DOI https://doi.org/10.36059/978-966-397-315-9-41

РОЗГОЛОШЕННЯ ПЕРСОНАЛЬНИХ ДАНИХ ЯК СКЛАДОВА ОБ'ЄКТИВНОЇ ТА СУБ'ЄКТИВНОЇ СТОРІН ЗЛОЧИНУ В МЕДИЧНІЙ ГАЛУЗІ

Карпушина Марія Григорівна
orcid.org/0000-0003-4125-4202
аспірантка Академії адвокатури України (м. Київ),
спеціаліст сектору юридичного забезпечення
Регіонального сервісного центру ГСЦ Міністерства внутрішніх справ України в Дніпропетровській області (м. Дніпро)
Науковий керівник: **Вереша Роман Вікторович**
orcid.org/0000-0003-4996-0283
доктор юридичних наук, завідувач кафедри кримінального та адміністративного права
Академії адвокатури України (м. Київ)

Міжособистісна комунікація є вкрай важливою для медичної справи. Створення соціального контакту на комунікативному рівні між пацієнтами та лікарями, іншими відвідувачами та медичним персоналом сприяє уникненню конфліктних ситуацій. Зрозуміло, що самі по собі конфліктні ситуації не створюють складу кримінально караних діянь та не суть в собі ознак проступків. Проте, загострення конфліктних ситуацій може провокувати подальші дії, які спроможні нести в собі ознаки шкідливих та протиправних діянь, за настання яких можуть наступати певні види відповідальності: цивільна (матеріальна, моральна), адміністративна, кримінальна, трудова (дисциплінарнау відношенні медичного персоналу).

Так, сучасною міжнародною та вітчизняною нормативною базою урегульовано дотримання прав пацієнта в правовому сенсі. Наразі існують положення основної міжнародної угоди, які регламентують охорону і захист прав пацієнта у системі відносин «лікар-пацієнт» на міжнародному рівні – Європейська Хартія прав пацієнтів, та Закон України «Основи законодавства України про охорону здоров'я». З метою захисту персональних даних особи Україною ратифіковано Конвенцію про захист осіб у зв'язку з автоматизованою обробкою персональних даних і Додатковий протокол до Конвенції про захист осіб у зв'язку з автоматизованою обробкою персональних даних щодо органів нагляду та транскордонних потоків даних [1], а також прийнято Закон України «Про захист персональних даних». Відповідальність

за розголошення персональних даних пацієнта, та/або використання його персональних відомостей в ході проведення клінічного дослідження також може наставати в як окремо так і в поєданні з відповідальністю яка застосовується відповідно до норми статті 145 Кримінального кодексу України (КК України) – незаконне розголошення лікарської таємниці. За КК України, незаконне розголошення лікарської таємниці це умисне розголошення лікарської таємниці особою, якій вона стала відома у зв'язку з виконанням професійних чи службових обов'язків, якщо таке діяння спричинило тяжкі наслідки.

У результаті опрацювання чинних редакцій статей 141, 142 КК України, можуть бути запропоновані деякі уточнення до редакції статей з приділенням уваги проведенню клінічних випробувань лікарських засобів без інформованої згоди, доповнення терміну «письмова згода» у змісті диспозиції статті 141 змістом «інформована» згода зі спеціальним розшифруванням цього поняття у примітці до статті. Підставою тому, є суспільна значущість захисту персональних даних на національному рівні., а тому треба щоб пацієнт не лише надав згоду на обробку його особистої інформації, а також розумів значення дій на які він надає згоду.

Цікавим є зарубіжний досвід юридичної відповідальності за порушення законодавства у сфері захисту персональних даних. Наприклад, законодавство США є досить жорстким і надалі лише посилює відповідальність за втрату або незаконний доступ до баз персональних даних. Досвід європейських країн і США у сфері захисту персональних даних став підґрунтям для дослідження цієї проблеми Організацією економічної співпраці та розвитку (далі – ОЕСР), яка розпочала активну діяльність у цьому напрямі у 1969 році. Саме тоді виникли спроби вивчення комп'ютеризації та автоматизації обробки даних. У 1978 році ОЕСР створила групу експертів, основною спеціалізацією якої стали випадки транскордонної передачі інформації та захист відповідних даних.

Отже, можна визначити основні орієнтири у сфері національної регуляції захисту персональних даних і міжнародний досвід у розв'язанні цієї проблеми. Зусилля держав-членів Конвенції про захист осіб у зв'язку з автоматизованою обробкою персональних даних № 108 [2], та ОЕСР сприяли приведенню законодавств багатьох країн до стандартизації захисту прав споживачів щодо захисту та обробки персональних даних не лише в мережі Інтернет, а й взагалі у всіх мережевих системах. Виконання вимог Директиви 97/66/ЄС «Стосовно обробки персональних даних і захисту права на невтручання в особисте життя в телекомунікаційному секторі» [3] значно підвищило рівень

безпеки під час транскордонних потоків передачі персональних даних та їхнього надійного збереження в країнах, що взяли на себе відповідальність за виконання вказівок Директиви. При цьому різниця в підходах національних законодавств нівелюється досягненням основної мети – забезпечення основних прав людини у сфері охорони здоров'я [4 ; с. 45–49].

Станом на сьогодні на національному рівні функціонує низка нормативно-правових актів, які регулюють доступ запитувачів до окремих видів інформації та подання документів на розгляд до уповноважених органів. Такими нормативно-правовими актами є Конституція України, Закон України «Про інформацію», Закон України «Про захист персональних даних», Закон України «Про звернення громадян» тощо.

Особа, яка являється пацієнтом, в будь-якому випадку не позбавлена права на звернення до суду у встановленому законом порядку, в разі порушення на його думку особистий прав, свобод та інтересів з боку клініциста, персоналу медичного закладу. До останніх відноситься конституційне, адміністративне судочинство та механізм звернення до Європейського Суду з прав людини [5; 3–9].

З розвитком інформаційних технологій у медичній сфері, а саме – запровадженням інформаційно-телекомунікаційних технологій у поєднанні із збільшенням об'ємів і напрямів використання інформації, її передання новітніми засобами комунікації значно розширилися можливості зі збирання, зберігання й обробки інформації щодо окремих громадян у закладах охорони здоров'я. Активність у формуванні автоматизованих баз даних, обробка та поширення відомостей про осіб без їхнього відома, згоди, (особливо проблемні питання почали виявлятись із реформуванням медичної галузі) призвели до виникнення проблеми інформаційної безпеки як медичних працівників, пацієнтів, так і третіх осіб щодо захисту персональних даних.

За відсутності чіткого механізму детального регулювання питань збирання, використання і знищення персоніфікованої інформації у сфері медицини існує, як указують науковці, ризик порушення права на приватність такої інформації [6; с. 45–46]. Загалом цифровізація медичної галузі видається слушною та раціональною інтеграційною складовою імплементації економічних, політичних та правових складових в геополітичні потоки міжнародної спільноти.

На прикладі Єдиної інформаційної системи Міністерства внутрішніх справ можливе внесення пропозицій щодо цифровізації медичної галузі в частині обробки, збору, структурування, збереження та використання інформації яка містить лікарську таємницю.

У відповідності до пункту 2 Положення про єдину інформаційну систему Міністерства внутрішніх справ, єдина інформаційна система МВС – багатофункціональна інтегрована автоматизована система, що безпосередньо забезпечує реалізацію функцій її суб'єктів, інформаційну підтримку та супроводження їх діяльності і становить сукупність взаємозв'язаних функціональних підсистем, програмно-інформаційних комплексів, програмно-технічних та технічних засобів електронної комунікації, які забезпечують логічне поєднання визначених інформаційних ресурсів, обробку та захист інформації, внутрішню та зовнішню інформаційну взаємодію.

Інформаційні ресурси єдиної інформаційної системи МВС – визначені групи взаємозв'язаних задокументованих одиниць інформації, які формуються і об'єднуються в автоматизованих інформаційних системах суб'єктів єдиної інформаційної системи МВС за певними ознаками, у тому числі зазначені в переліку пріоритетних інформаційних ресурсів єдиної інформаційної системи Міністерства внутрішніх справ, затвердженому постановою Кабінету Міністрів України від 14 листопада 2018 р. N 1024 [7].

Основним важелем впровадження та використання ЄІС МВС слугує стійка ієрархічна інформаційна цифрова структура, що вміщує в собі значні блоки та обсяг інформаційних ресурсів даної системи. З врахуванням корупційних ризиків, інших супутніх факторів, доступ до блоків системи, їх частин, систем та підсистем може надаватися децентралізовано та з певними обмеженнями.

На прикладі Плану заходів з виконання Річної національної програми під егідою Комісії Україна – НАТО на 2021 р., з врахуванням беззаперечного пріоритету напрямку розвитку окремих програм держави в напрямку розвитку оборонного сектору економіки та посиленню національної безпеки, згаданим планом заходів передбачено впровадження програми підвищення обізнаності населення в правовій сфері, розвиток антикорупційних програм та підвищення рівня кібербезпеки.

Разом із тим, медична галузь в даному плані заходів згадується переважно щодо потенційної можливості забезпечення та охорони здоров’я працівників силових структур. Тобто в даному випадку мова не йде про громадянське суспільство в повному обсязі [8]. Разом із тим тенденції впливу держави на структурованість процесу в поєднанні із структурованістю та уніфікацією підходу реалізації процедури може використовуватись й в інших економічних, соціальних та суспільних галузях національного рівня.

Список використаних джерел:

1. Конвенція про захист осіб у зв'язку з автоматизованою обробкою персональних даних : Конвенція Ради Європи від 28.01.1981 р. : станом на 6 лип. 2010 р. URL: https://zakon.rada.gov.ua/laws/_show/994_326#Text (дата звернення: 03.05.2023).

2. Конвенція про захист осіб у зв'язку з автоматизованою обробкою персональних даних : Конвенція Ради Європи від 28.01.1981 р. : станом на 6 лип. 2010 р. URL: https://zakon.rada.gov.ua/laws/show/994_326#Text (дата звернення: 02.05.2023).

3. Директива 97/66/ЄС Європейського Парламенту і Ради «Стосовно обробки персональних даних і захисту права на невтручання в особисте життя в телекомунікаційному секторі» : Директива Європ. Союзу від 15.12.1997 р. № 97/66/ЄС : станом на 12 лип. 2002 р. URL: https://zakon.rada.gov.ua/laws/show/994_243#Text (дата звернення 03.05.2023).

4. Муляр Г. адміністративна відповідальність за порушення законодавства щодо захисту персональних даних у сфері охорони здоров'я. Правова позиція. *Адміністративне та митне право*. 2020. Т. 28, № 3. С. 45–49. URL: https://doi.org/10.32836/2521-6473.2020-3.8. (дата звернення: 03.05.2023).

5. Галай В. Способи захисту прав пацієнтів і Україні Детальніше: https://medkniga.com.ua/5200-sposobi-zahistu-prav-patsiyentiv-i-ukrayini/ : Науково-практ. посіб. Київ : «ВИД. ДІМ "СКІФ"», 2009. 72 с.

6. Коталейчук С. Реалізація та захист персоніфікованої інформації у законодавстві України: правове забезпечення. *Право України.* 2006. № 1. С. 46–50.

7. Про затвердження Положення про єдину інформаційну систему Міністерства внутрішніх справ та переліку її пріоритетних інформаційних ресурсів : Постанова Каб. Міністрів України від 14.11.2018 р. № 1024 : станом на 11 квіт. 2023 р. URL: https://zakon.rada.gov.ua/laws/show/1024-2018-п#Text (дата звернення: 03.05.2023).

8. Про затвердження плану заходів з виконання Річної національної програми під егідою Комісії Україна – НАТО на 2021 рік та показників ефективності її виконання : Розпорядж. Каб. Міністрів України від 16.06.2021 р. № 690-р. URL: https://zakon.rada.gov.ua/laws/show/690-2021-р#Text (дата звернення: 03.05.2023).