грамотності та обмеженість державної інформаційної політики щодо репродуктивних даних.

Наше дослідження субординується з висновками британських експертів, які зазначають, що користувачам бракує навичок для захисту своїх даних під час застосування FemTech, незважаючи на висловлені занепокоєння щодо конфіденційності, тому що більшість із них вважає, що це питання безпеки даних має бути вирішене на державному рівні [58]. Інше дослідження доводить, що 49% споживачів медичних репродуктивних додатків відчують себе нездатними захистити свої дані через брак знань або часу, а також складність пов'язаних із цим процесів [59].

Поведінковий вимір цієї проблеми також отримав емпіричне підтвердження. Для визначення зв'язку між рівнем занепокоєння щодо витоку репродуктивних даних та поведінковим рішенням відтермінувати медичний огляд (рис. 2) було застосовано ранговий коефіцієнт Спірмена. Аналіз виявив статистично значущу позитивну кореляцію ($p = 0,514$; $p = 0,0026$), що свідчить про таке: посилення страху витоку інтимної репродуктивної інформації суттєво збільшує ймовірність відтермінування візиту до лікаря. Отже, тривога, пов'язана з конфіденційністю даних, виступає вагомим поведінковим фактором, який негативно впливає на своєчасність отримання медичної допомоги.

Окремої уваги потребують ризики, пов'язані зі стрімким розвитком ШІ. Алгоритми ШІ здатні здійснювати прихова-

ний збір інформації, створювати цифрові профілі або прогнозувати репродуктивні стани на підставі побічних даних (shadow profiling). Корпорації, які володіють такими технологіями, фактично формують «інфраструктуру приватності», що виходить за межі державного контролю. Це породжує серйозні питання щодо прозорості, етичності та правомірності обробки даних, які стосуються найінтимніших аспектів життя людини. Користувачі ШІ стикаються з різноманітними загрозами інформаційній безпеці, зокрема більшість дослідників акцентують на загрозах, що несе ШІ через неетичність використання даних [60] цією технологічною системою.

Питання актуалізується з огляду на те, що розвиток ШІ в охороні здоров'я відбувається стрімкими темпами, і тому посилюється дискусія щодо управління його розвитком, оскільки багато технологій перебуває в приватній власності. В. Murdoch зазначає, що характер впровадження ШІ може означати, що корпорації, клініки та державні органи відіграватимуть суттєвішу, ніж зазвичай, роль в отриманні, використанні та захисті інформації про здоров'я пацієнтів [61]. Це породжує питання конфіденційності, пов'язані з впровадженням та безпекою даних під час використання технологій на базі ШІ.

Інформація про репродуктивне здоров'я є незворотною, і витік таких даних неможливо компенсувати шляхом «заміни» ідентифікатора, як це відбувається, наприклад, із втраченим паролем. Це означає, що цифрові інциденти у сфері репродуктивної медицини мають довготривалі та часто незворотні наслідки.

На нашу думку, правове регулювання проблеми, що породжена двома зазначеними вище обставинами, ускладнене через: новизну питання; відсутність суттєвих важелів державного впливу на власників цифрових додатків та платформ (значна частина наявних технологій перебуває у власності великих технологічних корпорацій, як-от «Google»,

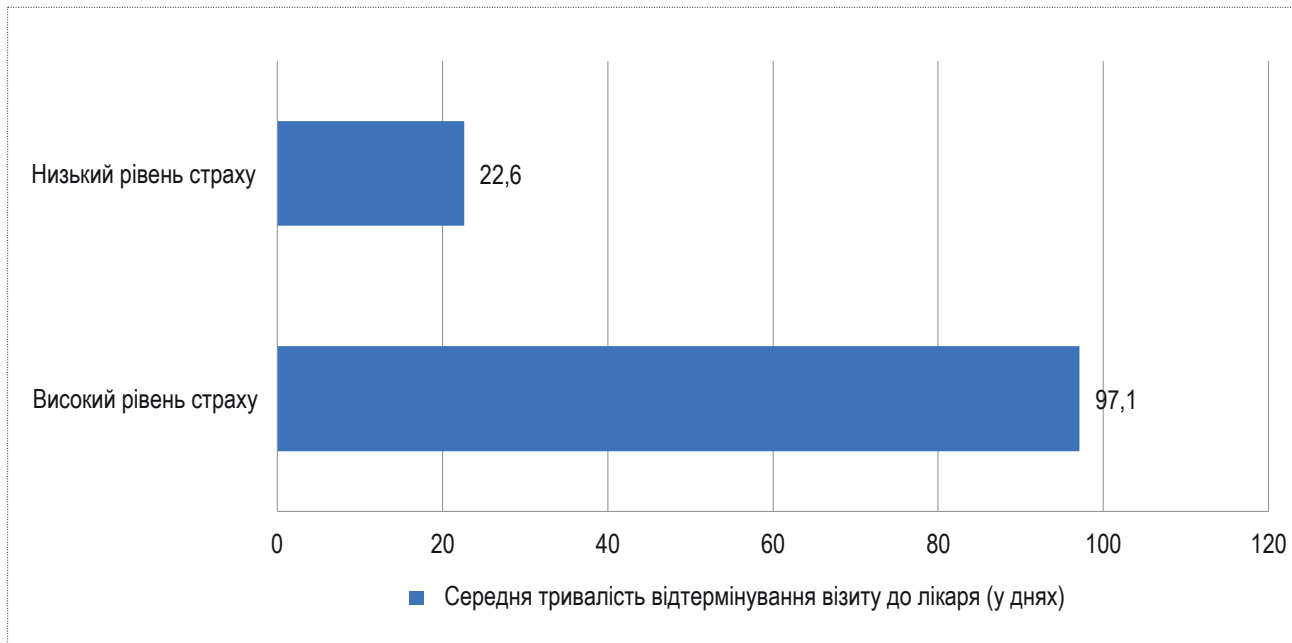


Рисунок 2. Статистичне спостереження за поведінковими рішеннями респондентів щодо відтермінування звернення за медичною допомогою через страх витоку репродуктивних даних

«Microsoft», «IBM», «Apple» та інших, причому компанії «по-своєму формують пропозиції щодо майбутнього охорони здоров'я та різних аспектів світової галузі охорони здоров'я в контексті користування медичною інформацією» [61]; відсутність стандартів міжнародного та європейського рівнів; швидкість техніко-технологічних змін та непрогнозованість розвитку цифрових можливостей у сфері забезпечення, охорони та захисту репродуктивного здоров'я. Тому для формування пропозицій щодо удосконалення чинної системи гарантування захисту репродуктивної інформації необхідно вивчити міжнародні стандарти в цій сфері та позитивний досвід держав щодо врегулювання проблеми.

Отже, технологічні загрози у сфері репродуктивних даних мають комплексний характер і виходять далеко за межі технічної кібербезпеки. Вони охоплюють комерційні, етичні, соціальні та юридичні ризики, що впливають на реалізацію репродуктивних прав, рівень довіри до медичних сервісів та доступ до охорони здоров'я. З огляду на високу чутливість цих відомостей та зростання популярності цифрових платформ, проблема захисту репродуктивних даних вимагає системного оновлення правового регулювання, впровадження технічних стандартів та розбудови культури обізнаного цифрового користування.

Регуляторне забезпечення захисту репродуктивних даних в умовах цифровізації: проблеми та напрями вдосконалення

Питання власності, контролю та належного управління біологічними матеріалами набуває нової гостроти в умовах прискореної цифровізації. Інтеграція репродуктивної медицини в національну екосистему електронної охорони здоров'я України є відносно новим процесом, що супроводжується як значними можливостями, так і серйозними

ризиками. ЕСОЗ, створена в межах стратегії «Цифрова держава» й координувана Міністерством охорони здоров'я та Міністерством цифрової трансформації, має забезпечити ефективну взаємодію між медичними закладами, лабораторіями та страховими організаціями. У межах цієї системи постачальників репродуктивних медичних послуг заохочують переходити від паперової документації до цифрових, стандартизованих і потенційно безпечних реєстрів.

Однак на відміну від Європейського Союзу в Україні досі бракує спеціалізованого вторинного законодавства, яке б регулювало цифрову обробку саме репродуктивних чи генетичних даних, що належать до категорії найбільш чутливих.

Цей нормативний розрив формує низку системних ризиків для конфіденційності, безпеки та прав пацієнтів:

1. Технічні та кібербезпекові ризики. Одним із головних ризиків є вразливість місцевих баз даних приватних клінік та центрів ЕКЗ, багато з яких покладаються на комерційне програмне забезпечення без сертифікованого шифрування або належних журналів аудиту. За даними, що відображають загальні тенденції кіберінцидентів у медичному секторі України, значна частина порушень медичних даних стосується несанкціонованого доступу до локальних медичних баз даних часто через слабкі протоколи автентифікації або використання незахищеного комерційного програмного забезпечення [62]. На відміну від компонентів ЕСОЗ, які проходять державну експертизу Державної служби спеціального зв'язку та захисту щодо відповідності вимогам технічного захисту інформації, комерційні медичні інформаційні системи, що використовуються в приватній репродуктивній медицині, не завжди мають таку сертифікацію, що робить такі дані легкою мішенню.

2. Транскордонна передача даних без належної правової основи. Це є критичним правовим ризиком, що виникає

через невідповідність української практики міжнародним стандартам. Як уже згадувалось вище, Конвенція Ради Європи 108+ вимагає, щоб передача даних забезпечувала адекватний рівень захисту в країні-отримувачі [63]. Деякі українські центри репродуктивної медицини співпрацюють з іноземними генетичними лабораторіями для проведення преімплантаційного генетичного тестування. Однак угоди про передачу даних рідко містять гарантії, що відповідають вимогам GDPR, як-от Стандартні договірні положення або інші належні гарантії. Це викликає питання щодо рівня захисту, що надається генетичній інформації під час експорту за межі ЄС / Європейського економічного співтовариства. Отже, якщо українські центри не використовують Стандартні договірні положення, вони порушують міжнародний принцип контролю місця призначення даних, ставлячи під загрозу конфіденційність генетичних даних пацієнтів. Особливо важливо, що Конвенція 108+ прямо вимагає надання «конкретних гарантії» для генетичних даних, зокрема суворих правил зберігання, обмежень передачі, посиленого контролю доступу. В Україні ж відсутність спеціалізованого вторинного законодавства не дає змоги забезпечити ці гарантії в повному обсязі.

3. Відсутність чіткої політики зберігання даних та проблема відкликання згоди. Принцип мінімізації зберігання є фундаментальним у сучасному захисті даних. Українські клініки часто зберігають репродуктивні дані протягом необмеженого часу. Це є прямим порушенням принципу мінімізації зберігання. Згідно зі ст. 5(1)(e) GDPR, дані повинні зберігатися лише стільки, скільки необхідно для їх обробки. Відсутність такого обмеження в українській медичній практиці збільшує ризик неправомірного використання даних та конфліктів щодо відкликання згоди пацієнта. Хоча Україна не імплементувала ст. 5(1)(e) GDPR, Керівні принципи Організації економічного співробітництва та розвитку щодо біобанків (2009) вимагають, щоб тривалість зберігання була пропорційною науковим цілям та передбачала механізми відкликання згоди [64]. Також невизначеність щодо механізмів відкликання згоди на використання ембріонів, гамет чи сурогатних послуг в електронних реєстрах може призвести до правових конфліктів. Керівні принципи Організації економічного співробітництва та розвитку щодо біобанків (2009) чітко визначають найкращі практики щодо тривалості зберігання та механізмів відкликання згоди, але їх застосування в українській ЕКОЗ для репродуктивних даних є несистематизованим.

4. Алгоритмічні ризики та профілювання на основі ШІ. Це найсучасніший етичний та регуляторний ризик, пов'язаний із технологічним прогресом у медицині. Новітні репродуктивні технології покладаються на ШІ для аналізу якості ембріонів або прогнозування результатів фертильності. Ці алгоритми часто використовують великі набори даних, що містять конфіденційні дані про здоров'я та генетичні параметри. Як показують дослідження M. Shabani та L. Marelli, навіть псевдонімізовані геномні дані можуть бути повторно ідентифіковані шляхом комбінованої обробки великих масивів інформації, що значно підвищує ризики для конфіденційності в цифрових системах репродуктивної медицини [65]. Без прозорого управління даними та стандартів

пояснювальності використання таких інструментів ШІ може призвести до дискримінаційних результатів або порушень конфіденційності. Закон ЄС про ШІ (AI Act), положення якого наберуть чинності у 2026 році, класифікуватиме такі медичні системи ШІ як «високоризикові», накладаючи суворі зобов'язання щодо якості даних та людського нагляду [66]. Українське законодавство поки не має аналогічних механізмів, що створює нормативну прогалину.

5. Етичні наслідки цифровізації для професійних відносин у репродуктивній медицині. Цифровізація в репродуктивній медицині трансформує не лише обробку даних, але й стосунки між лікарем і пацієнтом. Конфіденційність, яка колись забезпечувалася професійним обов'язком лікаря, тепер залежить від складних цифрових інфраструктур, що охоплюють багатьох посередників: постачальників хмарних послуг та програмного забезпечення, лабораторних партнерів. Тому, цифрові екосистеми децентралізують моральну відповідальність та розмивають межі лікарської таємниці. Тож правові механізми повинні еволюціонувати від індивідуальних професійних зобов'язань до системних рамок управління даними.

Отже, цифровізація репродуктивної медицини демонструє парадокс прогресу: що досконалішими стають технології, то більш крихкою виявляється конфіденційність даних. Поточні правові реформи в Україні, зокрема проєкт Закону «Про захист персональних даних», узгоджений із GDPR, є важливим кроком до модернізації, однак їх практична імплементація у сфері ЕКОЗ, генетичної медицини та електронних реєстрів залишається неповною. Забезпечення реального захисту репродуктивних даних вимагає комплексного перегляду політики, створення чітких технічних стандартів, посилення нагляду та формування культури свідомого цифрового користування, що бере до уваги чутливість цієї категорії медичної інформації.

ВИСНОВКИ

Цифровізація репродуктивної медицини створює нову онтологію приватності, у межах якої дані про фертильність, менструальний цикл, вагітність, ДРТ та генетичні характеристики стають частиною складної інформаційної екосистеми. Ця екосистема, з одного боку, відкриває можливості для підвищення якості медичної допомоги, персоналізованої діагностики та розширення доступу до медичних сервісів, а з іншого – генерує безпрецедентні юридичні, етичні та соціальні ризики. Репродуктивні дані мають подвійний характер, що визначає їхню максимальну чутливість і неспівмірність наслідків у разі цифрових порушень. Саме тому питання їхнього належного управління виходить за межі медичної та інформаційної безпеки й набуває цивілізаційно-гуманітарного значення.

Проведений аналіз виявив, що соціальні уявлення, культурні табу та політична поляризація безпосередньо впливають на довіру до цифрових репродуктивних сервісів. Репродуктивне здоров'я зберігає високий рівень приватності в суспільному дискурсі, а громадяни часто не володіють достатньою інформацією щодо можливостей і ризиків цифрової медицини. Низький рівень цифрової обізнаності та

фрагментарне розуміння політики конфіденційності сприяють поширенню страхів щодо неправомірного доступу до інтимних даних, що підтверджується емпіричними результатами: лише 3,1% респондентів проведеного нами опитування добре орієнтуються в ризиках, тоді як понад 40% ніколи серйозно не замислювалися над ними.

Емпірична частина дослідження продемонструвала статистично значущі зв'язки між використанням репродуктивних цифрових застосунків та рівнем занепокоєння можливістю витоку інтимних даних ($\chi^2 = 40,461$; $p < 0,001$). Зокрема, користувачі репродуктивних додатків виявляють значно вищий рівень недовіри до цифрової обробки інформації, ніж користувачі загальних медичних сервісів. Водночас особи, які повністю уникають будь-яких медичних застосунків, демонструють ще вищий рівень тривожності, що свідчить про страх невідомого та низький рівень цифрової компетентності. Важливим поведінковим наслідком виявлених закономірностей є те, що підвищений страх витоку репродуктивних даних статистично корелює з рішенням відтермінувати медичний огляд ($p = 0,514$; $p = 0,0026$). Це означає, що проблеми конфіденційності можуть перерости в бар'єри в доступі до медичної допомоги, що створює загрозу для здоров'я та безпеки пацієнтів.

Правовий аналіз засвідчив, що традиційні механізми захисту медичної таємниці, закріплені в Основах законодавства України про охорону здоров'я та Цивільному кодексі України, уже не відповідають складності сучасних цифрових процесів. У сфері репродуктивної медицини правовий режим конфіденційності охоплює не лише інформацію про стан здоров'я, але й генетичні, біометричні та донорські відомості, що створює багаторівневий простір вразливостей. В Україні досі бракує спеціалізованого вторинного законодавства щодо обробки репродуктивних даних, чітких правил транскордонної передачі, політики щодо строків зберігання даних, а також механізмів відкликання згоди відповідно до міжнародних стандартів (GDPR, Конвенція 108+, рекомендації Організації економічного співробітництва та розвитку щодо біобанків).

Цифрові загрози посилюються через низку системних чинників: від кібернедостатності приватних клінік та відсутності аудитів безпеки до використання алгоритмів ШІ, здатних до повторної ідентифікації генетичних профілів, тінювого профілювання та каптації персональних даних через комерційні модулі аналітики. Реальні скандали, пов'язані з використанням менструальних та фертильних додатків (як от додатки «Flo», «Premom», сторонні брокери даних), демонструють глобальність проблеми й потребують адаптації національної правової політики.

Узагальнюючи результати теоретичного та емпіричного аналізу, можна сформулювати такі ключові висновки:

1. Цифрова обробка репродуктивних даних створює унікальний комплекс ризиків, що виходять за межі класичного інституту медичної таємниці та вимагають міждисциплінарних рішень.
2. Соціальний контекст (табу, стигма, політична поляризація) суттєво впливає на довіру до цифрових сервісів і формує поведінкові патерни користувачів.

3. Низька цифрова грамотність та обмежені знання про конфіденційність ускладнюють можливість громадян самостійно захистити свої цифрові сліди.

4. Емпіричні дані підтверджують статистично значущу залежність між використанням репродуктивних додатків та побоюванням щодо витоку інтимної інформації.

5. Страх втрати конфіденційності впливає на медичну поведінку – сприяє відтермінуванню візитів до лікаря, що може погіршувати стан здоров'я.

Проведене дослідження демонструє, що цифровізація репродуктивної медицини формує новий тип правових і соціальних викликів, які не можуть бути вирішені виключно за допомогою інструментів традиційного медичного права.

Загалом результати дослідження дають змогу сформулювати три ключові напрями вдосконалення політики щодо захисту репродуктивних даних:

1. Нормативний рівень. Необхідно:
 - гармонізувати національне регулювання з GDPR із чітким обмеженням обробки чутливих даних;
 - визначити «репродуктивні дані» як окрему чутливу категорію;
 - установити спеціальні стандарти для комерційних медичних інформаційних систем;
 - унормувати механізми транскордонної передачі даних із застосуванням стандартних договірних положень;
 - визначити строки зберігання репродуктивних даних та механізми відкликання згоди;
 - запровадити регуляторні принципи використання ШІ в репродуктивній медицині.

2. Громадський та соціокультурний рівень. З огляду на виявлену гендерну асиметрію (загроза релевантна для 40% жінок і лише 20% чоловіків) та низьку обізнаність громадян, необхідно:

- підвищувати цифрову грамотність користувачів;
- забезпечувати прозорість політики конфіденційності;
- формувати культуру поваги до приватності репродуктивної інформації;
- розвивати інституції громадського нагляду й незалежного аудитування цифрових сервісів mHealth.

3. Технічний рівень. Сучасні виклики вимагають технічних рішень, здатних мінімізувати ризики втручання, профілювання та витоку:

- запровадження блокчейн-рішень для захищеного обміну;
- застосування генераторів випадкових ключів та методів перетину приватних множин;
- обов'язкове шифрування та журналювання доступу;
- незалежний аудит кіберзахищеності медичних інформаційних систем;
- прозорість алгоритмів ШІ та застосування механізмів людського нагляду.

Отже, захист конфіденційності репродуктивних даних в умовах цифровізації є міждисциплінарною проблемою, що поєднує право, етику, медицину, технології та соціальний контекст. З огляду на високу чутливість таких даних та їхню здатність впливати на приватне життя, здоров'я, автономію і навіть юридичний статус особи, Україна потребує комплексної модернізації політики конфіденційності. Лише по-

єднання нормативних змін, суспільної обізнаності та технологічної безпеки дасть змогу забезпечити реальний захист репродуктивних прав людини та сприяти довірі до цифрової медицини.

З огляду на визначені ризики, очевидно є необхідність впровадження підходу багаторівневого гарантування: нормативного, технічного, етичного та організаційного. У цьому контексті пропонується застосовувати Policy Brief «Захист репродуктивних та генетичних даних в умовах цифровізації», який є дієвим практичним інструментом внутрішнього регулювання для клінік ДРТ, що дає змогу запровадити високі стандарти кібербезпеки, управління даними, прозорості та підзвітності.

Запропоновані рекомендації доцільно впроваджувати в діяльність клінік допоміжних репродуктивних технологій через затвердження у формі внутрішнього наказу керівника закладу охорони здоров'я, оскільки вони охоплюють прогресивні стандарти захисту репродуктивних та генетичних даних і випереджають чинне законодавство, проте відповідають міжнародним вимогам і забезпечують належний рівень безпеки цифрових медичних систем (додаток).

Конфлікт інтересів

Автори заявляють про відсутність конфлікту інтересів.

Додаток

POLICY BRIEF ЗАХИСТ РЕПРОДУКТИВНИХ ТА ГЕНЕТИЧНИХ ДАНИХ В УМОВАХ ЦИФРОВІЗАЦІЇ (ДЛЯ КЛІНІК ДРТ)

1. ПРОБЛЕМА

Клініки допоміжних репродуктивних технологій (ДРТ) обробляють найчутливіші види даних: інформацію про фертильність, безпліддя, використання ДРТ, донорство гамет та ембріонів, результати генетичних тестів, дані про сурогатне материнство. Це водночас медичні та генетичні дані, пов'язані не лише з пацієнтом, а й із донорами, реципієнтами та потенційними нащадками.

ЄС кваліфікує такі дані в ст. 9 GDPR як «спеціальні категорії персональних даних» (health та genetic data), а їх обробка дозволена лише за дотримання суворих умов і посиленних гарантій безпеки.

Модернізована Конвенція 108+ Ради Європи окремо виділяє дані про здоров'я, генетичні та біометричні дані як такі, що потребують «відповідних гарантій, закріплених законодавством».

Для клініки ДРТ це означає: звичайного «медичного» рівня захисту недостатньо – потрібна спеціальна політика управління ризиками, кібербезпекою та доступом до даних.

2. МЕТА ВНУТРІШНЬОЇ ПОЛІТИКИ

Забезпечити відповідність клініки ДРТ міжнародним стандартам (GDPR / Конвенція 108+, ISO/IEC 27001).

Гарантувати пацієнтам захист репродуктивних і генетичних даних на рівні, що мінімізує ризики витоку, дискримінації та стигматизації.

Побудувати прозору систему відповідальності та аудиту всередині клініки.

3. КЛЮЧОВА НОРМАТИВНА РАМКА

GDPR, ст. 9, ст. 32 – спеціальні категорії даних; вимога «відповідних технічних і організаційних заходів», включно із шифруванням та псевдонімізацією, управлінням доступом, регулярним тестуванням безпеки.

Конвенція 108+ (2018), ст. 6 – посилений захист генетичних та медичних даних, зокрема щодо зберігання, передачі та трансграничного обігу.

ISO/IEC 27001:2013/2022 – міжнародний стандарт системи управління інформаційною безпекою (ISMS), який описує вимоги до політик, контролю доступу, журналів, управління ризиками, тощо.

OECD Guidelines on Human Biobanks and Genetic Research Databases (2009) – рекомендації щодо зберігання, строків, інформованої згоди та відкликання згоди в контексті генетичних даних.

4. РЕКОМЕНДАЦІЇ ДЛЯ ВНУТРІШНЬОЇ ПОЛІТИКИ КЛІНІКИ ДРТ

4.1. Управління та відповідальність

Що прописати в політиці:

Призначити Відповідального за захист даних (Data Protection Officer (DPO)) або аналогічну роль – вимога GDPR для організацій, які системно обробляють чутливі дані.

Затвердити Реєстр операцій із даними (які категорії даних, для яких цілей, хто має доступ, де зберігаються).

Встановити процедуру оцінки впливу на захист даних (Data Protection Impact Assessment (DPIA)) для всіх нових IT-систем, генетичних реєстрів або проєктів із використанням ШІ.

Чому це важливо:

Без формалізації ролі DPO та реєстру обробок клініка фактично не контролює, де і як «розповзаються» репродуктивні й генетичні дані.

DPIA – інструмент, прямо рекомендований GDPR для обробки високоризикових даних, зокрема в охороні здоров'я.

4.2. Класифікація та мінімізація даних

Що прописати:

Запровадити окрему категорію «репродуктивні та генетичні дані» (фертильність, діагноз безпліддя, дані про ДРТ, статус донора / реципієнта, генетичні тести, ембріони, кріо-банк тощо).

Для цієї категорії встановити:

- чітко визначені цілі обробки (ст. 5(1)(b) GDPR – purpose limitation);
- принцип мінімізації – збираємо лише те, що дійсно потрібно для лікування / правових обов'язків;
- строки зберігання – фіксовані (наприклад, N років після завершення лікування або закінчення договору), з подальшою анонімізацією або знищенням.

Чому це важливо:

Необмежене зберігання даних суперечить принципу мінімізації, який є базовим у GDPR та рекомендаціях OECD щодо біобанків.

4.3. Системна кібербезпека

Що має бути обов'язково:

Шифрування даних (AES-256 або еквівалент): у спокої (на серверах, у базах, на ноутбуках / носіях) і під час передачі (TLS/HTTPS, VPN). GDPR прямо називає шифрування та псевдонімізацію рекомендованими технічними заходами безпеки (ст. 32).

Двофакторна автентифікація (2FA): для доступу до медичної інформаційної системи (МІС), хмарних сервісів, панелей адміністрування. Це відповідає принципу «рівень безпеки, адекватний ризику», закріпленому в ст. 32 GDPR.

Аудит доступів та журнали (логи): кожен доступ до репродуктивних / генетичних даних має логуватися: хто, коли, до яких записів звертався, що змінював.

Журнали логів зберігати не менше 3–5 років (мінімум – строк давності типових претензій / скарг). Це дає змогу виконати вимоги щодо «здатності забезпечити конфіденційність, цілісність, доступність та стійкість» системи та забезпечує доказову базу в разі інцидентів.

Вимоги до хмарних провайдерів: використовувати лише хмари, які мають сертифікацію ISO/IEC 27001 (і, бажано, ISO/IEC 27701 для приватності) або еквівалентні стандарти.

У договорах – окремий розділ про обробку персональних даних, географію зберігання (країна / центр обробки даних), транскордонну передачу та процедуру повідомлення про інциденти.

Чому це важливо:

Згідно з аналізами кіберінцидентів у медичній сфері, найбільша частка витоків пов'язана саме зі слабким контролем доступу та відсутністю журналів аудиту, а не з «хакерськими атаками» у вузькому розумінні.

4.4. Захист внутрішніх медичних інформаційних систем (пояснення до блоку 4)

Внутрішня МІС клініки ДРТ повинна:

Мати сертифікат технічного захисту інформації (ТЗІ) або ISO/IEC 27001.

Для України – сертифікація Державної служби спеціального зв'язку та захисту інформації України (ТЗІ) для систем, де обробляються медичні дані.

Альтернатива / доповнення – відповідність ISO/IEC 27001 як загальноновизнаному міжнародному стандарту ISMS (Information Security Management System).

Підтримувати шифрування на рівні бази даних і резервних копій. Якщо МІС не шифрує дані «за замовчуванням», це суперечить принципам security by design, закріпленим у GDPR.

Мати функцію псевдонімізації даних: наприклад, усі дослідження / звітність / аналітика щодо ембріонів мають виконуватися на базі ідентифікаторів (коди пацієнтів, донорів, ембріонів), а не ПІБ. Псевдонімізація прямо згадується в ст. 32 GDPR як рекомендований захід безпеки.

Мати контроль доступу за ролями (RBAC): гінеколог бачить одні поля, ембріолог – інші, адміністратор – лише службову інформацію без медичних деталей, бухгалтер – тільки фінансові дані. Принцип «мінімально необхідних прав» є базовим як у GDPR, так і в ISO/IEC 27001.

Чому це важливо:

У нинішніх реаліях значна частина приватних МІС не відповідає цим вимогам (немає шифрування, логів, ролей доступу). Для клініки ДРТ це створює неприйнятний ризик, оскільки витік інформації про донорів, сурогатних матерів чи ембріони матиме набагато тяжчі наслідки, ніж витік «звичайних» медичних даних.

4.5. ШІ та аналітичні платформи

Що потрібно:

Внутрішня політика має забороняти завантаження репродуктивних / генетичних даних у публічні або неконтрольовані ШІ-сервіси.

Для алгоритмів, які використовуються для відбору ембріонів, прогнозування успіху ДРТ тощо, слід:

- проводити DPIA;
- документувати джерела даних;
- вимагати від постачальника опису логіки роботи та заходів безпеки.

Чому це важливо:

Європейський AI Act відносить медичні ШІ-системи до високоризикових і вимагає посиленого контролю даних та людського нагляду.

4.6. Пацієнти, інформована згода та обізнаність

Що закріпити:

Окрема форма інформованої згоди на обробку репродуктивних і генетичних даних, де чітко пояснюються:

- які дані збираються;
- для яких цілей;
- кому й куди можуть передаватися (зокрема, за кордон);
- строки зберігання;
- право на відкликання згоди та наслідки цього.

Регулярне інформування пацієнтів (буклети, сайт, плакати) про правила конфіденційності й права у сфері репродуктивних даних.

Чому це важливо:

Це безпосередньо впливає із загальних принципів GDPR (прозорість, інформованість, право на відкликання згоди) та міжнародних біоетичних стандартів щодо генетичних досліджень.

5. ОЧІКУВАНИЙ ЕФЕКТ

Впровадження описаних заходів дозволить клініці ДРТ:

- зменшити ризик витоків репродуктивних та генетичних даних і пов'язаних позовів / репутаційних втрат;
- підвищити довіру пацієнтів та донорів, що є критично важливим у сфері ДРТ;
- наблизити практику клініки до європейських стандартів права охорони здоров'я та захисту даних;
- бути готовою до майбутньої гармонізації українського законодавства з GDPR та Конвенцією 108+.

ЛІТЕРАТУРА/REFERENCES

- Малій Б.
Цивільно-правовий режим охорони права на лікарську таємницю [Інтернет]. Теорія і практика інтелектуальної власності. 2025; 2: 31–7.
Доступно: <https://essuir.sumdu.edu.ua>.
Maliy B.
Civil law regime of protection of the right to medical secrecy [Internet]. Theory and practice of intellectual property. 2025; 2: 31–7. Available from: <https://essuir.sumdu.edu.ua>.
- Ярославський СЮ.
Суб'єкти інформаційних правовідносин в медичній сфері України. Юридичний науковий електронний журнал—електронне наукове фахове видання. 2025; 5: 370–4.
Yaroslavsky S.
Yu. Subjects of information legal relations in the medical sphere of Ukraine. Legal scientific electronic journal—electronic scientific professional journal. 2025; 5: 370–374.
DOI: 10.32782/2524-0374/2025-5/83.
- Hendrata WM, Karim A.
Legal Protection of Patients' Confidentiality in the Era of Mandatory Electronic Medical Records. Widya Pranata Hukum: Jurnal Kajian dan Penelitian Hukum. 2025; 7(2): 236–57.
DOI: 10.37631/widya pranata.v7i2.1723.
- Балинская ОМ, Теремецкий ВИ, Жаровская И та ін.
Право пациента на конфиденциальность в сфере здравоохранения [Интернет]. Georgian Medical News. 2021;12 (321):147–53. Доступно: https://www.geomednews.com/Articles/2021/12_2021/V321_N12_December_2021.pdf.
Balynskaya OM, Teremetskiy VI, Zharovskaya I, et al. The patient's right to confidentiality in the field of health care [Internet]. Georgian Medical News. 2021;12 (321):147–53. Available from: https://www.geomednews.com/Articles/2021/12_2021/V321_N12_December_2021.pdf.
- Діордіца ІВ, Коваленко ІА, Коваль ОМ.
Правова охорона персональних даних у сфері охорони здоров'я в Україні. Науковий вісник Ужгородського Національного Університету. Серія: Право. 2024; 82(2): 141–6.
Djorditsa IV, Kovalenko IA, Koval OM.
Legal protection of personal data in the sphere of health care in Ukraine. Scientific Bulletin of Uzhhorod National University. Series: Law. 2024; 82(2): 141–6.
DOI: 10.24144/2307-3322.2024.82.2.22.
- Блашук ТВ, Придатко ДО.
Забезпечення конфіденційності медичної інформації при обробці даних пацієнта в процесі функціонування Електронної системи охорони здоров'я. Юридичний науковий електронний журнал. 2024; 5: 661–4.
Blaschuk TV, Prydatko DO.
Ensuring the confidentiality of medical information when processing patient data in the process of functioning of the Electronic Health Care System. Legal Scientific Electronic Journal. 2024; 5: 661–4.
DOI: 10.32782/2524-0374/2024-5/165.
- Блашук ТВ, Придатко ДО.
Особливості доступу до медичної інформації правоохоронних органів, адвокатів та суду. Держава та регіони. Серія «Право». 2024;2(1): 59–65.
Blaschuk TV, Prydatko DO.
Peculiarities of access to medical information of law enforcement agencies, lawyers and the court. State and regions. Series "Law". 2024;2(1): 59–65.
DOI: 10.32782/1813-338X-2024.1.2.10.
- Jawad LA.
Security and privacy in digital healthcare systems: challenges and mitigation strategies. Abhigyan. 2024; 42(1): 23–31.
DOI: 10.1177/09702385241233073.
- Chukwunweike JN, Yussuf M, Okusi O, et al.
The role of deep learning in ensuring privacy integrity and security: Applications in AI-driven cybersecurity solutions. World Journal of Advanced Research and Reviews. 2024; 23(2), 2550.
DOI: 10.30574/wjar.2024.23.2.2550.
- Herzog NJ, Celik D, Sulaiman RB.
Artificial intelligence in healthcare and medical records security. In Cybersecurity and Artificial Intelligence: Transformational Strategies and Disruptive Innovation. 2024: 35–57. Cham: Springer Nature Switzerland.
DOI: 10.53889/citj.v2i2.555.
- Buchan MC, Bhawra J, Katapally TR.
Navigating the digital world: development of an evidence-based digital literacy program and assessment tool for youth. Smart Learning Environments. 2024;11(1), 8.
DOI: 10.1186/s40561-024-00293-x.
- Sindikis S, Showkat G.
The digital revolution in India: bridging the gap in rural technology adoption. Journal of Innovation and Entrepreneurship. 2024;13(1), 29.
DOI: 10.1186/s13731-024-00380-w.
- Nowrozzy R, Ahmed K, Kayes ASM, et al.
Privacy preservation of electronic health records in the modern era: A systematic survey. ACM Computing Surveys. 2024; 56(8): 1–37.
DOI: 10.1145/3653297.
- El-Saleh AA, Sheikh AM, Albroom, et al.
The internet of medical things (IoMT): opportunities and challenges. Wireless networks. 2025;31(1): 327–44.
DOI: 10.1007/s11276-024-03764-8.
- Filley E.
Data Privacy at the Border: How to Balance National Security Concerns and Privacy Interests When Conducting Forensic Border Searches of Electronic Devices [Internet]. Wash. & Lee J. Civ. Rts. & Soc. Just. 2025; 31: 203. Available from: <https://scholarlycommons.law.wlu.edu/crsj/vol31/iss2/6/>.
- Pring R.
Confidentiality and the right to know. In The politics and ethics of evaluation Routledge. 2024: 8–18.
- Asmitha M, Rajgopal SM.
Exploring unique techniques to preserve confidentiality and authentication. [Internet]. 2024 2nd International Conference on Intelligent Data Communication Technologies and Internet of Things (IDCIoT). 2024: 440–447. Available from: <https://www.proceedings.com/content/073/073892webtoc.pdf>.
- Chung RJ, Lee JB, Hackell JM, Alderman EM.
Confidentiality in the care of adolescents: Technical report. Pediatrics. 2024; 153(5), e204066327.
DOI: 10.1542/peds.2024-066327.
- Gbagbo FY, Ameyaw EK, Yaya S.
Artificial intelligence and sexual reproductive health and rights: a technological leap towards achieving sustainable development goal target 3.7. Reproductive Health. 2024; 21(1), 196.
DOI: 10.1186/s12978-024-01924-9.
- Tohit NFM, Haque M.
Leveraging technology to transform sexual and reproductive health services. Bangladesh Journal of Medical Science. 2024; 23(4): 896–906.
DOI: 10.3329/bjms.v23i4.76502.
- Hossain MM, Kashem MA, Nayan NM, et al.
Medical Cyber-physical system for predicting maternal health in developing countries using machine learning. Healthcare Analytics. 2024; 5, 100285.
DOI: 10.1016/j.health.2023.100285.
- Gottlieb SL, Spielman E, Abu-Raddad L, et al.
WHO global research priorities for sexually transmitted infections. The Lancet Global Health. 2024; 12(9), e1544–e1551.
DOI: 10.1016/S2214-109X(24)00266-3.
- Agbeyangi AO, Lukose JM.
Telemedicine adoption and prospects in sub-Saharan Africa: a systematic review with a focus on South Africa, Kenya, and Nigeria. In Healthcare. 2025;13(7):762
DOI: 10.3390/healthcare13070762.
- Søndergaard MLJ, Ciolfi Felice M, Balaam M.
Designing menstrual technologies with adolescents. Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems. 2021; 1–14.
DOI: 10.1145/3411764.3445480.
- Alfawzan N, Christen M, Spitale G, et al.
Privacy, data sharing, and data security policies of women's mHealth apps: scoping review and content analysis. JMIR mHealth and uHealth. 2022;10, 5: e33735.
DOI: 10.2196/33735.
- Amelang K.
(Not) Safe to Use: Insecurities in Everyday Data Practices with Period-Tracking Apps. In New Perspectives in Critical Data Studies: The Ambivalences of Data Power. Springer. 2022:297–321.
DOI: 10.1007/978-3-030-96180-0_13.
- Alhammad N, Alajlani M, Abd-alrazaq A, et al.
Patients' Perspectives on the Data Confidentiality, Privacy, and Security of mHealth Apps: Systematic Review. J Med Internet Res. 2024;26:e50715.
DOI: 10.2196/50715.
- Darebo T, Spigt M, Teklewold B, et al.
The sexual and reproductive healthcare challenges when dealing with female migrants and refugees in low and middle-income countries (a qualitative evidence synthesis). BMC Public Health. 2024;24,520.
DOI: 10.1186/s12889-024-17916-0.
- Cao J, Laabadi H, Mathis CH.
«I Deleted It After the Overturn of Roe v. Wade»: Understanding Women's Privacy Concerns Toward Period-Tracking Apps in the Post Roe v. Wade Era. In Proceedings of the 2024 CHI Conference on Human Factors in Computing Systems. 2024:1–22.
DOI: 10.1145/3613904.3642042.
- Cross J.
Reproductive Justice for All: The Way Forward with Empowerment. Social Work in Public Health. 2025:1–10.
DOI: 10.1080/19371918.2025.2568059.
- Olebara OP.
A contradiction between the illegality of abortion under the Nigerian laws and the reproductive health rights of women in Nigeria: An analysis [Internet]. Alex Ekwueme Federal University Law Journal. 2025; 2. Available from: <https://nigerianjournalonline.org/index.php/AEFLJ/article/view/1666>.

32. Latifnejad Roudsari R. Navigating a Path to Integrity: Ethical Dilemmas of Artificial Intelligence in Publishing Midwifery and Reproductive Health Research. *Journal of Midwifery and Reproductive Health*. 2025;13(4):4978–80. DOI: 10.22038/jmrh.2025.91636.2793.
33. Office of United Nations High Commissioner for Human Rights (OHCHR). Sexual and reproductive health and rights. [Internet]. Available from: <https://www.ohchr.org/en/women/sexual-and-reproductive-health-and-rights>.
34. European Union. General Data Protection Regulation (EU) 2016/679 [Internet]. Official Journal of the European Union, L119, 1–88. Available from: <https://gdpr-text.com/>.
35. Україна, Про захист персональних даних: Закон України № 2297 станом на 12.02.2025 р. [Інтернет]. Доступно: <https://zakon.rada.gov.ua/laws/show/2297-17#Text>. Ukraine, On the Protection of Personal Data: Law of Ukraine No. 2297 as of 12 February 2025 [Internet]. Available from: <https://zakon.rada.gov.ua/laws/show/2297-17#Text>.
36. Україна, Основи законодавства України про охорону здоров'я № 2801-XII станом на 18.06.2019 р. [Інтернет]. Доступно: <https://zakon.rada.gov.ua/laws/show/2801-12#Text>. Ukraine, Fundamentals of the Legislation of Ukraine on Health Care No. 2801-XII [Internet]. Available from: <https://zakon.rada.gov.ua/laws/show/2801-12#Text>.
37. Україна, Цивільний кодекс України: Закон України № 435-IV станом на 21.08.2025 р. [Інтернет]. Доступно: <https://zakon.rada.gov.ua/laws/show/435-15#Text>. Ukraine, Civil Code of Ukraine: Law of Ukraine No. 435-IV as of 21 August 2025 [Internet]. Available from: <https://zakon.rada.gov.ua/laws/show/435-15#Text>.
38. Європейська Конвенція про захист прав людини і основоположних свобод: документ Ради Європи від 4 листопада 1950 року. [Інтернет]. Доступно: https://zakon.rada.gov.ua/laws/show/995_004#Text. European Convention for the Protection of Human Rights and Fundamental Freedoms: Council of Europe document of 4 November 1950 [Internet]. Available from: https://zakon.rada.gov.ua/laws/show/995_004#Text.
39. European Court of Human Rights. Case of Z v. Finland, no. 22009/93, Judgment of 25 February 1997. Strasbourg: ECHR [Internet]. Available from: https://hudoc.echr.coe.int/eng#_ftn1.
40. European Court of Human Rights. Case of I v. Finland, no. 20511/03, Judgment of 17 July 2008 [Internet]. Available from: <https://hudoc.echr.coe.int/eng#%7B%22itemid%22%3A%22001-87510%22%7D>.
41. European Court of Human Rights. Case of L.L. v. France, no. 7508/02, Judgment of 10 October 2006 [Internet]. Available from: <https://hudoc.echr.coe.int/eng#%7B%22itemid%22%3A%22001-77356%22%7D>.
42. Council of Europe. Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (CETS No. 223) [Internet]. 2018 Available from: <https://www.coe.int/en/web/data-protection/convention108-and-protocol>.
43. Україна, Про допоміжні репродуктивні технології: Проект Закону № 13683 від 22.08.2025 р. [Інтернет]. Доступно: https://itd.rada.gov.ua/billinfo/Bills/Card/57179?utm_source=On%20Assisted%20reproductive%20technologies%3ADraft%20Law%20No.%2013683%20of%2022%20August%202025. On Assisted reproductive technologies: Draft Law No. 13683 of 22 August 2025 [Internet]. Available from: https://itd.rada.gov.ua/billinfo/Bills/Card/57179?utm_source=On%20Assisted%20reproductive%20technologies%3ADraft%20Law%20No.%2013683%20of%2022%20August%202025.
44. Isaacs N, Ntinga X, Keetsi T. Are mHealth Interventions Effective in Improving the Uptake of Sexual and Reproductive Health Services among Adolescents? A Scoping Review. *International Journal of Environmental Research and Public Health*. 2024;21(2),165. DOI: 10.3390/ijerph21020165.
45. Ziller A, Mueller TT, Stieger S, et al. Reconciling privacy and accuracy in AI for medical imaging. *Nat Mach Intell*. 2024; 6: 764–74. DOI: 10.1038/s42256-024-00858-y.
46. Ninsima LR, Chiumia IK, Ndejo R. Factors influencing access to and utilisation of youth-friendly sexual and reproductive health services in sub-Saharan Africa: a systematic review. *Reprod Health*. 2021;18,135. DOI: 10.1186/s12978-021-01183-y.
47. Huq AZ, Wexler R. Digital Privacy for Reproductive Choice in the Post-Roe Era [Internet]. *New York University Law Review*. 2023;98:555–602. Available from: <https://ssrn.com/abstract=4191990>.
48. The Organisation for the Review of Care and Health Apps. Data Privacy Matters. Period. ORCHA. [Internet]. Report on the Data Security of Period Tracking Apps, 2022. Available from: <https://info.orchahhealth.com/data-security-period-tracking-apps>.
49. Statista. 2022. Leading period tracker and female health apps worldwide in April 2022, by downloads. [Internet]. Available from: <https://www.statista.com/statistics/1307702/top-period-tracker-apps-worldwide-by-downloads/>.
50. Federal Trade Commission. Ovulation Tracking App Premom Will be Barred from Sharing Health Data for Advertising Under Proposed FTC Order [Internet]. 2023. Available from: <https://www.ftc.gov/news-events/news/press-releases/2023/05/ovulation-tracking-app-premom-will-be-barred-sharing-health-data-advertising-under-proposed-ftc>.
51. Alsebayel G, Troiano GM, Gunawan J et al. “An Ad Posing as Medical Advice”: User Accounts of Dark UX in FemTech mHealth Apps. *Proceedings of the ACM on Human-Computer Interaction*. 2025; 9(5):1–34. DOI: 10.1145/3743736.
52. Cahn AF, Manis E. Pregnancy Panopticon: Abortion Surveillance After Roe [Internet]. 2022. Surveillance Technology Oversight Project (S.T.O.P.). Available from: https://static1.squarespace.com/static/5c1bfc7eee175995a4ceb638/t/6297d83433c19479f037ab8c/1654118453441/2022.6.1_.
53. Data brokers resist pressure to stop collecting info on pregnant people. 2023. Available from: <https://perma.cc/FNL4-A6DZ>.
54. Saadat M, Keramat A, Jahanfar S, et al. Barriers and facilitators to accessing sexual and reproductive health services among transgender people: a meta-synthesis. *International journal of social determinants of health and health services*. 2024; 54(1): 40–51. DOI: 10.1177/27551938231187863.
55. Heward-Belle S, Gifti S, Lovell, R. Analysing the scientific literature on transgender and gender diverse persons' experiences with sexual and reproductive health care services from an intersectional perspective. *Int J Equity Health*. 2025;24,12. DOI: 10.1186/s12939-024-02328-8.
56. Amelang K. (Not) Safe to Use: Insecurities in Everyday Data Practices with Period-Tracking Apps. In *New Perspectives in Critical Data Studies: The Ambivalences of Data Power*. Springer. 2022:297–321. DOI: 10.1007/978-3-030-96180-0_13.
57. Hohmann-Marriott B. Periods as powerful data: User understandings of menstrual app data and information. *New Media & Society*. 2021;14614448211040245. DOI: 10.1177/14614448211040245.
58. Mehrmehdaz M, Almeida T. «My sex-related data is more sensitive than my financial data and I want the same level of security and privacy»: User Risk Perceptions and Protective Actions in Female-oriented Technologies. 2023. DOI: arXiv preprint arXiv:2306.05956.
59. Quach S, Thaichon P, Martin KD, et al. Digital technologies: tensions in privacy and data. *J. of the Acad. Mark. Sci*. 2022;50:1299–323. DOI: 10.1007/s11747-022-00845-y.
60. Huang L. Ethics of Artificial Intelligence in Education: Student Privacy and Data Protection. *Science Insights Education Frontiers*, 2023;16(2):2577–87. DOI: 10.15354/sief.23.re202.
61. Murdoch, B. Privacy and artificial intelligence: challenges for protecting health information in a new era. *BMC Med Ethics*. 2021;22,122 DOI: 10.1186/s12910-021-00687-3.
62. Річний аналітичний огляд [про кібербезпеку] [Інтернет]. Рада національної безпеки та оборони України. 2025. Доступно: https://www.rnbo.gov.ua/files/2024/NATIONAL_CYBER_SCC/20250109. Annual Analytical Review [on Cybersecurity] [Internet]. National Security and Defense Council of Ukraine. 2025 Available from: https://www.rnbo.gov.ua/files/2024/NATIONAL_CYBER_SCC/20250109.
63. Convention for the protection of individuals with regard to the processing of personal data (CETS No. 223) / Council of Europe [Internet]. Strasbourg, 2018. Available from: <https://mbkaya.com/it-law-coe-convention-108-plus/>.
64. OECD Guidelines on Human Biobanks and Genetic Research Databases, Organization for Economic Co-operation and Development [Internet]. Paris, 2009. Available from: <https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0375>.
65. Shabani M, Marelli L. Re-identifiability of genomic data and the GDPR: Assessing the re-identifiability of genomic data in light of the General Data Protection Regulation [Internet]. *EMBO Rep* 2019;20(6):e48316, Available from: <https://www.embopress.org/doi/full/10.15252/embr.201948316>.
66. 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 (Artificial Intelligence Act). [Internet]. Available from: <https://eur-lex.europa.eu/eli/reg/2024/1689/oj>.

КОНФІДЕНЦІЙНІСТЬ ІНФОРМАЦІЇ ПРО РЕПРОДУКТИВНЕ ЗДОРОВ'Я ЛЮДИНИ: ЦИФРОВІ ВИКЛИКИ ТА ПРОБЛЕМИ ПРАВОВОГО РЕГУЛЮВАННЯ

A.I. Суббот, д. ю. н., професор, завідувач кафедри публічного та європейського права ПЗВО «Київський міжнародний університет», м. Київ

K.O. Калаченкова, к. ю. н., доцентка кафедри господарського та адміністративного права Донецького національного університету ім. Василя Стуса, м. Вінниця

V.V. Берч, д. ю. н., доцентка, професорка кафедри конституційного права та порівняльного правознавства Ужгородського національного університету, м. Ужгород

A.V. Басалаєва, PhD, доцентка кафедри конституційного права Київського національного університету ім. Тараса Шевченка, м. Київ

B.P. Ратушна, к. ю. н., доцентка кафедри права Львівського національного університету ветеринарної медицини та біотехнологій ім. Степана Гжицького, м. Львів

V.I. Продан, PhD, старша викладачка кафедри конституційного права та порівняльного правознавства юридичного факультету ДВНЗ «Ужгородський національний університет», м. Ужгород

Обґрунтування. Цифровізація (диджиталізація) охорони здоров'я, зростання ринку мобільних застосунків та інтегрованих платформ mHealth, а також активне застосування штучного інтелекту створюють нову реальність для збирання та обробки репродуктивних даних, які належать до найчутливіших категорій медичної інформації. Витік або неналежне використання таких відомостей підривають приватність, порушують медичну таємницю, створюють ризики дискримінації та стигматизації і безпосередньо впливають на реалізацію репродуктивних прав. В українських умовах ці виклики ускладнюються фрагментарністю правового регулювання, недостатнім рівнем правової політики у сфері цифрової медицини та низькою обізнаністю щодо репродуктивних прав серед громадян.

Мета дослідження: міждисциплінарний аналіз екзистенційних викликів цифровізації у сфері конфіденційності інформації про репродуктивне здоров'я людини.

Матеріали та методи. Методологічна основа охоплює діалектичний, етико-нормативний, феноменологічний і міжкультурний підходи із застосуванням порівняльно-правового, статистичного та догматичного методів. Емпірична частина ґрунтується на результатах онлайн-опитування (n = 643), спрямованого на визначення рівня довіри населення до захисту конфіденційної інформації у сфері репродуктивного здоров'я. Нормативний аналіз охоплював дослідження Загального регламенту про захист даних Європейського Союзу (General Data Protection Regulation (GDPR), Конвенції 108+, українського законодавства та міжнародних рекомендацій.

Результати. Аналіз засвідчив, що саме репродуктивні дані сприймаються як найбільш ризиковані щодо цифрової обробки. Респонденти, які користуються цифровими сервісами для моніторингу фертильності чи менструального циклу, демонстрували підвищений рівень страху щодо витоку конфіденційної інформації. Виявлено статистично значущі зв'язки між занепокоєнням і поведінковими рішеннями, зокрема схильністю відтермінувати медичні консультації. Ідентифіковано такі ключові виклики: комерційне профілювання, недобросовісні практики збору даних, алгоритмічна дискримінація, повторна ідентифікація генетичних даних, вразливість інформаційних систем та недостатня інтегрованість національного регулювання з GDPR і Конвенцією 108+. Виявлено прогалини в українській системі правового регулювання, зокрема відсутність окремої категоризації репродуктивних даних, слабкість технічних стандартів захисту та неврегульованість транскордонної передачі.

Висновки. Результати проведеної роботи підтверджують необхідність формування нової комплексної правової політики, орієнтованої на підвищення рівня захисту приватності та медичної таємниці в умовах цифровізації. Ключові кроки передбачають: визначення репродуктивних даних як окремої категорії; гармонізацію національного регулювання з GDPR та Конвенцією 108+; впровадження технічних стандартів безпеки для платформ mHealth; правову регламентацію використання штучного інтелекту у сфері репродуктивної медицини; розбудову механізмів інформованої згоди; підвищення рівня обізнаності у сфері репродуктивних прав.

Ключові слова: репродуктивне здоров'я, репродуктивні дані, штучний інтелект, цифровізація, диджиталізація, приватність, конфіденційна інформація, медична таємниця, правова політика, правове регулювання.

PRIVACY OF HUMAN REPRODUCTIVE HEALTH INFORMATION: DIGITAL CHALLENGES AND REGULATORY ISSUES

A.I. Subbot, doctor of juridical sciences, professor, head of the Department of Public and European Law, Kyiv International University, Kyiv

K.O. Kalachenkova, candidate of juridical sciences, associate professor, Department of Economic and Administrative Law, Vasyl' Stus Donetsk National University, Vinnytsia

V.V. Berch, doctor of juridical sciences, associate professor, professor of the Department of Constitutional Law and Comparative Law, Uzhhorod National University, Uzhhorod

A.V. Basalaya, PhD, lecturer of Constitutional Law Department, Taras Shevchenko National University of Kyiv, Kyiv

B.P. Ratushna, candidate of juridical sciences, associate professor, Department of Law, Stepan Gzhyskyi National University of Veterinary Medicine and Biotechnologies of Lviv, Lviv

V.I. Prodan, PhD, senior lecturer, Department of Constitutional Law and Comparative Jurisprudence, Faculty of Law, Uzhhorod National University, Uzhhorod

Background. The digitalization of healthcare, the rapid expansion of mobile applications and integrated mHealth platforms, as well as the increasing use of artificial intelligence, are reshaping the ways reproductive data are collected, processed, and shared. These data belong to the most sensitive categories of medical information, and their leakage or improper use undermines privacy, violates medical secrecy, creates risks of discrimination and stigmatization, and directly affects the realization of reproductive rights. In the Ukrainian context, these challenges are intensified by fragmented legal regulation, insufficient development of public policy in digital health, and a generally low level of awareness in the field of reproductive rights.

Objective of the study: to conduct an interdisciplinary analysis of the existential challenges posed by digitalization for the confidentiality of information related to human reproductive health.

Materials and methods. The methodological framework combines dialectical, ethical-normative, phenomenological and complementary approaches with comparative-legal, statistical, and doctrinal methods. The empirical component is based on an online survey (n = 643) assessing public trust in mechanisms protecting confidential information in the field of reproductive health. The regulatory analysis covered the General Data Protection Regulation (GDPR), Convention 108+, Ukrainian legislation, and international standards.

Results. The findings indicate that reproductive data are perceived as the most vulnerable to risks associated with digital processing. Users of digital services for fertility or menstrual cycle tracking demonstrated significantly higher levels of concern regarding potential data breaches. Statistically significant associations were revealed between anxiety related to data leakage and behavioral decisions, particularly the tendency to postpone medical consultations. Key challenges were identified, including commercial profiling, unfair data collection practices, algorithmic discrimination, re-identification of genetic data, system vulnerabilities, and insufficient alignment of national regulation with GDPR and Convention 108+. The study also revealed gaps in Ukrainian health law, such as the absence of a distinct category of reproductive data, inadequate technical security standards, and unregulated cross-border data transfers.

Conclusions. The results confirm the need to develop an integrated legal policy aimed at strengthening privacy and medical secrecy in the context of digitalization. Priority steps include: defining reproductive data as a separate protected category; harmonizing national regulation with GDPR and Convention 108+; implementing unified technical security standards for mHealth platforms; creating a legal framework for the use of artificial intelligence in reproductive medicine; reinforcing mechanisms of informed consent; and improving public awareness of reproductive rights.

Keywords: reproductive health, reproductive data, artificial intelligence, digitalization, privacy, confidential information, medical secrecy, legal policy, legal regulation.