Правові аспекти інформаційної безпеки у телемедицині в Україні

Legal Aspects of Information Security in Telemedicine in Ukraine

Гжегож Павловські [1], Ольга Барабаш [2], Мирослав Ковалів [2], Мар'яна Хмиз [3], Ірина Мисюк [3], Аліна Грищук [2]

Grzegorz Pawlowski, Olha Barabash, Myroslav Kovaliv, Mariana Khmyz, Iryna Mysiuk, Alina Hryshchuk

[1] *Zaklad Handlowo-Uslugowy BHP*
17 Kostrzynska Street, Gorzyca, 69-113, Poland

[2] *Lviv State University of Internal Affairs*
26 Horodotska Street, Lviv, 79007, Ukraine

[3] *Ivan Franko National University of Lviv*
1 Universytetska Street, Lviv, 79000, Ukraine

DOI: 10.22178/pos.87-2

JEL Classification: K30

Received 10.10.2022
Accepted 20.11.2022
Published online 30.11.2022

Corresponding Author:
Myroslav Kovaliv
mkovaliv1@ukr.net

Анотація. У статті з позиції сучасної теорії інформаційного права, на основі чинного українського законодавства та нормативно-правових актів Європейського Союзу, розглянуто правові аспекти інформаційної безпеки у телемедицині в Україні. Актуальність теми зумовлена необхідністю удосконалення законодавства України з метою комплексного теоретичного обґрунтування підвищення ефективності забезпечення інформаційної безпеки. У ході дослідження застосовано методологію системного комплексного аналізу правових явищ із застосуванням факторного та еволюційного методів дослідження. Зазначено, сучасні інформаційні технології дозволяють лікарям надавати дистанційну медичну допомогу, здійснювати постійний моніторинг стану здоров'я пацієнтів. У період пандемії COVID-19 зросла потреба у наданні віддаленої медичної допомоги. Вказано, що телемедичні технології використовуються для проведення досліджень та виявлення захворювань на основі автоматизованої обробки великих масивів персональних і медичних даних. В умовах цифровізації медицини зростає значення інформаційної безпеки пацієнтів та інших суб'єктів телемедичної діяльності. Обробка великих обсягів персональних даних про здоров'я пацієнтів в інформаційних системах підвищує ризики порушення недоторканності приватного життя та потребує більш високих стандартів захисту інформації.

Ключові слова: інформаційні системи; інформаційно-комунікаційні технології; медицина; медичні пристрої; персональні дані; кіберзагрози; Україна.

Abstract. In the article, the legal aspects of information security in telemedicine in Ukraine are considered from the modern theory of information law based on current Ukrainian legislation and regulations of the European Union. The topic's relevance is due to the need to improve the legislation of Ukraine to provide a comprehensive theoretical justification for enhancing the effectiveness of information security. In the course of the study, the methodology of the systematic, comprehensive analysis of legal phenomena using factor and evolutionary research methods was applied. It is noted that modern information technologies allow doctors to provide remote medical care to monitor patients' health constantly. During the COVID-19 pandemic, the need for remote medical care has increased. It is indicated that telemedicine technologies are used to conduct research and detect diseases based on the automated processing of large amounts of personal and medical data. In the digitalization of medicine, the importance of information security of patients and other subjects of telemedicine activities is growing. The processing of large amounts of personal data on patients' health in information systems increases the risks of privacy violations and requires higher standards of information protection.

Keywords: information systems; information and communication technologies; medicine; medical devices; personal data; cyber threats; Ukraine.

ВСТУП

Впровадження інформаційних технологій в медицину впливає на управління системою охорони здоров'я, трансформує ринок медичних послуг, залучає до економіки охорони здоров'я нових учасників економічних відносин – власників телемедичних платформ, операторів зв'язку, операторів хмарних сервісів, виробників телемедичних пристроїв, розробників програмного забезпечення. Дані процеси трансформації суспільних відносин у медицині вимагають адекватних механізмів правового регулювання, що закріплюють правовий статус суб'єктів правовідносин у сфері застосування інформаційних технологій в медицину (телемедицині), захищають права пацієнтів та публічні інтереси у сфері охорони здоров'я.

Важливе значення для розробки проблеми мали праці вчених-правознавців і практиків: В. Б. Авер'янова, О. О. Баранова, О. І. Берлача, Н. П. Бортник, Ю. П. Битяка, І. С. Гриценко, П. В. Діхтієвського, С. С. Єсімова, Р. А. Калюжного, Т. О. Коломоєць, В. К. Колпакова, О. В. Кузьменко, В. І. Курила, Є. В. Курінного, Р. С. Мельника, В. Я. Настюка, Н. М. Оніщенка, О. І. Остапенка, О. О. Селіванова, Р. М. Скриньковського, О. І. Харитонової, Я. М. Шевченка та інших.

Розвиток інформаційних технологій та поява нових технологій у охороні здоров'я потребує вивчення правовідносин, що виникають у цій сфері.

Отже, з огляду на викладене вище, *метою статті* є вивчення особливостей правовідносин у сфері інформаційної безпеки у телемедицині в Україні.

РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ

Стаття 3 Закону України «Основи законодавства України про охорону здоров'я» визначає поняття «телемедицина» як комплекс дій, технологій та заходів, що застосовуються під час надання медичної допомоги [1, с. 723]. Незважаючи на широкий спектр правових питань, пов'язаних із здійсненням телемедичної діяльності, найбільша кількість досліджень та наукових дискусій у галузі телемедицини та електронної охорони здоров'я сконцентрована на питаннях інформаційної безпеки (захист персональних даних, забезпечення безпеки інформаційних систем охорони здоров'я, організація електронного документообігу в медицині тощо).

Така увага до інформаційної безпеки в телемедицині пояснюється причинами етико-правового характеру. Ігнорування проблем інформаційної безпеки перекреслює всі переваги телемедичних технологій, оскільки від ступеня забезпечення інформаційної безпеки залежить довіра громадян до нових технологій, їхня готовність передати надзвичайно важливу сферу свого життя в «руки» комп'ютерів, мереж зв'язку, інформаційних систем та алгоритмів.

Від інформаційної безпеки телемедицини у результаті залежить фізична безпека пацієнтів. Тільки високі стандарти захисту інформації, розумний баланс між публічними та приватними інтересами в інформаційній сфері здатні легітимувати використання нових технологій в охороні здоров'я.

Інші правові аспекти телемедичної діяльності тим чи іншим чином пов'язані з питаннями інформаційної безпеки та опосередковано виконують функцію забезпечення інформаційної безпеки.

Ліцензійні вимоги до телемедичної діяльності повинні охоплювати: вимоги до інформаційної безпеки медичних виробів (пристроїв та програмного забезпечення), до кваліфікації працівників у сфері поводження з телемедичними технологіями; встановлення належного контакту з пацієнтом та ознайомлення з історією хвороби пацієнта, яке здійснюється через процедури ідентифікації та автентифікації; питання відповідальності, які включають відповідальність за неналежну експлуатацію інформаційних систем, незаконне опрацювання персональних даних, розголошення лікарської таємниці, а також інші правопорушення в інформаційній сфері, які можуть спричинити негативні наслідки для пацієнтів; страхування, яке може передбачати покриття ризиків інформаційної безпеки під час надання телемедичних послуг.

Міждисциплінарна природа означених питань характеризує інформаційну безпеку не як приватну, другорядну чи факультативну проблему, а як загальну та невід'ємну частину процесу переходу від традиційної охорони здоров'я до телемедичної та електронної охорони здоров'я.

Доктрина інформаційної безпеки України визначає інформаційну безпеку як стан захищеності особистості, суспільства та держави від внутрішніх та зовнішніх інформаційних загроз, при якому забезпечуються реалізація конституційних прав і свобод людини та громадянина, гідна якість та рівень життя громадян, суверенітет, територіальна цілісність, оборона та безпека держави [2].

Назване визначення є похідним від визначення національної безпеки, що охоплює питання забезпечення інформаційної безпеки в масштабах держави. У Стратегіях національної та інформаційної безпеки України наголошується на створенні умов для реалізації прав і свобод, сталого соціально-економічного розвитку [3; 4]. Такий позитивний підхід до розуміння безпеки є прогресивним та відповідає потребам суспільства. У такій парадигмі розвиток телемедицини може бути віднесений до напрямів забезпечення інформаційної безпеки в економічній сфері, у сфері суспільної безпеки, науки та технологій. Захист від зовнішніх та внутрішніх загроз не повинен недооцінюватися при забезпеченні інформаційної безпеки.

Як зазначають дослідники питань правового забезпечення інформаційної безпеки, світоглядна парадигма, де перевага надається терміну «захищеність», не втрачає значущості з урахуванням появи нових ризиків та загроз.

Стан захищеності не є статичним, а вимагає постійного вдосконалення у зв'язку з новими викликами та погрозами, що виникають у динамічний інформаційний вік, їх транскордонністю, надзвичайно швидким розвитком, трансформацією, коли інформаційні технології стрімко розвиваються та приносять суспільству не тільки благо, а й безліч проблем, а також використовуються у злочинних цілях. Телемедицина є однією з найбільш схильних до кіберзагроз сфер.

Статистика демонструє стрімке зростання кількості кібератак на інформаційні системи охорони здоров'я у всьому світі, а загальна шкода від інцидентів для галузі вимірюється мільярдами доларів США. Основними методами атак на медичні установи є зараження шкідливим програмним забезпеченням та злом облікових записів співробітників.

В Україні відзначається зростання кількості внутрішніх витоків медичних даних з вини співробітників медичних організацій, що підтверджує актуальність протидії не лише зовнішнім, а й внутрішнім загрозам безпеці.

У зарубіжній доктрині та закордонних правових актах поширений підхід до розуміння інформаційної безпеки, за якого інформаційна безпека охоплює питання захисту інформації та інформаційних систем від кіберзагроз.

У цьому контексті забезпечення інформаційної безпеки передбачає захист інформаційних систем від несанкціонованого доступу, спотворення, модифікації, знищення інформації.

Наприклад, у правових документах Європейського Союзу до інформаційної безпеки відносять безпеку мереж та інформаційних систем, що означає здатність протидіяти будь-якій дії, яка наражає на небезпеку доступність, автентичність, цілісність або конфіденційність інформації, що зберігається, передається або обробляється. У українському законодавстві дана діяльність охоплюється поняттям «захист інформації», що розкривається у Законі України «Про захист інформації в інформаційно-комунікаційних системах» [5].

Окремі вимоги щодо захисту інформаційних систем містяться у законодавстві України про безпеку критичної інформаційної інфраструктури. У національній доктрині інформаційного права України наголошується, що відносини щодо забезпечення інформаційної безпеки недоцільно зводити лише до правовідносин із захисту інформації [6].

Особливістю даного підходу до інформаційної безпеки є комплексне охоплення всіх питань, пов'язаних з інформаційними правовідносинами охоронного та регулятивного характеру. У такому значенні до інформаційної безпеки належать відносини суб'єктів інформаційно-правової діяльності щодо: формування та розвитку інформаційної інфраструктури; реалізації права на інформацію; захисту особистості, суспільства, держави від недоброякісної, хибної інформації та дезінформації; захисту інформації, зокрема персональних даних, в інформаційних системах; захисту прав споживачів та розвитку конкуренції в інформаційній сфері; реалізації відповідальності за правопорушення в інформаційній сфері; стандартизації як засобу забезпечення сумісності у комунікаційних мережах [7, 8, 9, 10, 11].

Таке визначення інформаційної безпеки є виправданим у контексті вибудовування державної політики в інформаційній сфері, як це реалізовано у Доктрині інформаційної безпеки України.

Такий підхід ототожнює правове забезпечення інформаційної безпеки з інформаційним правом та не дозволяє відокремити специфічний предмет правового регулювання. З метою дослідження правових аспектів інформаційної безпеки доцільно провести внутрішнє розмежування питань інформаційної безпеки групи питань, мають загальне цільове призначення.

Методологічно правові аспекти інформаційної безпеки можна поділити на дві групи. Перші покликані забезпечувати інформаційну взаємодію (оборот даних) з метою реалізації прав і законних інтересів суб'єктів права. Друга група питань стосується протидії кіберзагроз. Якщо раніше основними питаннями інформаційної безпеки були питання протидії кіберзагрозам, то в умовах розвитку цифрової економіки важливими є питання забезпечення інформаційної взаємодії, обороту даних.

Оборот даних є необхідною умовою для сталого соціально-економічного розвитку в інформаційному суспільстві. У правовій доктрині Європейського Союзу питання правового забезпечення інформаційної взаємодії та обороту даних охоплюються поняттям інтероперабельності.

Стосовно медицини правові аспекти кібербезпеки включають питання правового забезпечення безпеки критичної інформаційної інфраструктури у сфері охорони здоров'я, вимоги до захисту інформаційних систем охорони здоров'я, питання відповідальності за правопорушення у сфері використання інформаційних систем охорони здоров'я.

Дані питання не мають вираженої специфіки у сфері електронної охорони здоров'я, які істотно відрізняли б підходи до забезпечення кібербезпеки телемедицини від інших областей. Правові аспекти обігу даних включають питання правового режиму інформації, що використовується в телемедицині, та правового забезпечення електронного документообігу в телемедицині. Правовий режим інформації встановлює юридичні властивості інформації. Інші правові засоби забезпечення інформаційної безпеки встановлюють правові умови, у яких реалізується правовий режим інформації.

Електронний документообіг у телемедичній установі становить інфраструктурну базу інформаційного обміну, без якого неможлива телемедична діяльність. Ключові аспекти правового забезпечення інформаційної безпеки електронного документообігу в телемедичній галузі включають правові основи створення електронних записів про здоров'я пацієнтів, організації інформаційних систем охорони здоров'я та їх взаємодії, вимоги до ідентифікації та автентифікації суб'єктів [12, с. 119].

Для забезпечення інформаційної безпеки важливо гарантувати безпеку медичного обладнання, пристроїв та програмного забезпечення, що використовуються для передачі інформації між суб'єктами телемедичної діяльності та її обробки.

Особливо це питання набуває актуальності у зв'язку з розвитком «Інтернету речей» у медицині (включаючи пристрої, що імплантуються в організм людини, що формують «Інтернет людей»), архітектура якого вимагає додаткових рішень у сфері інформаційної безпеки. Подібний підхід характерний для Національної економічної стратегії на період до 2030 року [13].

У телемедицині велике значення мають вимоги, які пред'являються до виробників телемедичних пристроїв та розробників програмного забезпечення. На прикладі даних суб'єктів найбільш чітко простежується необхідність у визнанні дуалізму правовідносин у сфері телемедицини про розмежування правовідносин у сфері професійної медичної діяльності та правовідносин, не пов'язаних з професійною медичною діяльністю.

Традиційно виробники медичних пристроїв підпадають під сферу спеціального регулювання у сфері безпеки медичних інформаційних технологій та систем (далі – медичних пристроїв). У Європейському Союзі безпека медичних пристроїв та додатків підпадає не тільки під регулювання універсальної Директиви про загальну безпеку продуктів, а й спеціального законодавства, включаючи Директиву про медичні вироби [14].

В Україні передбачено процедуру реєстрації медичних пристроїв, у тому числі програмно-

го забезпечення, що включає експертизу якості, безпеки та ефективності. Якщо пристрій або програмний додаток не підпадає під законодавче визначення медичного пристрою, то на нього поширюється загальне регулювання безпеки продуктів та законодавство про захист прав споживачів. У правовій літературі країн Європейського Союзу наголошується на необхідності диференціації медичних пристроїв та програмних додатків, що використовуються в телемедичній медицині, на спеціалізовані та загального використання (гаджети, девайси та додатки для підтримки здорового способу життя, що вимірюють пульс, тиск, фізичну активність).

Відповідно, диференціації повинні піддатися вимоги, які пред'являються до виробників пристроїв та розробників програмних додатків у телемедичній медицині. Одним із критеріїв такої диференціації може бути обумовлена виробником мета використання пристроїв та додатків. Якщо пристрій/додаток призначений для використання в терапевтичних, діагностичних, клінічних та інших медичних професійних цілях, він підпадає під режим медичних пристроїв.

Якщо виріб, наприклад, дозволяє здійснювати моніторинг фізіологічних параметрів, але не призначений для спеціалізованого використання, під спеціальний режим медичних пристроїв він не підпадає. Для введення в цивільний обіг не потрібно проходити встановлені для медичних пристроїв дозвільні процедури. Неякісні пристрої та програми загального використання можуть заподіяти шкоду здоров'ю людини, спотворюючи інформацію про параметри здоров'я людини. Доцільно запровадити спеціальні вимоги щодо забезпечення безпеки таких медичних виробів, включивши до Плану заходів з реалізації угоди про асоціацію відповідну Директиву Європейського Союзу [15].

Одним із правових засобів встановлення таких вимог може бути прийняття технічного регламенту безпеки пристроїв і додатків загального користування для моніторингу фізіологічних параметрів.

Умовою введення таких пристроїв та програмного забезпечення у цивільний обіг має бути обов'язок виробника та продавця з інформування споживача про цілі використання пристрою/додатка, обмеження використання, можливі похибки у вимірі фізіологічних параметрів. Принципи забезпечення безпеки та конфіденційності повинні враховуватись при розробці стандартів, технічних регламентів, підготовці технічних завдань на розробку пристроїв.

Основну частину медичної інформації, що обробляється у процесі здійснення телемедичної діяльності, становлять персональні дані пацієнтів. Ця категорія інформації є найбільш чутливою та вразливою перед загрозами інформаційній безпеці.

Інформація про стан здоров'я пацієнтів є найбільш цінною інформацією, в обробці якої зацікавлені багато суб'єктів.

Існуючі гарантії права на недоторканність приватного життя, правовий режим персональних даних та правовий режим лікарської таємниці певною мірою виступають обмежувачами для впровадження інформаційних технологій у медицину, яка потребує більш вільного інформаційного обміну.

Дистанційний моніторинг стану здоров'я, забезпечення повсюдного доступу до електронних медичних карт пацієнтів, проведення медичних досліджень з використанням електронних записів про здоров'я пацієнтів потребують гнучкого підходу до правового регулювання відносин у сфері медичних даних. Зміна технології ставить питання щодо пошуку іншого балансу між правом на доступ до інформації та правом на недоторканність приватного життя у сфері охорони здоров'я. Найбільш гостро проблема співвідношення публічних інтересів у сфері охорони здоров'я та недоторканності приватного життя постала під час пандемії COVID-19.

Активне вторгнення у приватне життя громадян з метою забезпечення охорони громадського здоров'я порушило питання про можливе усунення балансу приватних та публічних інтересів у сфері персональних даних.

Чинне законодавство про персональні дані виявилося недостатньо підготовленим до надзвичайних обставин, подібних до пандемії COVID-19, внаслідок чого заходи, що вживаються урядами в терміновому порядку, виходили за рамки встановленого правового режиму, нерідко носили неконтрольований характер і викликали занепокоєння громадян за збереження кордонів приватного життя не тільки під час пандемії, а й після неї. Вразли-

вою виявилася та система безпеки даних, що збиралася, мала місце витоку інформація щодо пацієнтів з COVID-19.

Зміни правового режиму персональних даних про стан здоров'я повинні здійснюватися в рамках конституційних засад: будь-які обмеження прав і свобод повинні обґрунтовуватися необхідністю захисту цінностей, що охороняються конституцією, бути справедливими, адекватними, пропорційними і не порушувати права і свободи, що обмежуються.

ВИСНОВКИ

1. У системі правового забезпечення телемедицини інформаційна безпека є важливим елементом, оскільки у сучасних умовах, коли інформаційні технології проникають у життя людини, від інформаційної безпеки безпосередньо залежить його фізична безпека, реальна захищеність прав і законних інтересів. Усі інші правові питання телемедицини включають аспекти інформаційної безпеки.

2. З урахуванням розуміння інформаційної безпеки в правовій доктрині з метою дослідження правового забезпечення інформаційної безпеки в медичній галузі запропоновано розмежувати коло питань, пов'язаних з обігом інформації між суб'єктами правовідносин та питання протидії кіберзагрозам в Україні.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ / REFERENCES

1. Katynska, L. (2022). Poniattia telemedytsyny v zakonodavstvi Ukrainy [The concept of telemedicine in the legislation of Ukraine]. In *Yevropeiskyi vybir Ukrainy, rozvytok nauky ta natsionalna bezpeka v realiiakh masshtabnoi viiskovoi ahresii ta hlobalnykh vyklykiv XXI stolittia* (pp. 722–725). Retrieved from http://dspace.onua.edu.ua/handle/11300/19771 (in Ukrainian).
2. Doktryna informatsiinoi bezpeky Ukrainy [Information Security Doctrine of Ukraine] (Ukraine), 25.02.2017, No 47/2017. Retrieved September 01, 2022, from https://zakon.rada.gov.ua/laws/show/47/2017#Text (in Ukrainian).
3. Stratehiia natsionalnoi bezpeky Ukrainy [National security strategy of Ukraine] (Ukraine), 14.09.2020, No 392/2020. Retrieved September 01, 2022, from https://www.president.gov.ua/documents/3922020-35037 (in Ukrainian).
4. Stratehiia informatsiinoi bezpeky [Information security strategy] (Ukraine), 28.12.2021, No 685/2021. Retrieved September 01, 2022, from https://zakon.rada.gov.ua/laws/show/685/2021#Text (in Ukrainian).
5. Pro zakhyst informatsii v komunikatsiinykh systemakh [On the protection of information in communication systems] (Ukraine), 05.07.1994, No 80/94-BP. Retrieved September 01, 2022, from https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80#Text (in Ukrainian).
6. Malashko, O., & Yesimov, S. (2017). Content of state activities to ensure information security. *Internauka, 15*. doi: 10.25313/2520-2057-2020-15-6341
7. Skrynkovskyy, R., & Malashko, O. (2020). Structural and classification characteristics of providing information security. *Internauka. Series: "Juridical Sciences," 7*(29). doi: 10.25313/2520-2308-2020-7-6200
8. Sopilnyk, L., Skrynkovskyy, R., Malashko, O., & Sopilnyk, R. (2017). Features of providing information security: the experience of individual countries of Eastern Europe. *Internauka, 12*. doi: 10.25313/2520-2057-2020-12-6226
9. Malashko, O. (2017). Priority areas for improving information security in Ukraine. *Internauka. Series: "Juridical Sciences," 6*(28). doi: 10.25313/2520-2308-2020-6-6163
10. Sopilnyk, L., Skrynkovskyy, R., Vikonskyi, V., Kovaliv, M., Zayats, R., Yesimov, S., & Malashko, O. (2020). Features of Legal Support of Information Security in the Use of Cloud Technologies by Public Authorities. *Path of Science, 6*(6), 5006–5013. doi: 10.22178/pos.59-6

11. Skrynkovskyy, R., Sopilnyk, R., Malashko, O., Vikonskyi, V., Kovaliv, M., Protsiuk, T., Yesimov, S., & Zayats, R. (2020). Principles of Legal Regulation of the Use of Cloud Technologies for Personal Data Processing. *Path of Science, 6*(7), 2022–2029. doi: 10.22178/pos.60-9

12. Kovaliv, M., Yesimov, S., & Yarema, O. (2022). *Informatsiine pravo Ukrainy* [Information law of Ukraine]. Lviv: Lvivskyi derzhavnyi universytet vnutrishnikh sprav (in Ukrainian).

13. Pro zatverdzhennia Natsionalnoi ekonomichnoi stratehii na period do 2030 roku [On approval of the National Economic Strategy for the period until 2030] (Ukraine), 03.03.2021, No 179. Retrieved September 01, 2022, from https://zakon.rada.gov.ua/laws/show/179-2021-%D0%BF#Text (in Ukrainian).

14. Concerning measures for a high common level of security of network and information systems across the Union (EU), 06.07.2016, No 2016/1148. Retrieved September 01, 2022, from https://eur-lex.europa.eu/eli/dir/2016/1148/oj

15. Pro vykonannia Uhody pro asotsiatsiiu mizh Ukrainoiu, z odniiei storony, ta Yevropeiskym Soiuzom, Yevropeiskym spivtovarystvom z atomnoi enerhii i yikhnimy derzhavamy-chlenamy, z inshoi storony [On the implementation of the Association Agreement between Ukraine, of the one part, and the European Union, the European Atomic Energy Community and their Member States, of the other part] (Ukraine), 25.10.2017, No 1106. Retrieved September 01, 2022, from https://zakon.rada.gov.ua/laws/show/1106-2017-%D0%BF#Text (in Ukrainian).