Вищий навчальний заклад «Український католицький університет»

Факультет суспільних наук
назва факультету
Кафедра теорії права та прав людини
(повна назва кафедри)

Пояснювальна записка

до дипломного проекту (магістерської роботи)
магістр
(освітній ступінь)

на тему : «Медичні дані: правова охорона та захист»

Виконав:
студент ІІ курсу, групи СПЛ__/М
спеціальності 081 «Право»
(шифр і назва спеціальності)
_____ Ган Н.Р._____
(прізвище та ініціали)
Керівник _____Сенюта І.Я. _____
(прізвище та ініціали)
Рецензент_____Квіт Н.М. _____
(прізвище та ініціали)

Львів – 2021 року

ЗМІСТ

ВСТУП

В епоху стрімкої інформаційної глобалізації та транскордонної передачі даних актуальним питанням є охорона та захист персональних даних, у тому числі, медичних даних. Пандемія коронавірусної хвороби (COVID-19) загострила проблему необхідності дотримання особистого немайнового права на нерозголошення персональних, зокрема медичних даних, а також потреби знаходження балансу між правом на приватне життя та громадським здоров'ям.

Постановою Кабінету Міністрів України від 25.04.2018 р. № 411 затверджено Порядок функціонування електронної системи охорони здоров'я. Перехід до електронної системи охорони здоров'я означає з-поміж іншого внесення персональних даних пацієнтів до електронної системи охорони здоров'я вже на етапі підписання декларації з сімейним лікарем та подальшу обробку таких даних. Це, своєю чергою, передбачає зміни в правовій охороні медичних даних і забезпечення додаткових гарантій обробки персональних даних пацієнтів. Зважаючи на актуальність тематики в Україні та беручи до уваги перехід на електронну систему охорони здоров'я більшості розвинутих країн світу, наша праця присвячена дослідженню правового регулювання саме медичних даних.

Проблематику захисту такого різновиду персональних даних як медична інформація досліджували С. В. Антонов, П. П. Андрушко, М. В. Бем, С. Б. Булеца, А. А. Герц, В. В. Валах, З. С. Гладун, І. М. Городиський, Н. М. Квіт, О. В. Кохановська, Р. А. Майданик, Х. В. Майкут, А. І. Марущак , І. Я. Сенюта, С. Г. Стеценко, О. М. Родіоненко, Х. Я. Терешко, І. В. Шатковська тощо, однак тема не втрачає своєї актуальності. Про це свідчить низький рівень імплементації механізмів охорони та захисту персональних даних, масові порушення прав суб'єктів персональних даних, низька ефективність притягнення винних до відповідальності за порушення прав суб'єктів медичних даних у сфері надання медичної допомоги. Вищеперелічене є однією із перешкод на шляху до європейської інтеграції України, на який стала наша держава, підписавши Угоду про асоціацію між Україною, з однієї сторони, та

Європейським Союзом, Європейським співтовариством з атомної енергії і їхніми державами-членами, з іншої сторони, що також підтверджує актуальність обраної нами тематики.

Основною метою даної роботи є визначення ефективних механізмів охорони та захисту медичних даних і пропозицій щодо їх удосконалення, з'ясування основних прогалин у законодавстві щодо забезпечення прав суб'єктів медичних даних у сфері надання медичної допомоги та притягнення винних до відповідальності за їх порушення.

Для досягнення цієї мети, в межах даного дослідження, необхідно виконати такі завдання:

- розкрити правову природу та обсяг поняття «медичні дані»;
- визначити місце медичних даних у системі персональних даних;
- з'ясувати механізми охорони та захисту медичних даних за законодавством України та запропонувати шляхи їх вдосконалення;
- проаналізувати загальні вимоги до обробки персональних, в тому числі, медичних даних;
- проаналізувати функціонування системи e-Health в Україні в контексті захисту персональних, в тому числі, медичних даних;
- з'ясувати спеціальні права суб'єктів медичних даних у сфері надання медичної допомоги;
- встановити особливості притягнення до юридичної відповідальності винних за порушення інформаційних прав суб'єктів медичних даних;
- висвітлити національну судову практику та практику Європейського суду з прав людини, пов'язану з захистом медичних даних.

Об'єктом дослідження є юридична категорія «медичні дані» як особливий різновид персональних даних з чутливою обробкою. Предметом дослідження є стан, закономірності та перспективи розвитку правової категорії «медичні дані». З'ясування таких закономірностей здійснено через дослідження наукових поглядів, ідей, концепцій і теорій, норм міжнародно-правових стандартів, нормативно-правових актів України та зарубіжних країн, а також

судової та іншої правозастосовної практики щодо юридичної конструкції «медичні дані».

Під час аналізу цієї проблематики був використаний системний метод для з'ясування місця медичних з-поміж персональних даних, формально-юридичний метод щодо визначення правової природи та обсягу поняття «медичні дані». Також було застосовано метод системного аналізу щодо виокремлення основних механізмів захисту персональних даних. Під час дослідження судової практики використовувався метод вивчення юридичної практики, а для з'ясування змісту відповідних правових норм і сутності оцінних понять – метод тлумачення права. Для виокремлення основної проблематики та з'ясування шляхів вдосконалення системи захисту медичних даних було застосовано метод правового моделювання.

Ключовими доктринальними джерелами роботи є праці низки науковців, зокрема, Х. Я. Терешко, яка у своїй дисертації на здобуття наукового ступеня кандидата юридичних наук на тему «Інформація як об'єкт цивільних правовідносин у сфері медичного обслуговування» (2019) розкрила, зокрема, зміст поняття «медична інформація» та її місце в системі «інформації у сфері медичного обслуговування». Проаналізовано кандидатську дисертацію Антонова С. В. «Цивільно-правова відповідальність за заподіяння шкоди здоров'ю при наданні платних медичних послуг» (2006), що розкрив зміст поняття «медична таємниця» та відзначив доцільність використання наведеного поняття на противагу поняття «лікарська таємниця". В основу джерел дослідження покладено докторську дисертацію І. Я. Сенюти «Цивільні правовідносини у сфері надання медичної допомоги в Україні: питання теорії та практики» (2018), в якій проаналізовано проблематику дотримання права на інформацію суб'єкта медичних даних, наприклад, особливі умови обробки медичних даних, пов'язані з доступом до таких студентів, інтернів; права на медичну таємницю. Опрацьовано науково-практичний посібник Бема М. В., Городиського І. М., Саттона Г., Родіоненко О. М. «Захист персональних даних:

Правове регулювання та практичні аспекти» (2015), який, зокрема, містить вичерпний аналіз окремих механізмів захисту персональних даних.

Магістерська робота складається із вступу, трьох основних розділів, висновків, списку використаних джерел. Перший розділ роботи поділений на чотири підпункти та містить аналіз правової природи категорії «медичні дані», теоретичних підходів до визначення обсягу поняття «медична інформація» та аналіз наявних нормативних механізмів охорони та захисту медичних даних. Другий розділ складається з трьох підпунктів та передбачає аналіз чинного національного законодавства щодо обробки медичних даних, у тому числі транскордонної передачі даних і функціонування електронної системи охорони здоров'я в Україні. У третьому розділі проаналізовані спеціальні інформаційні права суб'єктів медичних даних у сфері надання медичної допомоги та відповідальність за їх порушення. Містить два підпункти. Вперше системно досліджено правову конструкцію «медичні дані» крізь призму національної судової практики та практики Європейського суду з прав людини, а також виокремлено основні правозастосовні проблеми та механізми охорони та захисту такого виду чутливих персональних даних і запропоновано шляхи їх нормативного удосконалення, що становить наукову новизну праці.

СПИСОК УМОВНИХ ПОЗНАЧЕНЬ

1. Європейський суд з прав людини – ЄСПЛ.
2. Єдиний державний реєстр судових рішень – ЄДРСР.
3. Закон України «Основи законодавства України про охорону здоров'я» – Основи законодавства України про охорону здоров'я.
4. Кодекс законів про працю України – КЗпП.
5. Конвенція про захист прав людини і основоположних свобод - Конвенція.
6. Кодекс України про адміністративні правопорушення – КУпАП.
7. Кримінальний кодекс України – КК України.
8. Регламент Європейського Парламенту і Ради (ЄС) 2016/679 від 27 квітня 2016 року про захист фізичних осіб у зв’язку з опрацюванням персональних даних і про вільний рух таких даних, та про скасування Директиви 95/46/ЄС – Загальний регламент про захист даних.
9. Рекомендація № R (97) 5 Ради Європи щодо захисту медичних даних від 13.02.1997 р. - Рекомендація № R (97) 5.
10. Уповноважений Верховної Ради України з прав людини (Уповноважений ВР).
11. Цивільний кодекс України – ЦК України.

РОЗДІЛ 1. Медичні дані як різновид персональних даних: поняття, ознаки

1.1. Правова природа медичних даних і їх місце в системі персональних даних

Правова охорона медичних даних гарантується Конституцією України, норми якої мають пряму дію. Зокрема, в ст. 32 Основного Закону зазначено: «Ніхто не може зазнавати втручання в його особисте і сімейне життя, крім випадків, передбачених Конституцією України».[1] При цьому, обробка конфіденційної інформації без згоди особи може відбуватись лише у випадку передбачення винятків у законі та лише в інтересах національної безпеки, економічного добробуту та прав людини[2].

Для того, щоб належним чином розкрити зміст та обсяг поняття «медичні дані», необхідно насамперед зрозуміти його правову природу та встановити взаємозв'язок із суміжними поняттями.

Відповідно до ст. 1 Закону України «Про електронні документи та електронний документообіг», дані - це «інформація, яка подана у формі, придатній для її оброблення електронними засобами»[3]. Своєю чергою, Закон України «Про інформацію», визначає інформацію як «будь-які відомості та/або дані, які можуть бути збережені на матеріальних носіях або відображені в електронному вигляді»[4]. Таким чином, із буквального текстуального тлумачення законодавчих положень випливає, що медичні дані – це різновид інформації, а саме персональних даних, що подана у формі, придатній для оброблення автоматичними засобами.

Медичні дані є складовою персонанальних даних та, відповідно, підпадають під сферу дії законодавства про захист персональних даних. Згідно зі ст. 2 Закону України «Про захист персональних даних», «персональні дані -

[1] Конституція України: Верховна Рада України; Закон від 28.06.1996 р. № 254к/96-ВР // Відомості Верховної Ради України. – 1996. – № 30. – с.141.

[2] Там само.

[3] Закон України «Про електронні документи та електронний документообіг»: Верховна Рада України; Закон від 22.05.2003 № 851-IV // Відомості Верховної Ради України. – 2003. – № 36. – с.275.

[4] Закон України «Про інформацію»: Верховна Рада України; Закон від 02.10.1992 № 2657-XII // Відомості Верховної Ради України. – 1992. – № 48. – с.650.

відомості чи сукупність відомостей про фізичну особу, яка ідентифікована або може бути конкретно ідентифікована»[5]. Варто звернути увагу на те, що інформація про особу та персональні дані не є ідентичними поняттями. Плутанина пов'язана з некоректним, на нашу думку, ототожненням цих понять в ч. 1 ст. 11 Закону України «Про інформацію». У поданому вище визначенні «персональних даних» наголошується саме на здатності ідентифікувати конкретну особу, вирізнити людину з-поміж інших завдяки певній інформації. А тому, ми вважаємо, що деперсоналізована, анонімна інформація про особу, в тому числі медичного характеру, не є персональними даними за умови відсутності будь-яких ознак, що уможливлюють ідентифікацію особи та, відповідно, не підлягає правовій охороні відповідно до Закону України «Про захист персональних даних».

Це підтверджують також положення п. 1 Рекомендації № R (97) 5 про те, що «персональні дані включають в себе будь-яку інформацію, що стосується визначеної особи або особи, яку можна ідентифікувати. Особа не вважається такою, кого можна ідентифікувати, якщо її визначення вимагає невиправданого періоду часу та людських ресурсів. У випадках, коли особу не можна визначити, дані вважаються анонімними»[6].

При цьому, важливим є розмежування, чи справді анонімна, деперсоналізована інформація є такою, що не дає змогу ідентифікувати людину в кожному конкретному випадку, адже в сукупності з іншими даними, часто залишається можливість ідентифікації конкретної особи (так звана, опосередкована ідентифікація). До прикладу, деперсоналізовані дані солдатів, що використовували фітнес-трекери Strava, через використання даних GPS, спричинили виявлення у 2017 році місцезнаходження кількох військових

[5] Закон України «Про захист персональних даних»: Верховна Рада України; Закон від 01.06.2010 № 2297-VI // Відомості Верховної Ради України. – 2010. – № 34. – с.481.

[6] Recommendation on the Protection of Medical Data: Council of Europe, Committee of Ministers; Feb. 13, 1997. № R (97) 5 [Електронний ресурс]. – Режим доступу : https://www.coe.int/en/web/data-protection/legal-instruments.

баз США.[7] Саме тому, з метою захисту персональних даних в українській системі e-health, знеособлені медичні дані зберігають відокремлено від персональних даних пацієнтів (про це детальніше – в пп. 2.2 нашої праці). Ми вважаємо за необхідне наголосити, що до персональних, зокрема, медичних, даних належить не лише інформація, що прямо ідентифікує особу, але й знеособлена інформація, яка в сукупності з іншими даними, уможливлює ідентифікацію особи.

Важливо розмежовувати медичні дані, як різновид персональних, від конфіденційної медичної інформації. Персональні дані – це завжди інформація про живих фізичних осіб або ж про юридичних осіб. Інформація, що стосується, зокрема, медичної інформації померлих, має режим конфіденційності, однак Закон України «Про захист персональних даних» на неї не поширюється. Вказані правовідносини підлягають правовій охороні відповідно до Закону України «Про поховання та похоронну справу», ст. 7 якого гарантовано конфіденційність інформації про померлого.[8]

Таким чином, медичні дані за своєю природою є персональними даними, які, в силу необхідності підвищеної правової охорони, віднесені законодавцем до конфіденційної інформації. При цьому, знеособлені медичні дані не підпадають під законодавство про захист персональних даних за відсутності будь-яких інших даних, які дають змогу ідентифікувати людину, що на практиці досягнути доволі проблематично. Саме можливість ідентифікації конкретної особи (пряма або опосередкована) лежить в основі розмежування персональних даних та надання окремим категоріям даних відповідного правового захисту.

[7] Fitness tracking app Strava gives away location of secret US army bases. The Guardian. 2018. [Електронний ресурс]. – Режим доступу: https://www.theguardian.com/world/2018/jan/28/fitness-tracking-app-gives-away-location-of-secret-us-army-bases

[8] Закон України «Про поховання та похоронну справу»: Верховна Рада України; Закон від 10.07.2003 № 1102-IV // Відомості Верховної Ради України. – 2004. – № 7. – с. 47.

З’ясувавши правову природу медичних даних та розмежувавши суміжні до персональних даних поняття, пропонуємо визначити обсяг поняття «медичні дані».

1.2. Правове регулювання медичних даних за національним законодавством і за міжнародними стандартами

У національному законодавстві немає уніфікованого визначення поняття «медичних даних» або «медичної інформації». Зокрема, для формулювання такої правової конструкції використовуються такі терміни: «медична інформація» (ст. 39 Основ), «інформація про стан здоров’я» (ст. 285 ЦК України, ст. 39 Основ), «таємниця про стан здоров'я, факт звернення за медичною допомогою, діагноз, а також про відомості, одержані при його медичному обстеженні» (ст. 39-1 Основ)[9]. На нашу думку, такі формулювання не розкривають обсяг поняття «медичних даних» або ж невиправдано звужують її.

Поняття «медична інформація» розкрито у пп. 8 п. 2 Порядку функціонування електронної системи охорони здоров’я, затвердженого Постановою Кабінету Міністрів України від 25.04.2018 № 411 (далі – Порядок № 411), а саме: «медична інформація – це інформація про стан здоров’я пацієнта, його діагноз, відомості, одержані під час медичного обстеження, у тому числі відповідні медичні документи, що стосуються здоров’я пацієнта»[10]. Однак з поданого вище визначення поняття «інформація» методом синтезу можна виокремити, що документ є всього-на-всього матеріальним носієм, що містить інформацію. Саме тому, вважаємо за необхідне погодитися з критичним твердженням Терешко Х.Я. щодо віднесення медичної документації до переліку

[9] Основи законодавства України про охорону здоров'я: Верховна Рада України; Закон від 19.11.1992 р. № 2801-XII // Відомості Верховної Ради України. – 1993. – № 4. – с.19.

[10] Деякі питання електронної системи охорони здоров’я: Постанова Кабінету Міністрів України від 25.04.2018 № 411. [Електронний ресурс]. – Режим доступу : https://zakon.rada.gov.ua/laws/show/411-2018-%D0%BF#Text

видів медичної інформації, оскільки медична документація є джерелом інформації, а не самою інформацією.[11]

У рішенні Конституційного Суду України у справі щодо офіційного тлумачення ст. 3, 23, 31, 47, 48 Закону України «Про інформацію» та ст. 12 Закону України «Про прокуратуру» (справа К. Г. Устименка) від 30.10.1997 р. (справа № 18/203-97) під медичною інформацією суд розуміє: «свідчення про стан здоров'я людини, історію її хвороби, про мету запропонованих досліджень і лікувальних заходів, прогноз можливого розвитку захворювання, в тому числі про наявність ризику для життя і здоров'я, що за своїм правовим режимом належить до конфіденційної, тобто інформації з обмеженим доступом»[12].

Статтею 285 ЦК України, що стосується права на інформацію про стан свого здоров'я, передбачено, що «повнолітня фізична особа має право на достовірну і повну інформацію про стан свого здоров'я, у тому числі на ознайомлення з відповідними медичними документами, що стосуються її здоров'я».[13] Вважаємо, що інформація про стан свого здоров'я – це один із видів медичної інформації (медичних даних). Остання являє собою значно ширший спектр інформації, а тому ці поняття співвідносяться між собою як частина та ціле.

Із ст. 39 Основ (щодо обов'язку надання медичної інформації) можна виокремити такий обсяг досліджуваного поняття : «інформація про стан здоров'я пацієнта, мета проведення запропонованих досліджень і лікувальних заходів, прогноз можливого розвитку захворювання, у тому числі наявність ризику для життя і здоров'я».[14]

---

[11] Терешко Х. Я. Інформація як об'єкт цивільних правовідносин у сфері медичного обслуговування: дис. канд. юрид. наук: 12.00.03. Київ, 2019. 227 с. (ст.36)

[12] Рішення Конституційного Суду України у справі щодо офіційного тлумачення ст. 3, 23, 31, 47, 48 Закону України «Про інформацію» та ст. 12 Закону України «Про прокуратуру» (справа К. Г. Устименка) від 30.10.1997 (справа № 18/203-97). [Електронний ресурс]. – Режим доступу : http://zakon3.rada.gov.ua/laws/show/v005p710-97

[13] Цивільний кодекс України: Верховна Рада України; Закон від 16.01.2003 № 435-IV // Інформаційний бюлетень НКРЕ. – 2003. – № 7.

[14] Основи законодавства України про охорону здоров'я: Верховна Рада України; Закон від 19.11.1992 р. № 2801-XII // Відомості Верховної Ради України. – 1993. – № 4. – с.19

Згідно із п. 6 Роз'яснень основних положень Порядку повідомлення Уповноваженого Верховної ради з прав людини щодо визначення обробки персональних даних, яка становить особливий ризик для прав і свобод суб'єктів персональних даних, під станом здоров'я особи розуміється «медична інформація про особу, що містить не лише свідчення про стан здоров'я, а й про історію її хвороби, про запропоновані дослідження і лікувальні заходи, прогноз можливого розвитку захворювання, в тому числі і про наявність ризику для життя і здоров'я (виняток становлять медичні довідки, листи працездатності тощо, які обробляються володільцем при реалізації трудових відносин)».[15] На нашу думку, таке розширювальне тлумачення законодавчих положень є виправданим та необхідним для належного застосування права.

У проекті Закону України «Про права пацієнтів» від 01.03.2013 № 2438 міститься натомість невиправдано широке визначення «медичної інформації про пацієнта» як «будь-яких відомостей про стан здоров'я пацієнта, у тому числі щодо діагностики, лікування чи профілактики захворювання, а також про особисте, сімейне життя або інші відомості про пацієнта, які стали відомі медичному працівнику у процесі надання медичної допомоги».[16] На нашу думку, попри те, що інформація про особисте, сімейне життя пацієнта є складовою медичної таємниці (п. 3.1 нашої праці), такі відомості/дані безпосередньо не пов’язані з поняттям «медичні дані».

Для визначення обсягу поняття «медичних даних» слід звернутись до міжнародних та регіональних документів. Відповідно до положень принципу 7 (право на інформацію) Лісабонської декларації про права пацієнтів, норми якої мають декларативний характер, медична інформація

---

[15] Роз'яснення основних положень Порядку повідомлення Уповноваженого щодо визначення обробки персональних даних, яка становить особливий ризик для прав і свобод суб'єктів персональних даних : Уповноважений Верховної Ради України з прав людини; Роз’яснення від 08.01.2014 [Електронний ресурс]. – Режим доступу: https://zakon.rada.gov.ua/laws/show/n0003715-14#Text

[16] Проект Закону України «Про права пацієнтів» від 01.03.2013 № 2438 [Електронний ресурс]. – Режим доступу: http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=45938

розглядається як зафіксована у будь-яких медичних записах інформація про пацієнта щодо стану його здоров'я.[17]

Обґрунтоване визначення міститься в ст. 3 (право на інформацію) розділу 2 Європейської хартії прав пацієнтів, яка попри відсутність обов'язкової юридичної сили користується значним авторитетом. А саме, медична інформація – це будь-якого роду інформація, що стосується стану здоров'я пацієнта, медичних послуг і способів їх отримання, всього, що доступно завдяки науково-технічному прогресові.[18]

Зауважимо, що пунктом 1 Рекомендації № R (97) 5 до медичних даних віднесено не лише всі персональні дані про стан здоров'я фізичної особи та ті, які чітко і тісно пов'язані з даними про стан здоров'я, але й генетичні дані.[19]

Необхідно розмежовувати поняття «медичні дані» та «інформацію у сфері медичного обслуговування», яке за обсягом є ширшим поняттям, оскільки включає в себе як інформацію, пов'язану з наданням медичної допомоги, яка є приватноправовою за характером, складовою якої є медична інформація (медичні дані), так і публічно-правову та приватно-правову інформацію, пов'язану з процесом організації надання медичної допомоги.

Зокрема, Х. Я. Терешко визначає «інформацію у сфері медичного обслуговування» як «відомості та/або дані, які формуються при динаміці правовідносин у сфері медичного обслуговування, що опосередковують процес організації надання і надання медичної допомоги, а також провадження іншої ліцензійної діяльності у сфері охорони здоров'я, та збережені на матеріальних носіях або відображені в електронній формі».[20] Своєю чергою, Х. Я. Терешко поділяє інформацію, пов'язану з наданням медичної допомоги на: 1. Медичну

[17] Лісабонська декларація стосовно прав пацієнта: Міжнародний документ Всесвітньої медичної асоціації від 01.10.1981 [Електронний ресурс]. – Режим доступу : http://zakon3.rada.gov.ua/laws/show/990_016.

[18] Європейська хартія прав пацієнтів: Активна громадська мережа у співпраці з громадськими організаціями з 12 різних країн ЄС від 15.11.2002 [Електронний ресурс]. – Режим доступу : http://meduniv.lviv.ua/files/press-centre/2014/n180414/evropejska_ hartiya_prav_pacientiv.pdf.

[19] Recommendation on the Protection of Medical Data: Council of Europe, Committee of Ministers; Feb. 13, 1997. № R (97) 5 [Електронний ресурс]. – Режим доступу : https://www.coe.int/en/web/data-protection/legal-instruments

[20] Терешко Х. Я. Інформація як об'єкт цивільних правовідносин у сфері медичного обслуговування: дис. канд. юрид. наук: 12.00.03. Київ, 2019. 227 с. (ст.23)

інформацію (медичні відомості/дані); 2. Інформацію немедичного характеру, тісно пов'язану із медичними відомостями/даними; 3. Інформацію, пов'язану із приватним і сімейним життям.[21]

Аби визначити обсяг поняття «медичні дані» вважаємо за необхідне звернутись до судової практики.

Зокрема, в рішенні від 27.01.2017 р. в справі «Суріков проти України» (заява № 42788/06) Європейський суд з прав людини зазначив, що «інформація, пов'язана із розладом психічного здоров'я по своїй суті становить дуже чутливі персональні дані, незалежно від того, чи був зазначений конкретний медичний діагноз. Збирання, зберігання, розкриття або інші види обробки такої інформації підпадають під дію статті 8».[22]

У рішенні від 23.02.2016 р. у справі «Й.Й. проти Росії» (заява № 40378/06) ЄСПЛ також наголосив, що особиста інформація пацієнта є елементом його приватного життя. Захист особистих даних, особливо даних, що становлять лікарську таємницю, має фундаментальне значення у використанні громадянином його або її права на приватне та сімейне життя, гарантованого статтею 8 Конвенції.[23]

Вартує зазначити також рішення від 26.05.11 р. у справі «Р. Р. проти Польщі» (заява № 27617/04), в якому ЄСПЛ відзначив, що стан здоров'я плода є елементом здоров'я вагітної жінки, а тому розглядав наявність порушення права на доступ до зазначеної інформації в контексті статті 8 Конвенції.[24]

У рішенні Великої Палати від 04.12.2008 р. у справі «Маргер проти Сполученого Королівства» (заяви № 30562/04 та 30566/04) ЄСПЛ відніс дані

---

[21] Терешко Х. Я. Інформація як об'єкт цивільних правовідносин у сфері медичного обслуговування: дис. канд. юрид. наук: 12.00.03. Київ, 2019. 227 с.

[22] Рішення Європейського суду з прав людини від 27.01.2017 року у справі «Суріков проти України» (заява № 42788/06) [Електронний ресурс]. – Режим доступу: https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-170462%22]}

[23] Рішення Європейського суду з прав людини від 23.02.2016 року у справі «Й.Й. проти Росії» (заява № 40378/06) [Електронний ресурс]. – Режим доступу: https://hudoc.echr.coe.int/eng#{%22fulltext%22:[%22\%22CASE%20OF%20Y.Y.%20v.%20RUSSIA\%22%22],%22documentcollectionid2%22:[%22GRANDCHAMBER%22,%22CHAMBER%22],%22itemid%22:[%22001-161048%22]}

[24] Рішення Європейського суду з прав людини від 26.05.11 року у справі «Р. Р. проти Польщі» (заява № 27617/04) [Електронний ресурс]. – Режим доступу: https://hudoc.echr.coe.int/eng#{%22display%22:[%220%22],%22languageisocode%22:[%22UKR%22],%22appno%22:[%2227617/04%22],%22documentcollectionid2%22:[%22CHAMBER%22],%22itemid%22:[%22001-145424%22]}

ДНК до складу «персональних даних», попри той факт, що вони не записані на типових носіях, і належно обробити їх може лише спеціальний апарат.[25]

Беручи до уваги національне законодавство, міжнародні та регіональні документи, а також судову практику, вважаємо за необхідне запропонувати авторське визначення. «Медичні дані» - це: інформація про стан здоров'я пацієнта(ки), його/її діагноз, історію його/її хвороби, про запропоновані дослідження і лікувальні заходи, прогноз можливого розвитку захворювання, інші дані, які безпосередньо пов'язані із станом здоров'я пацієнта(ки) та процесом надання йому/їй медичної допомоги, а також, його/її генетичні дані.

1.3. Особливості медичних даних

У п.1.1. нашої роботи ми згадували першу властивість медичних даних, а саме належність до персональних даних та, відповідно, поширення на вказану категорію законодавства про захист персональних даних. Вважаємо за необхідне відзначити другу ознаку медичних даних, а саме – *«чутливість»* їх обробки.

«Чутливість обробки» передбачає підвищений рівень охорони та захисту, а також спеціальний порядок обробки такого різновиду персональних даних, оскільки у разі їх розкриття існує особливий ризик для прав і свобод особи.

Така властивість медичних даних випливає, насамперед, із закріплення додаткової вказівки в законі щодо конфіденційності такої інформації (ч.2 ст.11 Закону України «Про інформацію»). Тобто, це додаткова гарантія нерозголошення такої інформації навіть до моменту обмеження доступу до неї фізичною особою. Попри це, особа має право у разі потреби реалізувати своє право на розкриття персональної інформації про себе, навіть якщо вона належить до різновиду даних із чутливою обробкою.

[25] Рішення Європейського суду з прав людини від 04.12.2008 у справі «Маргер проти Сполученого Королівства» (заяви № 30562/04 та 30566/04) [Електронний ресурс]. – Режим доступу: https://hudoc.echr.coe.int/fre#{%22itemid%22:[%22001-90051%22]}

Медичні дані підлягають спеціальному режиму доступу та обробки відповідно до Закону України «Про захист персональних даних» (п.2.1 нашої праці). Важливим кроком до виконання міжнародно-правових зобов'язань щодо охорони та захисту персональних даних, стало прийняття Порядку повідомлення Уповноваженого Верховної Ради України з прав людини про обробку персональних даних, яка становить особливий ризик для прав і свобод суб'єктів персональних даних, про структурний підрозділ або відповідальну особу, що організовує роботу, пов'язану із захистом персональних даних при їх обробці, а також оприлюднення вказаної інформації (далі – Порядок № 1/02-14), відповідно до п.1.2 якого, обробка персональних даних, що становить особливий ризик для прав і свобод суб'єктів стосується, з-поміж іншого, і даних про стан здоров'я особи [26]. Відповідно до п.3.2 Рекомендації № R (97) 5 Ради Європи щодо захисту медичних даних від 13.02.1997 р., медичні дані про особу повинні збиратись та оброблятися лише медичними працівниками або особами чи органами, які працюють від імені медичних працівників.[27] Розпорядники інформації, які не є медичними працівниками, повинні збирати та обробляти медичні дані лише з дотриманням правил конфіденційності, які можна порівняти з правилами охорони здоров'я, або з використанням однаково ефективних гарантій, передбачених національним законодавством.[28] (детальніше про обробку даних у п.2.1).

Варто зазначити, що згідно із статтею 6 Конвенції про захист осіб у зв'язку з автоматизованою обробкою персональних даних №108 (далі – Конвенція №108), особливі категорії персональних даних, в тому числі дані, що стосуються здоров'я та генетичних даних, не можуть піддаватись автоматизованій обробці, якщо національне законодавство не забезпечує

[26] Порядок повідомлення Уповноваженого Верховної Ради України з прав людини про обробку персональних даних, яка становить особливий ризик для прав і свобод суб'єктів персональних даних, про структурний підрозділ або відповідальну особу, що організовує роботу, пов'язану із захистом персональних даних при їх обробці, а також оприлюднення вказаної інформації: Наказ Уповноваженого Верховної Ради України з прав людини від 08.01.2014 № 1/02-14 [Електронний ресурс]. – Режим доступу: https://zakon.rada.gov.ua/laws/show/v1_02715-14#n218

[27] Recommendation on the Protection of Medical Data: Council of Europe, Committee of Ministers; Feb. 13, 1997. № R (97) 5 [Електронний ресурс]. – Режим доступу : http://hrlibrary.umn.edu/instree/coerecr97-5.html

[28] Там само.

відповідних гарантій.[29] Винятки із цього правила повинні бути передбачені законодавством держави, відповідати критерію необхідності в демократичному суспільстві та мати на меті: захист державної та громадської безпеки, фінансових інтересів Держави або на боротьбу з кримінальними правопорушеннями; або ж захист суб'єкта даних або прав і свобод інших людей.[30]

Тісно пов’язана з попередньою особливістю медичних даних – їх *конфіденційність*.

Женевська декларація 1948 року є першим документом, який визначає необхідність забезпечення конфіденційності медичних даних через обов’язок лікаря берегти таємницю, яку йому довірили, навіть після смерті пацієнта.[31] Згодом, аналогічне положення було закріплене в Міжнародному кодексі медичної етики.[32] Відповідно до положень принципу 6 із «Дванадцяти принципів організації охорони здоров’я для будь-якої національної системи охорони здоров’я», усі особи, що беруть участь у процесі лікування пацієнта на будь-якій стадії лікування, або особи, під контролем яких здійснюється таке лікування, повинні усвідомлювати та дотримуватись вимог конфіденційності.[33] Принагідно зазначимо, що це перший документ в якому міститься обов’язок дотримання медичної таємниці не лише лікарями, але й іншими службовими та посадовими особами, що актуально у зв’язку з некоректним закріпленням в законодавстві України терміну «лікарська таємниця».

Також і в Лісабонській декларації щодо прав пацієнта від 1 жовтня 1981р. встановлено правомірним очікування пацієнта, що його лікар буде поважати конфіденційний характер медичних та особистих відомостей про

---

[29] Конвенція про захист осіб у зв'язку з автоматизованою обробкою персональних даних : Міжнародний документ Ради Європи від 28.01.1981 №108. Дата ратифікації Україною: 06.07.2010. Дата набрання чинності для України: 01.01.2011. [Електронний ресурс]. – Режим доступу : https://zakon.rada.gov.ua/laws/show/994_326#Text

[30] Там само.

[31] Женевська декларація: Міжнародний документ Всесвітньої медичної асоціації від 01.09.1948 [Електронний ресурс]. – Режим доступу : http:// zakon3.rada.gov.ua/laws/show/990_001.

[32] Міжнародний кодекс медичної етики: Міжнародний документ Всесвітньої медичної асоціації від 01.10.1949 [Електронний ресурс]. – Режим доступу : http://zakon2.rada.gov.ua/laws/show/990_002.

[33] Дванадцять принципів організації охорони здоров’я для будь-якої національної системи охорони здоровя: Міжнародний документ Всесвітньої медичної асоціації від 01.10.1963 [Електронний ресурс]. – Режим доступу : http://zakon4.rada.gov.ua/laws/show/990_004.

пацієнта.[34] Примітно, що останній нормативно-правовий акт відмежовує медичну інформацію від інших відомостей особистого життя пацієнта, отриманих медичними працівниками. Останнє є важливим в аспекті розмежування «медичних даних» та «медичної таємниці», яке ми наводимо в пп.3.1 нашої праці.

Відповідно до п.4 Положення про медичне обстеження, «телемедицину» та медичну етику, повинна бути забезпечена конфіденційність всіх даних усіх пацієнтів, а також повинен існувати строгий контроль за доступом до даних, технічний захист і суворі правові санкції за порушення.[35] Вважаємо, шо важливим є не лише декларування обов'язку конфіденційності, але й забезпечення ефективної охорони та захисту через організаційні та технічні заходи, постійний контроль уповноважених органів та, безумовно, юридична відповідальність за порушення відповідних прав суб'єктів даних.

Подальший аналіз конфіденційності медичних даних, а також взаємозв'язок зазначеного поняття та «медичної таємниці» проаналізований нами в пп.3.1 нашої праці.

1.4. Механізми охорони і захисту медичних даних

Для того, щоб досягти ефективної охорони або ж захисту своїх прав, що стосуються медичних даних, необхідно розмежовувати механізми охорони та, відповідно, способи захисту своїх прав.

Відповідно до загальноприйнятого в науковій літературі розуміння понять «охорона» та «захист», охорона прав та свобод стосується контрольно-наглядових заходів, які здійснюються до вчинення правопорушення, тоді як необхідність захисту – активного втручання у правовідносини задля відновлення права - виникає вже після його порушення, оспорювання або

[34] Лісабонська декларація стосовно прав пацієнта: Міжнародний документ Всесвітньої медичної асоціації від 01.10.1981 [Електронний ресурс]. – Режим доступу : http://zakon3.rada.gov.ua/laws/show/990_016.

[35] Положення про медичне обстеження, «телемедицину» та медичну етику: Міжнародний документ Всесвітньої медичної асоціації від 01.09.1992 [Електронний ресурс]. – Режим доступу : https://zakon.rada.gov.ua/laws/show/990_049#Text

невизнання або ж для усунення реальної загрози його порушення.[36] Однак, на практиці законодавець доволі часто використовує вказані поняття як синоніми, тим самим підмінюючи поняття.

Охорона медичних даних передбачає конкретні заходи, які унеможливлюють неправомірне втручання в особисте життя особи, за також забезпечують цілісність, недоторканність і конфіденційність медичних даних, а також забезпечують можливість реалізації особою своїх прав, пов'язаних із одержанням доступу до персональних даних особи.

ЄСПЛ неодноразово зазначав важливості охорони медичних даних та закликав забезпечити відповідні гарантії в законодавстві, щоб унеможливити незаконне розголошення вказаного різновиду персональних даних (справа «М.С. проти Швеції»).[37]

Пропонуємо виділити наступні механізми охорони медичних даних:

Згода на обробку медичних даних

Відповідно до ст. 2 Закону України «Про захист персональних даних», «згода суб'єкта персональних даних - добровільне волевиявлення фізичної особи (за умови її поінформованості) щодо надання дозволу на обробку її персональних даних відповідно до сформульованої мети їх обробки, висловлене у письмовій формі або у формі, що дає змогу зробити висновок про надання згоди».[38] Аналізуючи визначення, волевиявлення фізичної особи щодо надання дозволу на обробку її персональних даних повинно відповідати 3 ознакам – добровільності, поінформованості та повинно бути виражена у зовнішній формі, що дає змогу зробити висновок про надання згоди. Для обробки чутливих, в тому числі і медичних, даних згода також повинна виконувати

[36] Тихонова Б. Ю. Субъективные права советских граждан, их охрана и защита :Автореферат диссертации на соискание ученой степени кандидата юридических наук. Специальность 710 - Теория и история государства и права /Б. Ю. Тихонова ; Науч. рук. Ю. Г. Ткаченко ; Министерство высшего и среднего спеціального образования СССР. Всесоюзный юридический заочный институт. -М.,1972. – с. 11.

[37] Сенюта І. Я. Хрестоматія Рішень Європейського суду з прав людини у сфері охорони здоров'я (окремі аспекти) / І. Я. Сенюта, КРИМІНАЛЬНЕ ПРАВО І КРИМІНОЛОГІЯ Юридичний вісник 1 (50) 2019 190 Н. С. Скрипець // Юридична газета. – № 21 (311). – 2012. – С. 15–16. [Електронний ресурс]. – Режим доступу: https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-60564%22]}

[38] Закон України «Про захист персональних даних»: Верховна Рада України; Закон від 01.06.2010 № 2297-VI // Відомості Верховної Ради України. – 2010. – № 34. – с.481.

критерій однозначності (ст. 7 Закону України «Про захист персональних даних»).[39]

Згідно із п. 5 Роз'яснення Уповноваженого Верховної Ради України з прав людини до Типового порядку обробки персональних даних, «згода на обробку персональних даних має бути свідомим рішенням особи, яке вона приймає добровільно, без примусу і погроз»[40]. Добровільність передбачає вільне волевиявлення особи за відсутності як прямого, так і опосередкованого примусу. Останній може виникнути, зокрема, якщо отримання певних суспільних благ, зокрема медичних послуг, безпосередньо залежить від надання згоди на обробку персональних даних та, зокрема, охоплює за обсягом ширше коло інформації, обробка якої не є необхідною для виконання конкретної мети відповідного договору про надання послуг, наприклад, використання певної інформації в маркетингових цілях. У разі ж не надання згоди, особа втрачає можливість отримання відповідних благ. Про це йдеться у п.43 Преамбули Регламенту 2016/679:

«Щоб забезпечити, що згоду було надано добровільно, вона не повинна передбачати необхідність застосування дійсних законних підстав опрацювання персональних даних у спеціальному випадку, коли існує помітний дисбаланс між суб'єктом даних і контролером, зокрема коли контролер є органом публічної влади і, тому, малоймовірно, що згоду було надано добровільно за усіх обставин такої спеціальної ситуації. Презумпція ненадання добровільної згоди виникає у разі відсутності окремого дозволу на здійснення різних операцій опрацювання персональних даних, незважаючи на її відповідність окремому випадку, або, якщо виконання договору, в тому числі, надання послуги, залежить від надання згоди, незважаючи на те, що така згода не є обов'язковою для такого виконання.»[41]

[39] Закон України «Про захист персональних даних»: Верховна Рада України; Закон від 01.06.2010 № 2297-VI // Відомості Верховної Ради України. – 2010. – № 34. – с.481.

[40] Роз'яснення основних положень Порядку повідомлення Уповноваженого щодо визначення обробки персональних даних, яка становить особливий ризик для прав і свобод суб'єктів персональних даних : Уповноважений Верховної Ради України з прав людини; Роз'яснення від 08.01.2014 [Електронний ресурс]. – Режим доступу: https://zakon.rada.gov.ua/laws/show/n0003715-14#Text

[41] Регламент Європейського Парламенту і Ради (ЄС) 2016/679 від 27 квітня 2016 року про захист фізичних осіб у зв'язку з опрацюванням персональних даних і про вільний рух таких даних, та про скасування Директиви 95/46/ЄС (Загальний регламент про захист даних). Офіційний вісник Європейського Союзу L 119/1 від 04.05.2016 (офіційний переклад).

Саме тому, ми погоджуємось з критикою Кохановської О.В. щодо правомірності надання згоди через так звані «договори про приєднання», оскільки це унеможливлює право особи власноруч вносити зміни у зміст договору та, відповідно, може спричинити чимало зловживань.[42]

Поінформованість ж полягає в тому, щоб особа була належним чином ознайомлена з повною та достовірною інформацію як саме і ким її персональні дані будуть оброблятись, а також з правами, визначеними в ст.8 Закону України «Про захист персональних даних». Як зазначає в Роз'ясненнях Уповноважений ВР, «під інформованою згодою на обробку персональних даних варто розуміти добровільне, компетентне прийняття особою рішення про обробку її персональних даних, яке ґрунтується на одержанні нею повної, об'єктивної і всебічної інформації стосовно майбутньої обробки персональних даних.»[43] Уповноважений ВР ускладнив визначення «інформованості», додавши до нього вимогу добровільності, однак, на нашу думку, попри те, що вказані категорії перебувають у тісному взаємозв'язку, добровільність має безпосереднє відношення до вільного волевиявлення, тоді як інформованість полягає в повній обізнаності як саме, ким та з якою метою персональні дані особи підлягатимуть обробці.

Стосовно форми – закон визначає вимогу, щоб така давала змогу зробити висновок про надання згоди. Необхідно розуміти, що обов'язок доведення наявності добровільної та інформованої згоди лежить на володільцю даних, а тому надання згоди лише в усній формі або шляхом конклюдентних дій викликає труднощі в доведенні правомірності обробки даних. Тому, за загальним правилом, згода надається в письмовій чи електронній формі, часто шляхом укладення окремого документа – «згоди на обробку персональних даних». Хоча письмова або електронна форма згоди не єдиний можливий законний варіант. Достатньо, щоб така форма давала змогу зробити

[42] Кохановська О.В. До питання про захист персональних даних в Україні // Вісник Верховного Суду України. - 2011. - № 6. - С. 28-33. URL: http://nbuv.gov.ua/UJRN/vvsu_2011_6_8.

[43] Роз'яснення до Типового порядку обробки персональних даних: Уповноважений Верховної Ради з прав людини, 08.01.2014. База даних «Законодавство України»/ВР України. Режим доступу: https://zakon.rada.gov.ua/laws/show/n0001715-14#Text

недвозначний висновок про надання згоди, а володілець персональних даних міг довести наявність такої згоди протягом всього часу обробки даних.

Для згоди на обробку персональних даних з «чутливою» обробкою, в тому числі, медичних, законодавець закріпив додатковий критерій - однозначність. Як зазначає Бєлова Ю., така згода «повинна бути явно вираженою, зрозумілою та безсумнівною»[44].

Така позиція корелюється із положеннями п.11 ст.4 Регламенту 2016/679 (GDPR), в якому зазначено: «згода суб'єкта даних означає будь-яке вільно надане, конкретне, поінформоване та однозначне зазначення бажань суб'єкта даних, яким він або вона, шляхом оформлення заяви чи проявом чітких ствердних дій, підтверджує згоду на опрацювання своїх персональних даних».[45] Примітно, що окрім вже названих критеріїв, GDPR висуває нову вимогу – конкретність. Так, відповідно до ч.1 ст. 6 Регламенту, однією із умов правомірності опрацювання (обробки даних) є надання суб'єктом даних згоди на опрацювання своїх персональних, в тому числі медичних, даних для однієї чи декількох спеціальних цілей.[46] Відповідно, для кожної чітко визначеної цілі обробки є необхідною окрема згода суб'єкта даних. Конкретність безпосередньо пов'язана з метою обробки, і в українському законодавстві опосередковано випливає з принципу «конкретизації мети» (див. п.2.1 нашої праці). Окремо варто наголосити на ч.1. ст. 7 Регламенту, в якій на контролера (в українському законодавстві вказаний термін еквівалентний поняттю «володілець») покладено обов'язок бути спроможним довести те, що суб'єкт даних справді надав згоду на опрацювання своїх персональних даних.[47] Вважаємо за необхідне закріпити аналогічне положення і в українському законодавстві.

---

[44] Бєлова Ю. Умови дійсності згоди на обробку персональних даних / Ю. Бєлова // Підприємництво, господарство і право. — 2017. —№ 11. — Р. 14–18.

[45] Регламент Європейського Парламенту і Ради (ЄС) 2016/679 від 27 квітня 2016 року про захист фізичних осіб у зв'язку з опрацюванням персональних даних і про вільний рух таких даних, та про скасування Директиви 95/46/ЄС (Загальний регламент про захист даних). Офіційний вісник Європейського Союзу L 119/1 від 04.05.2016 (офіційний переклад).

[46] Там само.

[47] Там само.

Значний пласт обробки медичних даних складає діяльність з персональними даними в сфері охорони здоров'я. Варто відзначити, що в законодавстві існує дисонанс щодо необхідності отримання згоди в цілях охорони здоров'я медичним працівником або іншою особою закладу охорони здоров'я чи фізичною особою - підприємцем, яка одержала ліцензію на провадження господарської діяльності з медичної практики, та її працівниками в Законі України «Про державні фінансові гарантії медичного обслуговування населення», Порядку №411 та в Законі України «Про захист персональних даних», адже останнім передбачена відсутність обов'язку одержання згоди в конкретних цілях (про це детальніше в пп.2.1.).

Повідомлення суб'єкта даних про збирання його персональних даних та про їх передачу третім особам

Навіть у випадках, коли згода на обробку медичних даних не вимагається законом (в цілях охорони здоров'я та в інших випадках, про які ми зазначаємо в пп. 2.1 нашої роботи) законодавчо передбачений обов'язок володільця персональних даних (у сфері охорони здоров'я – медичного закладу або ФОП, яка одержала ліцензію на провадження господарської діяльності з медичної практики) повідомляти суб'єкта персональних даних про: - склад та зміст зібраних персональних даних;

- права суб'єкта персональних даних;
- мету збору персональних даних;
- осіб, яким передаються його персональні дані (ч.2 ст.12 Закону України «Про захист персональних даних»).[48]

Такий обов'язок повинен бути виконаний в момент збору персональних даних, якщо персональні дані збираються у суб'єкта персональних даних; та протягом тридцяти робочих днів з дня збору персональних даних - в усіх інших випадках.[49]

[48] Закон України «Про захист персональних даних»: Верховна Рада України; Закон від 01.06.2010 № 2297-VI // Відомості Верховної Ради України. – 2010. – № 34. – с.481.
[49] Там само.

Окрім обов'язку повідомлення суб'єкта даних про збирання його персональних даних, Закон окремо містить зобов'язання володільця даних протягом десяти робочих днів повідомляти про передачу таких даних третій особі, а також про кожну зміну, видалення чи знищення персональних даних або обмеження доступу до них (ст. 21 Закону України «Про захист персональних даних»).[50] При цьому, повідомлення суб'єкта даних про передачу його персональних даних третій особі не здійснюються, якщо такий обов'язок вже був виконаний володільцем відповідно до вимог ч.2 ст. 12 Закону України «Про захист персональних даних», а також у випадку передачі персональних даних за запитами при виконанні завдань оперативно-розшукової чи контррозвідувальної діяльності, боротьби з тероризмом; виконання органами державної влади та органами місцевого самоврядування своїх повноважень, передбачених законом або ж здійснення обробки персональних даних в історичних, статистичних чи наукових цілях.[51] Форма повідомлення законодавчо не визначена, однак на нашу думку, задля уникнення зловживань доцільно повідомляти суб'єкта персональних даних у письмовій формі.

Існують численні порушення наведеного механізму охорони персональних даних. За результатами проведеного дослідження, понад 75% веб-сайтів з українськими доменами, попри обробку персональних даних, не надають суб'єктам даних навіть інформації про найменування володільця їхніх персональних даних.[52] На нашу думку, причиною таких разючих правопорушень є, насамперед, не чітке законодавче формулювання, оскільки на практиці повідомляти суб'єкта даних про кожен факт збирання або ж кожної зміни персональних даних є доволі проблематично, а закон не містить жодних винятків. Іншою ж причиною, на нашу думку, є безкарність та труднощі в притягненні до відповідальності правопорушників у сфері захисту персональних даних (про це детальніше в пп.3.3).

---

[50] Закон України «Про захист персональних даних»: Верховна Рада України; Закон від 01.06.2010 № 2297-VI // Відомості Верховної Ради України. – 2010. – № 34. – с.481.

[51] Там само.

[52] Гуйван П.Д. Юридичне обґрунтування електронної обробки персональних даних. Актуальні проблеми вітчизняної юриспруденції № 6. Том 1.- 2018 – с. 92-96.

Письмове повідомлення Уповноваженого Верховної Ради України з прав людини про «чутливу» обробку персональних даних

Обов'язок повідомлення володільцем персональних даних Уповноваженого ВР про обробку персональних даних, яка становить особливий ризик для прав і свобод суб'єктів персональних даних, закріплений в ст. 9 Закону України «Про захист персональних даних». Законодавець встановив максимально допустимий строк здійснення такого обов'язку - протягом тридцяти робочих днів з дня початку такої обробки. Більше того, у разі зміни відомостей, що підлягають повідомленню, володілець персональних даних повинен також повідомляти про кожну із змін упродовж десяти робочих днів з дня її настання.[53]

Обов'язок повідомлення Уповноваженого ВР виникає при здійсненні володільцем будь-якого виду обробки медичних даних, за винятком якщо єдиною метою обробки персональних даних є ведення відкритого реєстру для інформування населення; для обробки окремими категоріями осіб (зокрема, громадськими об'єднаннями, професійними спілками, об'єднаннями роботодавців тощо) за умови обробки виключно персональних даних членів перелічених об'єднань, що відбувається за їх згодою; обробка зумовлена необхідністю реалізації роботодавцем-володільцем даних своїх прав та обов'язків у трудових правовідновинах.[54]

У порядку містяться обов'язкові реквізити щодо форми та порядок повідомлення Уповноваженого ВР, а також порядок оприлюднення Уповноваженим ВР отриманої інформації на офіційному веб-сайті.

На жаль, попри те, що Законом передбачена відповідальність за неповідомлення Уповноваженого ВР про обробку даних, що становить

[53] Закон України «Про захист персональних даних»: Верховна Рада України; Закон від 01.06.2010 № 2297-VI // Відомості Верховної Ради України. – 2010. – № 34. – с.481.

[54] Порядок повідомлення Уповноваженого Верховної Ради України з прав людини про обробку персональних даних, яка становить особливий ризик для прав і свобод суб'єктів персональних даних, про структурний підрозділ або відповідальну особу, що організовує роботу, пов'язану із захистом персональних даних при їх обробці, а також оприлюднення вказаної інформації: Наказ Уповноваженого Верховної Ради України з прав людини від 08.01.2014 № 1/02-14 [Електронний ресурс]. – Режим доступу: https://zakon.rada.gov.ua/laws/show/v1_02715-14#n218

особливий ризик для прав і свобод суб'єктів персональних даних в визначені Законом строки, належним чином імплементувати вказаний механізм охорони не вдалось.

Прототип вищевказаної гарантії від незаконної обробки даних передбачений в статті 20 вже не чинної Директиви 95/46/ЄС Європейського Парламенту та Ради у вигляді попередньої перевірки наглядовим органом певних операцій із обробки, визначених державами, що можуть мати певний ризик для прав і свобод суб'єктів даних.[55] Примітно, що в положеннях Директиви мова йде про попередню перевірку операцій з обробки окремих видів персональних даних наглядовим органом ще до її початку. Це справді ефективний механізм охорони від незаконної обробки чутливих даних. За підсумками такої перевірки, наглядовий орган може дозволити певні види обробки даних, заборонити їх або ж видати розпорядження щодо їх зміни.[56] Натомість, через недоречне законодавче формування, повідомлення Уповноваженого ВР відбувається вже після початку обробки даних. Саме тому, нерідко в правозастосовній практиці трапляється, що порушення (шляхом незаконної обробки) на момент повідомлення Уповноваженого ВР вже відбулось. У такому випадку, Уповноважений ВР може видати припис щодо припинення такої обробки або внесення змін. Однак, це не змінює факту того, що незаконна обробка даних вже відбулася, а отже, сформований законодавцем механізм охорони не діє.

Варто наголосити на п.3 вищезазначеної ч.3 Директиви. Зокрема, у разі прийняття законів та інших нормативно-правових актів, що передбачають певні зміни щодо операцій з обробки персональних даних, що мають певний ризик для прав і свобод суб'єктів даних, рекомендується (і є зараз поширеною європейською практикою, зокрема, згідно з ст. 36 Регламенту про попередню

[55] Директива 95/46/ ЄС Європейського Парламенту та Ради «Про захист фізичних осіб при обробці персональних даних і про вільне переміщення таких даних» від 24 жовтня 1995 року [Електронний ресурс]. – Режим доступу:https://zakon.rada.gov.ua/laws/show/994_242#Text

[56] Бем М. В., Городиський І. М., Саттон Г., Родіоненко О. М. Захист персональних даних: Правове регулювання та практичні аспекти: науково-практичний посібник. – К.: К.І.С., 2015.

консультацію з наглядовим органом[57]) проводити відповідну перевірку ще до завершення процесу нормотворення.[58] Натомість, на жаль, не є рідкістю несистематизоване внесення змін до законодавства та, серед іншого, і суперечність новоприйнятих законів та інших нормативно-правових актів вимогам законодавства про захист персональних даних.

Також, в правозастосовній практиці часто виникають ситуації, коли володільці направляють повідомлення Уповноваженому ВР з якомога загальнішою інформацією, що унеможливлює формування конкретних висновків щодо операцій, які здійснюються ними.[59] Такі зловживання здійснюються з метою уникнути відповідальності та продовжувати незаконну обробку персональних даних, що однозначно погіршує і без того складну ситуацію з охороною на захистом чутливих, в тому числі, медичних даних. А тому рекомендуємо внести зміни до законодавства щодо повідомлення Уповноваженого ВР ще до початку обробки медичних даних, та лише за підсумками такої перевірки у випадку санкціонування Уповноваженим ВР дозволити відповідні операції щодо обробки.

Визначення відповідальної особи чи структурного підрозділу в закладі охорони здоров'я щодо обробки персональних даних

Іншим важливим механізмом охорони медичних даних є визначення відповідальної(их) особи(іб) в закладі охорони здоров'я щодо обробки медичних даних. Так, йдеться про створення згідно з ч.2 ст. 24 Закону України «Про захист персональних даних» окремого структурного підрозділу або ж визначення окремої особи, що відповідальні за впровадження механізмів

[57] Регламент Європейського Парламенту і Ради (ЄС) 2016/679 від 27 квітня 2016 року про захист фізичних осіб у зв'язку з опрацюванням персональних даних і про вільний рух таких даних, та про скасування Директиви 95/46/ЄС (Загальний регламент про захист даних). Офіційний вісник Європейського Союзу L 119/1 від 04.05.2016 (офіційний переклад).

[58] Директива 95/46/ ЄС Європейського Парламенту та Ради «Про захист фізичних осіб при обробці персональних даних і про вільне переміщення таких даних» від 24 жовтня 1995 року [Електронний ресурс]. – Режим доступу:https://zakon.rada.gov.ua/laws/show/994_242#Text

[59] Бем М. В., Городиський І. М., Саттон Г., Родіоненко О. М. Захист персональних даних: Правове регулювання та практичні аспекти: науковопрактичний посібник. – К.: К.І.С., 2015.

охорони та захисту персональних, зокрема і медичних, даних при їх обробці.[60] Така законодавча вимога стосується як органів державної влади та місцевого самоврядування, так і будь-яких інших осіб, що являються володільцями (визначають мету обробки) та розпорядниками (здійснюють обробку даних відповідно до визначеної володільцем мети) персональних даних.

На відповідальних за обробку персональних даних з дотриманням необхідних механізмів охорони та захисту осіб Закон покладає обов'язок взаємодіяти з Уповноваженим ВР та його секретаріатом щодо консультування з питань запобігання та усунення порушень, що стосуються персональних даних, а також консультування та інформування осіб, що беруть участь в обробці даних, зокрема володільця та розпорядника, щодо окремих питань додержання законодавства про захист персональних даних та ефективного забезпечення необхідних механізмів охорони та захисту. [61]

Варто наголосити, що впродовж 30 днів з моменту створення структурного підрозділу або призначення відповідальної особи така інформація підлягає повідомленню Уповноваженому ВР.[62] Останній, своєю чергою, зобов'язаний оприлюднити на офіційному веб-сайті Уповноваженого отримані дані в окремому розділі «Інформація про структурний підрозділ або відповідальну особу, що організовує роботу, пов'язану із захистом персональних даних при їх обробці».[63] Після того, як обробка чутливих персональних даних завершилась, володілець повинен надіслати повідомлення про припинення обробки такої категорії даних. Як наслідок, на Уповноваженого ВР покладається обов'язок стосовно видалення опублікованої інформації з офіційного веб-сайту.[64]

Вказану гарантію можна віднести, одночасно, як до механізму охорони, так і захисту. Оскільки після визначення в медичному закладі відповідальної

[60] Закон України «Про захист персональних даних»: Верховна Рада України; Закон від 01.06.2010 № 2297-VI // Відомості Верховної Ради України. – 2010. – № 34. – с.481.
[61] Закон України «Про захист персональних даних»: Верховна Рада України; Закон від 01.06.2010 № 2297-VI // Відомості Верховної Ради України. – 2010. – № 34. – с.481.
[62] Там само.
[63] Там само.
[64] Там само.

особи або структурного підрозділу (спосіб охорони персональних даних), у разі виявлення ним (нею) актів порушень процесу обробки медичних даних, вони підлягають документальній фіксації ним (нею) та повідомленню, відповідно, Уповноваженого Верховної Ради України з прав людини.

Доцільним є, на нашу думку, деталізувати в законі завдання та повноваження відповідальної особи чи структурного підрозділу щодо обробки персональних даних, а також законодавчо визначити необхідні вимоги, що ставляться до таких осіб, насамперед, щодо наявності освіти, пов'язаної із захистом персональним даних.

Положення про обробку персональних даних на локальному рівні

У Законі України «Про захист персональних даних» та Типовому порядку обробки персональних даних, затвердженому наказом Уповноваженого ВР від 08.01.2014 № 1/02–14 визначено мінімально допустимі вимоги до володільців щодо охорони та захисту персональної інформації суб'єкта даних. Варто наголосити, що на локальному рівні закладу або ФОП, яка одержала ліцензію на провадження господарської діяльності з медичної практики, можуть встановлювати значно ширший перелік гарантій щодо обробки та захисту персональних даних. Кожен володілець повинен вживати всіх заходів від нього залежних для запобігання незаконній обробці даних, опираючись на специфіку його роботи (однак, не менше, ніж передбачено в Законі та Типовому порядку обробки).

Захист

Як визначено в п. 3.3. Типового порядку обробки персональних даних, затвердженого наказом Уповноваженого ВР від 08.01.2014 № 1/02–14, захист персональних даних передбачає «заходи, спрямовані на запобігання їх випадкових втрати або знищення, незаконної обробки, у тому числі незаконного знищення чи доступу до персональних даних».[65] Таким чином, увага Уповноваженого ВР акцентується саме на превентивній функції захисту – задля

[65] Типовий порядок обробки персональних даних, затверджений наказом Уповноваженого від 08.01.2014 № 1/02–14 [Електронний ресурс]. – Режим доступу: https://zakon.rada.gov.ua/laws/show/v1_02715-14#Text

запобігання порушення охоронюваного законом права. Ми цілком підтримуємо вказану позицію, зважаючи на виняткову важливість недопущення незаконної обробки, в тому числі, розголошення втрати медичних даних. Однак, наголошуємо, що значним пластом заходів із захисту є саме відновлення порушеного права.

Загалом, захист персональних даних, зокрема, медичних, можна поділити на 2 групи заходів. Перші – є превентивними і безпосередньо випливають із обов'язку володільця медичних даних здійснювати організаційні та технічні заходи з метою запобігання їх випадкової втрати або знищення, незаконної обробки, а також обов'язку розпорядників даних дотримуватись політики конфіденційності. Друга група заходів має на меті відновлення вже порушеного права.

Вичерпно наведено перелік необхідних для встановлення на локальному рівні організаційних та технічних заходів для захисту медичних даних у Рекомендації Комітету Міністрів Ради Європи R (97) 5, які зокрема можна поділити на такі групи: 1) контроль за доступом до обладнання; 2) контроль за даними; 3) управління пам'яттю; 4) контроль за використанням; 5) обмеження доступу до інформації; 6) контроль за нерозголошенням; 7) контроль за введенням даних; 8) контроль за передачею даних; 9) контроль за наявністю.[66]

Вважаємо, що необхідно розмежовувати організаційні заходи та технічні. Перші – мають на меті забезпечення такої упорядкованої діяльності людей, що унеможливить незаконне розкриття або ж порушення недоторканності персональних даних. Технічні ж заходи передбачають роботу, пов'язану з технікою задля реалізації такої ж мети – убезпечення від правовопорушень інформаційних прав суб'єктів даних.

В Типовому порядку обробки серед організаційних заходів слід відмітити визначення окремого обліку працівників, що мають доступ до персональних даних суб'єктів; визначення різних рівнів доступу працівників

[66] Recommendation on the Protection of Medical Data: Council of Europe, Committee of Ministers; Feb. 13, 1997. № R (97) 5 [Електронний ресурс]. – Режим доступу : http://hrlibrary.umn.edu/instree/coerecr97-5.html

задля забезпечення доступу кожного працівника лише з тією інформацією, яка є необхідною для нього/неї у зв'язку з виконанням своїх службових, трудових чи професійних обов'язків; письмове зобов'язання осіб, які наділені доступом до відповідних персональних даних в силу виконання своїх професійних, службових або трудових обов'язків, про нерозголошення такої інформації; обов'язкове ведення обліку операцій щодо обробки персональних даних суб'єкта та доступом до них; планування дій на випадок виникнення надзвичайних ситуацій, несанкціонованого розкриття персональних даних, пошкодження технічного обладнання; регулярне навчання співробітників, що мають доступ до персональних даних. [67] Серед спеціальних технічних заходів, Уповноважений ВР окремо зазначає «виключення несанкціонованого доступу до персональних даних, що обробляються та роботі технічного та програмного комплексу, за допомогою якого здійснюється обробка персональних даних»[68].

Примітно, що першим організаційним заходом, загальним для усіх володільців є облік та визначення різного рівня доступу до персональних даних суб'єктів. Кожен із працівників закладу охорони здоров'я/ФОП як володільця медичних даних пацієнтів повинен мати доступ лише до тих даних, які є необхідними для виконання його професійних чи службових або трудових обов'язків (і не більше). Такий захід необхідний, щоб мінімізувати коло суб'єктів, які можуть бути причетними до незаконної обробки, в тому числі розголошення конфіденційної інформації, її втрати чи видалення. Ведення обліку (не лише працівників, що мають доступ до персональних даних суб'єкта, але й обліку операцій, пов'язаних з обробкою персональних даних суб'єкта з зазначенням дати, часу, джерела збирання персональних даних суб'єкта, виду обробки, її мету та підстави, конкретного працівника, який здійснював обробку) має надважливе значення оскільки суб'єкт персональних даних має право на доступ до своїх персональних, в тому числі медичних, даних (ч.2 ст.8 Закону

[67] Типовий порядок обробки персональних даних, затверджений наказом Уповноваженого Верховної Ради з прав людини від 08.01.2014 № 1/02–14.
[68] Там само.

України «Про захист персональних даних»)[69], а отже, уповноважений знати хто саме і коли обробляв його медичні дані. Варто погодитись з Бем М. В., Городиським І. М., Саттоном Г. та іншими, що право особи на захист власних прав не матиме юридичного значення, якщо неможливо буде встановити ким, коли, у який спосіб оброблялися та кому передавалися його персональні дані.[70]

Такі положення узгоджуються з поширеною європейською практикою «приватність за задумом» (“privacy by design”), «приватність за замовчуванням» (“privacy by default”), та принципом мінімізації даних (“data minimization”). Так, відповідно до ч.2 ст.25 Загального регламенту,

«контролер повинен вжити відповідних технічних і організаційних заходів для гарантування того, що за замовчуванням опрацьовують лише ті персональні дані, які є необхідними для кожної спеціальної цілі опрацювання. Такий обов’язок застосовують до кількості зібраних персональних даних, ступеня їхнього опрацювання, періоду їхнього зберігання та їхньої доступності. Зокрема, такими заходами необхідно гарантувати ненадання за замовчуванням доступу до персональних даних без звернення особи до невизначеної кількості фізичних осіб»[71].

Тобто, володілець повинен вживати всіх можливих організаційних та технічних заходів ще до початку обробки відповідної інформації, ще на етапі проектування бізнес-процесів (наприклад, розробки системи e-health) для того, щоб унеможливити подальше незаконне розкриття інформації та продовжувати застосовувати ефективні заходи на кожному етапі для обробки лише тих персональні дані, які є необхідними для кожної конкретної мети. Тісно пов’язаний з останнім принцип “privacy by default”, який полягає в тому, що суб’єкт даних у таких правовідносинах не зобов’язаний вживати жодних заходів для забезпечення конфіденційності власних медичних даних, такий обов’язок лежить саме на володільцю інформації, і саме на нього покладаються додаткові

[69] Закон України «Про захист персональних даних»: Верховна Рада України; Закон від 01.06.2010 № 2297-VI // Відомості Верховної Ради України. – 2010. – № 34. – с.481.

[70] Бем М. В., Городиський І. М., Саттон Г., Родіоненко О. М. Захист персональних даних: Правове регулювання та практичні аспекти: науково-практичний посібник. – К.: К.І.С., 2015. – 220 с. Електронний доступ : https://rm.coe.int/168059920c

[71] Регламент Європейського Парламенту і Ради (ЄС) 2016/679 від 27 квітня 2016 року про захист фізичних осіб у зв’язку з опрацюванням персональних даних і про вільний рух таких даних, та про скасування Директиви 95/46/ЄС (Загальний регламент про захист даних). Офіційний вісник Європейського Союзу L 119/1 від 04.05.2016 (офіційний переклад).

труднощі, наприклад, у вигляді необхідності доведення отримання згоди суб'єкта даних на обробку медичних даних з конкретною метою.

Яскравим прикладом важливості дотримання належних гарантій стосовно визначення порядку доступу до персональних даних працівників є справа «І проти Фінляндії» (№ 20511/03). Заявниця, яка працювала медсестрою в інфекційній лікарні, проходила лікування на СНІД у цьому ж медичному закладі. Після виявлення факту розголошення своїх медичних даних, заявниця звернулася із скаргою до адміністративного органу, в якій просила встановити, хто і коли мав доступ до її медичної документації, а згодом і до суду через нездатність медичного закладу забезпечити захист її персональних даних від несанкціонованого доступу. У задоволенні скарги заявниці відмовили, пояснюючи це відсутністю доказів того, що інформацію було незаконно переглянуто, оскільки відповідна система обробки не передбачала облік операцій стосовно обробки медичної інформації конкретної особи, кожен із працівників мав доступ до медичних записів пацієнтів. ЄСПЛ встановив, що суди відмовили у задоволенні позовних вимог заявниці через неможливість доведення причинно-наслідкового зв'язку між недоліками системи безпеки медичного закладу щодо доступу до медичних даних та незаконним розголошенням персональної інформації. Однак, суд зазначив при цьому, що покладати на заявницю такий тягар доказування означало б ігнорування недоліків зберігання та доступу до медичної документації в лікарні в той час. Суд наголосив, що вирішальним фактором є те, що система зберігання у лікарні явно не відповідала вимогам закону. І хоча адміністрація медичного закладу згодом прийняла спеціальні заходи для захисту заявниці від несанкціонованого розкриття інформації обмеживши доступ до неї лише лікуючим персоналом, а також зареєструвавши заявницю під вигаданим ім'ям і номером соціального страхування, такі заходи були прийняті надто пізно оскільки незаконна обробка

медичних даних заявниці вже відбулась. Таким чином, Суд констатував порушення статті 8 Конвенції.[72]

При цьому, медичні працівники та інші особи, яким надано доступ до медичних даних суб'єкта даних у зв'язку з виконанням професійних, службових чи трудових обов'язків, повинні підписати письмове зобов'язання про нерозголошення медичної таємниці. Лише після виконання такого обов'язку, працівник вважається формально допущеним до персональних даних. Вказане положення є спеціальною нормою щодо закріпленого у п. «г» ч. 1 ст. 78 Закону України «Основи законодавства України про охорону здоров'я» обов'язку медичного працівника зберігати лікарську таємницю.

Як бачимо, володільці персональних даних (в сфері охорони здоров'я - заклади охорони здоров'я/ФОПи, які одержали ліцензію на провадження господарської діяльності з медичної практики) повинні здійснити всіх можливих від них дій для захисту персональних даних, в тому числі і шляхом імплементації на локальному рівні передбачених законом організаційних і технічних заходів.

Щодо недоліків національного законодавства, варто зазначити, що попри закріплення обов'язку повідомлення володільцем персональних даних Уповноваженого ВР про обробку чутливих персональних даних (ст. 9 Закону України «Про захист персональних даних») та «розмитого» обов'язку володільців, розпорядників персональних даних та третіх осіб забезпечити захист даних від випадкових втрати або знищення, від незаконної обробки (ст. 24 вищенаведеного Закону), Закон не регламентує поведінку суб'єктів персональних даних у разі порушень. Зокрема, в Законі України «Про захист персональних даних» немає закріплено обов'язку володільців, розпорядників та третіх осіб повідомити уповноважений орган про витік персональних даних. Це часто має наслідком неможливість відкриття адміністративного провадження у

[72] Рішення Європейського суду з прав людини від 17.10.2008 року у справі «I проти Фінляндії»» (заява № 20511/03) [Електронний ресурс]. – Режим доступу: http://hudoc.echr.coe.int/eng?i=001-87510.

зв'язку з обмеженими строками притягнення до відповідальності (протягом 3 місяців з дня вчинення – п.3.3 роботи).

Так, у разі неуспішності превентивної функції захисту персональних даних, настає необхідність у **відновленні порушеного охоронюваного законом права.**

Суб'єкт даних, виявивши порушення свого права у сфері захисту персональних, зокрема, медичних, даних (п.3.1-3.2 роботи), має право звернутися до Уповноваженого ВР або ж до суду. Також доцільним є направлення вмотивованої вимоги розпоряднику даних про необхідність припинення правопорушення одразу ж після виявлення такого.

Уповноважений ВР є однією з двох ключових інституцій (поряд з судом), на яку покладено контроль за дотриманням законодавства про захист персональних даних. Відповідно до ст. 23 Закону України «Про захист персональних даних», п.2.1 Порядку здійснення Уповноваженим ВР контролю за додержанням законодавства про захист персональних даних, Уповноважений ВР та/або уповноважені ним посадові особи, з метою виконання покладених на нього повноважень, здійснюють проведення планових, позапланових, виїзних та безвиїзних перевірок.[73]

У разі виявлення порушення свого права, звернення суб'єкта даних до Уповноваженого ВР зі скаргою буде підставою для позапланової перевірки володільця персональних даних на факт порушення ним законодавства про захист персональних даних. При цьому, звернення до Уповноваженого ВР має ґрунтуватися на фактичних обставинах, які повинні бути підтвердженими належними доказами. Зазначимо, що Уповноважений ВР має право проводити позапланові перевірки суб'єктів господарювання і за власною ініціативою, однак за наявності передбачених законом підстав.

[73] Порядок здійснення Уповноваженим Верховної Ради України з прав людини контролю за додержанням законодавства про захист персональних даних, затверджений Наказом Наказ Уповноваженого Верховної Ради України з прав людини від 08.01.2014 № 1/02-14. [Електронний ресурс]. – Режим доступу: https://zakon.rada.gov.ua/laws/show/v1_02715-14#Text.

Відповідно до п. 5.1 Порядку № 1/02-14, за результатами здійснення планової або позапланової перевірки Уповноважений ВР та/або уповноважена посадова особа складає акт перевірки додержання вимог законодавства про захист персональних даних, в якому містяться, серед іншого, факти (обставини), які встановлено за результатами перевірки, та висновок про результати перевірки (відсутність або наявність порушень законодавства про захист персональних даних).[74] У випадку виявлення правопорушення в результаті перевірки Уповноваженим ВР або ж безпосередньо на підставі обґрутованого та підтвердженого належними доказами звернення громадян, наступним кроком може бути винесення припису з метою припинення порушення або за наявності складу адміністративного правопорушення, передбаченого ст.188–39 КУпАП (п.3.2 нашої роботи), складення адміністративного протоколу та направлення його до суду. При цьому, за невиконання припису, як заходу реагування, що є обов'язковою до виконання вимогою, правопорушник нестиме відповідальність за ч.2 ст.188–39 КУпАП. Таким чином, володілець даних може двічі або тричі порушити законодавство, до того як буде притягнутим до адміністративної відповідальності, що на нашу думку, не є ефективним захистом персональних даних.

Хочемо наголосити на низькій ефективності притягнення до адміністративної відповідальності зі сторони Уповноваженого ВР, оскільки згідно з даними Єдиного державного реєстру судових рішень за 2019 рік (01.01.2019-01.01.2020) направлено до суду лише 10 протоколів про адміністративне правопорушення за ч.4 ст. 188-39 КУпАП. Згідно з даними щорічної доповіді Уповноваженого ВР про стан додержання та захисту прав і свобод людини і громадянина в Україні за 2019 рік, у другій половині 2019 року Уповноваженим ВР розпочато низку перевірок дотримання права на приватність під час функціонування електронної системи охорони здоров'я, за

[74] Порядок здійснення Уповноваженим Верховної Ради України з прав людини контролю за додержанням законодавства про захист персональних даних, затверджений Наказом Наказ Уповноваженого Верховної Ради України з прав людини від 08.01.2014 № 1/02-14. [Електронний ресурс]. – Режим доступу: https://zakon.rada.gov.ua/laws/show/v1_02715-14#Text

результатами яких *видано 3 приписи та надано рекомендації в 9 актах реагування* щодо належного виконання вимог законодавства в сфері захисту персональних даних.[75] Вищевказане можна пояснити малою чисельністю штатних працівників в Департаменті у сфері захисту персональних даних Секретаріату Уповноваженого ВР, що, на нашу думку, потребує законодавчих змін.

Висновки до розділу 1

1. Запропоновано авторське визначення поняття «медичні дані», а саме це: інформація про стан здоров'я пацієнта(ки), його/її діагноз, історію його/її хвороби, про запропоновані дослідження і лікувальні заходи, прогноз можливого розвитку захворювання, інші дані, які безпосередньо пов'язані із станом здоров'я пацієнта(ки) та процесом надання йому/їй медичної допомоги, а також, його/її генетичні дані.

2. До особливостей медичних даних належать поширення на них законодавства про захист персональних даних; «чутливість» їх обробки та конфіденційність за замовчуванням.

3. Медичні дані є особливою категорією персональних даних та, з огляду на віднесення їх обробки до такої, що становить особливий ризик для прав і свобод, потребують додаткових механізмів охорони та захисту. До механізмів охорони зачисляємо: 1) наявність однозначної, добровільної, поінформованої згоди суб'єкта даних на обробку його/її даних, поданої в формі, що дозволяє дійти висновку про її надання (окрім випадків, коли згода на обробку персональних даних не потребується, в тому числі, в цілях охорони здоров'я); 2) обов'язок володільця медичних даних повідомляти суб'єкта даних про збирання його персональних даних, про їх передачу третім особам та інші дії (про кожну зміну, видалення чи знищення персональних даних або обмеження доступу до них); 3) обов'язок

[75] Щорічна доповідь Уповноваженого Верховної Ради України з прав людини про стан додержання та захисту прав і свобод людини і громадянина в Україні за 2019 рік. [Електронний ресурс]. – Режим доступу: https://dpsu.gov.ua/upload/zvit_za_2019.pdf

повідомлення Уповноваженого Верховної Ради України з прав людини про обробку медичних даних; 4) визначення відповідальної(их) особи(іб) в закладі охорони здоров'я щодо обробки медичних даних; 5) положення про обробку персональних даних на локальному рівні.

4. Механізми захисту медичних даних можна поділити на 2 групи заходів. Перші є превентивними і безпосередньо випливають із обов'язку володільця медичних даних здійснювати організаційні та технічні заходи з метою запобігання їх випадкової втрати або знищення, незаконної обробки. Друга група заходів має на меті відновлення вже порушеного права через діяльність Уповноваженого Верховної Ради України з прав людини або суду.

5. Пропонуємо внести зміни до законодавства шляхом: 1) доповнення вимоги «конкретності» до згоди на обробку персональних, у тому числі медичних, даних; 2) усунення дисонансу в нормативно-правових актах щодо необхідності одержання згоди для обробки медичних даних в цілях охорони здоров'я, відповідно до вимог п.6 ч.2. ст. 7 Закону України «Про захист персональних даних»; 3) змін до встановлених строків виконання обов'язку повідомлення володільцем персональних даних Уповноваженого Верховної Ради України з прав людини про обробку медичних даних, а саме встановлення таких ще до початку обробки чутливих персональних даних; 4) деталізації завдань, повноважень відповідальної особи чи структурного підрозділу щодо обробки персональних, у тому числі медичних, даних, а також визначення необхідних кваліфікаційних вимог щодо таких осіб.

РОЗДІЛ 2. Обробка медичних даних і права людини.

2.1. Обробка медичних даних (порівняння законодавства України та ЄС).

Відповідно до статті 2 Закону України «Про захист персональних даних», обробка персональних даних – це «будь-яка дія або сукупність дій, таких як збирання, реєстрація, накопичення, зберігання, адаптування, зміна, поновлення, використання і поширення (розповсюдження, реалізація, передача), знеособлення, знищення персональних даних, у тому числі з використанням інформаційних (автоматизованих) систем».[76] В оновленій версії статті 2b, 2c Конвенції 108 (відповідно до внесених змін протоколом CETS № 223 від травня 2018 року) міститься аналогічне визначення, а саме – «будь-яка операція або набір операцій, що виконуються з персональними даними, такі як збір, зберігання, консервація, зміна, пошук, розкриття, надання доступності, видалення, знищення або виконання логічних та / або арифметичних операцій із такими даними. Коли автоматизована обробка не використовується, «обробка даних» означає операцію або набір операцій, що виконуються над персональними даними в рамках структурованого набору таких даних, які є доступними або відновними за певними критеріями».[77]

Варто зазначити, що в Законі «Про захист персональних даних» існує колізія щодо співвідношення понять «обробка», «використання» та «захист». Зокрема, в ч.1 ст. 10 Закону до використання, з-поміж іншого, віднесено дії щодо захисту персональних даних[78]. Водночас, в ст. 2 Закону у визначенні поняття «обробка персональних даних» законодавець обґрунтовано, на нашу думку, одним із її елементів закріпив «використання», натомість «захисту» там немає.[79]

---

[76] Закон України «Про захист персональних даних»: Верховна Рада України; Закон від 01.06.2010 № 2297-VI // Відомості Верховної Ради України. – 2010. – № 34. – с.481.

[77] Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data Strasbourg, 10.X.2018 [Електронний ресурс]. – Режим доступу: https://rm.coe.int/16808ac918.

[78] Закон України «Про захист персональних даних»: Верховна Рада України; Закон від 01.06.2010 № 2297-VI // Відомості Верховної Ради України. – 2010. – № 34. – с.481.

[79] Там само.

Необхідно погодитись з Бемом М. В., Городиським І. М., Саттоном Г. та іншими стосовно того, що захист персональних даних слід відмежовувати від обробки, оскільки такий не передбачає вчинення окремих дій з персональними даними, а тому є окремою категорією, яку необхідно відмежовувати від поняття їх «обробки» та «використання». Натомість, «використання» доцільно розглядати як один із видів «обробки» персональних даних.[80]

Ключовим питанням є підстави обробки медичних даних. В ст. 32 Конституції України зазначено:

«Ніхто не може зазнавати втручання в його особисте і сімейне життя, крім випадків, передбачених Конституцією України.

Не допускається збирання, зберігання, використання та поширення конфіденційної інформації про особу без її згоди, крім випадків, визначених законом, і лише в інтересах національної безпеки, економічного добробуту та прав людини.»[81]

Аналізуючи вищенаведені положення Основного Закону, можна дійти висновку, що збирання, зберігання, використання поширення та будь-який інший вид обробки персональних даних про особу можливий лише на підставі її згоди або в випадках, чітко окреслених в законі та лише в інтересах національної безпеки, економічного добробуту та прав людини. Аналогічне положення (за винятком пропуску необхідної мети) передбачено в п. 2.7 Типового порядку обробки даних, відповідно до якого обробка персональних даних здійснюється володільцем персональних даних лише за згодою суб'єкта персональних даних, за винятком тих випадків, коли така згода не вимагається Законом.[82] Варто зазначити, що володільцем медичних даних у сфері охорони здоров'я є, зокрема, заклад охорони здоров'я чи фізична особа - підприємець, яка одержала ліцензію на провадження господарської діяльності з медичної практики.

---

[80] Бем М. В., Городиський І. М., Саттон Г., Родіоненко О. М. Захист персональних даних: Правове регулювання та практичні аспекти: науково-практичний посібник. – К.: К.І.С., 2015. – 220 с. Електронний доступ : https://rm.coe.int/168059920c.

[81] Конституція України: Верховна Рада України; Закон від 28.06.1996 р. № 254к/96-ВР // Відомості Верховної Ради України. – 1996. – № 30. – с.141.

[82] Типовий порядок обробки персональних даних, затверджений наказом Уповноваженого від 08.01.2014 № 1/02–14 [Електронний ресурс]. – Режим доступу: https://zakon.rada.gov.ua/laws/show/v1_02715-14#Text

Винятки, коли отримання згоди суб'єкта персональних даних не потребується чітко визначені законом. Зокрема, в ст. 11 (де наведено загальні підстави обробки персональних даних) та в ч.2 ст. 7 Закону України «Про захист персональних даних» (де закріплені дещо суворіші вимоги до обробки «чутливих» даних»). Так, обробка медичних даних як різновиду «чутливих» даних, за загальним правилом, є забороненою (ч.1 ст.7 Закону)[83]. Однак, така заборона не застосовується у випадках, визначених в ч.2. ст.7 Закону. Зокрема, якщо обробка персональних даних:

«1) здійснюється за умови надання суб'єктом персональних даних ***однозначної згоди*** на обробку таких даних;

2) необхідна для здійснення прав та ***виконання обов'язків володільця у сфері трудових правовідносин відповідно до закону із забезпеченням відповідного захисту***;

(…)

6) ***необхідна в цілях охорони здоров'я,*** встановлення медичного діагнозу, для забезпечення піклування чи лікування або надання медичних послуг, ***функціонування електронної системи охорони здоров'я*** за умови, що такі дані ***обробляються медичним працівником або іншою особою закладу охорони здоров'я чи фізичною особою - підприємцем, яка одержала ліцензію на провадження господарської діяльності з медичної практики, та її працівниками, на яких покладено обов'язки щодо забезпечення захисту персональних даних та на яких поширюється дія законодавства про лікарську таємницю***, працівниками центрального органу виконавчої влади, що реалізує державну політику у сфері державних фінансових гарантій медичного обслуговування населення, на яких покладено обов'язки щодо забезпечення захисту персональних даних.»[84]

Хочемо окремо наголосити на вищевикладеному п.6 ч.2. ст. 7 Закону. До набрання чинності (30.01.2018 року) редакції Закону України «Про захист персональних даних» від 19.10.2017 №2168-VIII, заклади охорони здоров'я та фізичні особи - підприємці, які одержали ліцензію на провадження господарської діяльності з медичної практики потребували отримання окремої згоди суб'єкта персональних даних на внесення медичних даних до електронної системи охорони здоров'я.

Зокрема, у справі № 127/2999/1, Вінницький апеляційний суд, обґрунтовано, на нашу думку, дійшов до висновку про необхідність видалення

[83] Закон України «Про захист персональних даних»: Верховна Рада України; Закон від 01.06.2010 № 2297-VI // Відомості Верховної Ради України. – 2010. – № 34. – с.481.

[84] Там само.

медичних даних позивача оскільки згоди позивача (суб'єкта персональних даних) на внесення її медичних даних до електронного реєстру в період з 03.06.2015 до 18.04.2017 не було. Відповідно до п.5 чинного на період спірних правовідносин Положення про електронний реєстр пацієнтів, затвердженого постановою Кабінету Міністрів України від 06.06.2012 №546, збір, обробка та внесення до реєстру даних про пацієнта здійснювалась виключно за його згодою (п.5 Положення).[85]

Однак, із набранням чинності нової редакції ст. 7 Закону України «Про захист персональних даних» та, відповідно, скасуванням МОЗ України форми «Інформована добровільна згода пацієнта на обробку персональних даних» (Наказ Міністерства охорони здоров'я України від 8 серпня 2014 р. № 549), а також вилученням п. 5 в Декларації про вибір лікаря, який надає первинну медичну допомогу «Збір і обробка персональних даних» в попередній редакції Наказу Міністерства охорони здоров'я України від 19.03.2018 № 503 (далі наказ МОЗ №503), в якому пацієнт надавав згоду на обробку персональних даних, ***згода на обробку медичних даних для мети, визначеної в п.6 ч.2. ст. 7 Закону не потребується***. Станом на зараз, в п.5 Декларації про вибір лікаря, який надає первинну медичну допомогу, затвердженій Наказом МОЗ № 503 у редакції наказу Міністерства охорони здоров'я України від 29 травня 2018 року № 1023, міститься графа для підпису пацієнта (законного представника) для підтвердження ним добровільного вибору лікаря, який надає первинну медичну допомогу, достовірності наданих даних та ***факту повідомлення про його/її права*** відповідно до Закону України «Про захист персональних даних», а також про мету збирання та обробки його/її персональних даних.[86] На нашу думку, чинна редакція Декларації про вибір лікаря, який надає первинну медичну

[85] Постанова Вінницького апеляційного суду від 10.12.2019 року у справі № 127/2999/19 [Електронний ресурс]. – Режим доступу: https://reyestr.court.gov.ua/Review/86324230.

[86] Наказ МОЗ України від 19.03.2018 № 503 "Про затвердження Порядку вибору лікаря, який надає первинну медичну допомогу, та форми декларації про вибір лікаря, який надає первинну медичну допомогу" [Електронний ресурс]. – Режим доступу: https://moz.gov.ua/article/ministry-mandates/nakaz-moz-ukraini-vid-19032018--503-pro-zatverdzhennja-porjadku-viboru-likarja-jakij-nadae-pervinnu-medichnu-dopomogu-ta-formi-deklaracii-pro-vibir-likarja-jakij-nadae-pervinnu-medichnu-dopomogu?preview=1

допомогу, цілком відповідає чинним вимогам Закону України «Про захист персональних даних».

Необхідно зазначити, що у зв'язку з тим, що законодавець не систематизовано вносить зміни до законодавства, існує колізія між вищенаведеними положеннями Закону України «Про захист персональних даних» та Закону України «Про державні фінансові гарантії медичного обслуговування населення». Зокрема, в ч.2 та ч.3 ст.11 останньозгаданого Закону передбачена можливість доступу до медичних даних, що знаходяться в електронній системі охорони здоров'я лише за умови отримання окремої згоди суб'єкта даних, а також необхідність надання згоди на обробку власних персональних даних при підписанні декларації про вибір лікаря. [87]

Наведені положення суперечать п.6 ч.2 ст. 7 Закону України «Про захист персональних даних», в якому законодавець закріпив можливість обробки персональних даних пацієнта (його законного представника) конкретними суб'єктами за вищенаведеної мети без отримання окремої згоди. Варто погодитись із думкою І. Сенюти, що колізія повинна вирішуватись на користь Закону України «Про захист персональних даних», оскільки він є спеціальним у зв'язку з прямою законодавчою вказівкою в ч.1 ст. 7 Закону України «Про державні фінансові гарантії медичного обслуговування населення». [88]

Не відповідають вимогам чинного законодавства про захист персональних даних і положення пп. 5 п. 8 Порядку №411, де закріплена одна з вимог щодо функціональних можливостей електронної системи охорони здоров'я, а саме забезпечувати «можливість надання пацієнтами (їх законними представниками) згоди у письмовій формі або у формі, що дає змогу зробити висновок про надання згоди, на доступ до даних про себе (про пацієнта для законних представників), що міститься в електронній системі охорони здоров'я,

[87] Закон України «Про державні фінансові гарантії медичного обслуговування населення»: Верховна Рада України; Закон від 19.10.2017 № 2168-VIII// Відомості Верховної Ради України. – 2018. – № 5. – с.31.

[88] Сенюта І. Чому надані Омбудсманом роз'яснення породжують правову невизначеність? 2020 р.[Електронний ресурс]. – Режим доступу: https://advokatpost.com/advokat-seniuta-chomu-nadani-ombudsmanom-roz-iasnennia-porodzhuiut-pravovu-nevyznachenist/?fbclid=Iw.

лікарям, третім особам».[89] У п. 30 Порядку передбачена можливість подання заяви пацієнта (його законного представника) про відкликання заяви про надання згоди на обробку персональних даних або про надання доступу третім особам до інформації, що міститься у центральній базі даних.[90] Враховуючи, що законодавство про захист персональних даних не передбачає надання згоди на обробку персональних даних, контраверсійним видається положення про відкликання такої згоди. На нашу думку, враховуючи вищенаведені положення ч.1 ст. 7 Закону України «Про державні фінансові гарантії медичного обслуговування населення», застосуванню підлягають саме положення Закону України «Про захист персональних даних».

Враховуючи вищенаведені колізії у правовому регулюванні підстав для обробки персональних, в тому числі, медичних даних, вважаємо за необхідне законодавчо систематизувати та узгодити Закон України «Про державні фінансові гарантії медичного обслуговування населення» та Порядок №411 відповідно до вимог спеціального Закону в системі захисту персональних даних, а саме – Закону України «Про захист персональних даних».

Вважаємо за необхідне наголосити на особливому режимі обробки персональних даних володільцем бази персональних даних, з яким суб`єкт персональних даних перебуває у трудових відносинах. Так, згідно з п. 2 вищенаведеної ч.2. ст.7 Закону України «Про захист персональних даних», дозволяється обробка медичних даних, яка є необхідною для здійснення прав та виконання обов'язків володільця у сфері трудових правовідносин відповідно до закону ***із забезпеченням відповідного захисту***.[91] А отже, роботодавець, як володілець персональних даних працівника, з яким укладено трудовий договір/контракт, ***має право на обробку персональних даних такого працівника без його окремої згоди***, однак лише в тій мірі, що є ***необхідною*** для

[89] Порядок функціонування електронної системи охорони здоров'я, затверджений Постановою Кабінету Міністрів України від 25.04.2018 №411. [Електронний ресурс]. – Режим доступу: https://zakon.rada.gov.ua/laws/show/411-2018-%D0%BF#Text

[90] Там само.

[91] Закон України «Про захист персональних даних»: Верховна Рада України; Закон від 01.06.2010 № 2297-VI // Відомості Верховної Ради України. – 2010. – № 34. – с.481.

здійснення прав та виконання обов'язків за конкретним трудовим договором/контрактом.

Так, в справі № 554/4546/19 Полтавський апеляційний суд в своїй постанові від 01 липня 2020 року обґрунтовано на нашу думку, відмовив в задоволенні апеляційної скарги ОСОБА_1 (працівника) на рішення Октябрського районного суду м. Полтави від 19 лютого 2020 року про відмову в задоволенні позовних вимог ОСОБА_1 до Акціонерного товариства «Полтаваобленерго» (роботодавця) та до низки медичних закладів міста Полтави про захист персональних даних, визнання дій незаконними, встановлення заборони вчиняти певні дії та стягнення моральної шкоди.[92]

Відповідно до обставин справи, встановлено, зокрема, що згідно із запитом роботодавця, а саме ПАТ «Полтаваобленерго», від 14 липня 2015 року №01-1/8731, до головного лікаря Другої міської клінічної лікарні, запитувалась інформація щодо працівника ОСОБА_1 з приводу листка непрацездатності №084355, який був наданий останнім роботодавцю, у зв`язку із тим, що в листку непрацездатності не зазначена дата, з якої ОСОБА_1 необхідно приступити до роботи, а також запитувалась інформація про знаходження ОСОБА_1 на лікуванні у медичному закладі. Вказаний запит не вимагав уточнення діагнозу, методів лікування, а стосувався лише підтвердження перебування працівника ОСОБА_1 на лікуванні у зазначеному закладі охорони здоров`я відповідно до відкритого листка непрацездатності №084355 з 03.06.2015 по 17.06.2015 р. та за період з 18.06.2015р. до часу звернення з даним запитом (14.07.2015 року). На вказаний запит уповноваженим представником Другої міської клінічної лікарні надано відповідь за вих. №01-1437 від 23.07.2015 р. за інформацією з приводу листка непрацездатності №084355. Також роботодавцем було направлено низку запитів аналогічного змісту до інших медичних закладів щодо знаходження у них ОСОБА_1 на лікуванні відповідно до наданого працівником листка працездатності. У відповідь на

[92] Постанова Полтавського апеляційного суду від 01 липня 2020 року у справі № 554/4546/19 [Електронний ресурс]. – Режим доступу: https://reyestr.court.gov.ua/Review/90614697

вказані запити медичні заклади повідомили про відсутність факту звернення до них ОСОБА_1.

Суд наголосив на праві перевірки роботодавцем виданого відповідно до Інструкції №455 листка непрацездатності щодо правомірності його видачі працівнику згідно з листом Міністерства охорони здоров`я від 12.06.2017р.№3.04.02-Н-7698/6898-зв.[93] А також, суд обгрунтовано зазначив, що оскільки ОСОБА_1 не був пацієнтом, зокрема, Четвертої міської клінічної лікарні міста Полтави, відповідно, вказаний медичний заклад не був володільцем жодної інформації щодо нього, персональних даних останнього, та відомостей, що становлять лікарську таємницю. Таким чином, з досліджених письмових доказів судом не встановлено порушень права позивача на захист персональних даних, а також права на таємницю про стан здоров`я.[94]

Ми згідні з висновками суду, однак не цілком погоджуємось з обгрунтуванням. На нашу думку, запити роботодавця ПАТ «Полтаваобленерго» містили вимогу щодо надання медичних даних про його працівника (ОСОБА_1), а саме власне факт звернення до відповідного медичного закладу за медичною допомогою, що є складовою медичної таємниці. Однак, вказані дії роботодавця підпадають під п. 2 вищенаведеної ч.2. ст.7 Закону України «Про захист персональних даних», є виправданими та співмірними, оскільки не містили вимоги надання інформації про діагноз та методи лікування працівника, а лише факт його звернення за медичною допомогою відповідно до наданого останнім листка непрацездатності.

При цьому, роботодавець не повинен зловживати наданими йому правами. У справі № 712/3841/17 Верховний Суд в своїй постанові від 21 серпня 2019 року задовольнив касаційну скаргу ОСОБА_1 про скасування рішення Апеляційного суду Черкаської області від 17 серпня 2017 року та залишення в силі рішення Соснівського районного суду міста Черкаси від 05 липня 2017 року, яким задоволено позовні вимоги ОСОБА_1 (працівника до

[93] Постанова Полтавського апеляційного суду від 01 липня 2020 року у справі № 554/4546/19 [Електронний ресурс]. – Режим доступу: https://reyestr.court.gov.ua/Review/90614697
[94] Там само.

Публічного акціонерного товариства «Черкасиобленерго» (далі - роботодавець), Комунального некомерційного підприємства «Олександрівська центральна районна лікарня» Олександрівської районної ради Кіровоградської області (далі - КНП «Олександрівська ЦРЛ») про визнання незаконним та скасування наказу про відсторонення від роботи, стягнення середнього заробітку, відшкодування моральної шкоди, визнання дій неправомірними, визнання медичного висновку таким, що не втратив чинність. Касаційна скарга була обґрунтована тим, що відповідач безпідставно відсторонив позивача від роботи, оскільки позивач не ухилявся від проходження медичного огляду, а пройшов його в іншій медичній установі України, що не суперечить вимогам чинного законодавства.[95]

Матеріалами справи встановлено, на виконання вимоги роботодавця (ПАТ «Черкасиобленерго») працівник (ОСОБА_1) пройшов медичний огляд у медичному закладі - КНП «Олександрівська ЦРЛ», за результатом якого медична комісія надала висновок про придатність позивача до роботи на посаді начальника енергоінспекції Черкаського міського РЕМ ПАТ «Черкасиобленерго». Вказаний висновок було надано роботодавцю, проте останній звернувся з листами до медичного закладу, в яких просив підтвердити кваліфікацію лікарів, які проводили 21 вересня 2016 року медичний огляд позивача, а також повідомити, чи було враховано цією медичною установою інвалідність позивача на час проходження ним медичного огляду. При цьому, судом встановлено, що під час проходження медичного огляду позивач надав комісії лікарів всі необхідні документи та відомості щодо стану свого здоров`я та наявності у нього другої групи інвалідності.

Суд обґрунтовано на нашу думку зазначив, що всі особи (зокрема і ті, що не є медичними працівниками), які користуються правом доступу до медичної інформації, зобов`язані зберігати в таємниці всі отримані про пацієнта відомості і повинні бути поінформовані про відповідальність, пов`язану з її

[95] Постанова Верховного суду від 21 серпня 2019 року в справі № 712/3841/17 [Електронний ресурс]. – Режим доступу: https://reyestr.court.gov.ua/Review/84005754.

розголошенням.[96] Ми згідні з висновком суду про те, що наявність у позивача другої групи інвалідності сама по собі не може бути підставою для звернення керівника установи до лікарів з вимогою, чи врахована вона при наданні висновку про можливість ним виконання своїх посадових обов`язків. Дії роботодавця в конкретному випадку не були необхідними для здійснення прав та виконання своїх обов'язків за трудовим договором.

Загальні вимоги до обробки медичних даних

Будь-яка обробка медичних даних повинна відповідати загальним вимогам до обробки персональних даних, передбаченим в ст. 6 Закону «Про захист персональних даних», які в науковій літературі та в Конвенції № 108 зазначені як принципи обробки персональних даних. Пропонуємо аналіз застосування вимог з посиланням на судову практику ЄСПЛ.

Принцип конкретизації мети

Передбачений в ч.1 ст. 6 Закону України «Про захист персональних даних», ч.1, п. «b» ч. 4 ст. 5 останньої версії Конвенції № 108 (відповідно до внесених змін протоколом CETS № 223) принцип конкретизації мети передбачає обов'язок володільця даних чітко формулювати мету обробки персональних даних у документах, що регулюють його діяльність[97]. Мета повинна бути явною, чітко визначеною та легітимною. За загальним правилом, володілець повинен одержати згоду суб'єкта персональних даних на обробку своєї персональної інформації стосовно кожної окремої мети, у разі ж її зміни – зобов'язаний знову отримати згоду відповідно до зміненої мети, якщо інше не передбачено законом.[98] Кожна операція щодо обробки даних повинна відповідати чітко визначеній меті їх обробки. Варто погодитись з позицією Бем М. В., Городиського І. М., Саттона Г. та іншими, що саме мета формує базові межі обробки, необхідні для того, щоб надати суб'єкту персональних даних

[96] Постанова Верховного суду від 21 серпня 2019 року в справі № 712/3841/17 [Електронний ресурс]. – Режим доступу: https://reyestr.court.gov.ua/Review/84005754.

[97] Закон України «Про захист персональних даних»: Верховна Рада України; Закон від 01.06.2010 № 2297-VI // Відомості Верховної Ради України. – 2010. – № 34. – с.481.

[98] Бем М. В., Городиський І. М., Саттон Г., Родіоненко О. М. Захист персональних даних: Правове регулювання та практичні аспекти: науково-практичний посібник. – К.: К.І.С., 2015. – 220 с. Електронний доступ : https://rm.coe.int/168059920c.

достовірну інформацію щодо того, як оброблятимуться дані, аби особа мала змогу контролювати їх обробку.[99]

Конвенція № 108 дозволяє збирання персональної інформації для подальшої обробки з метою архівування в суспільних інтересах, наукових, історично-дослідницьких або статистичних цілях, за умови дотримання відповідних гарантій, сумісних з цими цілями (п. «b» ч. 4 ст. 5)[100]. Також, в Рекомендації № R (97) 18 щодо захисту медичних даних міститься положення про необхідність забезпечення анонімності інформації у разі її використання інформації в науково-дослідницьких цілях[101]. Разом із тим, в п.12.2 Рекомендації передбачено винятки, коли знеособлення даних може не застосовуватись за дотримання низки гарантій[102].

В ч.8 Закону «Про захист персональних даних» міститься загальне положення, що у разі зміни первинної мети обробки персональних даних, подальша обробка у історичних, статистичних чи наукових цілях може здійснюватися лише у разі забезпечення їх належного захисту.[103] При цьому, законодавець не уточнює які саме механізми захисту він має на увазі. З огляду на зміст статті Закону, схильні вважати, що йде мова про окрему підставу обробки даних за умови дотримання певних гарантій. Варто також згадати ч. 2 ст. 40 Закону України «Основи законодавства України про охорону здоров'я», де зазначено, що у разі використання інформації, яка за змістом є медичною таємницею, в наукових цілях, необхідно забезпечити анонімність суб'єкта даних.[104] Попри те, що жодних застережень до статті не передбачено, вважаємо, що оскільки Конвенція № 108 є також складовою українського законодавства,

---

[99] Бем М. В., Городиський І. М., Саттон Г., Родіоненко О. М. Захист персональних даних: Правове регулювання та практичні аспекти: науково-практичний посібник. – К.: К.І.С., 2015. – 220 с. Електронний доступ : https://rm.coe.int/168059920c.

[100] Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data Strasbourg, 10.X.2018 [Електронний ресурс]. – Режим доступу: https://rm.coe.int/16808ac918

[101] Recommendation No. R (97) 5 on the Protection of Medical Data: Council of Europe, Committee of Ministers; Feb. 13, 1997. Електронний ресурс: https://www.umj.com.ua/article/37381/rekomendacii-radi-yevropi-shhodo-zaxistu-medichnix-danix

[102] Там само

[103] Закон України «Про захист персональних даних»: Верховна Рада України; Закон від 01.06.2010 № 2297-VI // Відомості Верховної Ради України. – 2010. – № 34. – с.481.

[104] Основи законодавства України про охорону здоров'я: Верховна Рада України; Закон від 19.11.1992 р. № 2801-XII // Відомості Верховної Ради України, 1993, № 4, с.19.

в виняткових випадках дозволяється використовувати в наукових цілях інформацію з ідентифікуючими даними про особу, однак лише в разі забезпечення низки гарантій передбачених Конвенцією та Рекомендаціями Ради Європи. За загальним правилом, необхідне знеособлення даних, що на нашу думку, є виправданим, зважаючи на ризики, до яких може призвести розголошення персональної інформації про особу третім особам.

Порушення принципу конкретизації мети констатовано у справі «Авілкіна та інші проти Росії». Відповідно до обставин справи, прокуратура проводила перевірку діяльності заявників – членів релігійної організації «Управлінський центр свідків Єгови» на підставі отриманого звернення, при цьому взаємодіючи з медичними закладами, в яких перебували на лікуванні заявники для збору їх медичних даних у зв'язку з відмовою переливання крові. Заявники не були підозрюваними чи обвинуваченими у жодному кримінальному злочині. А тому, ЄСПЛ не знайшов в діях прокуратури жодної гострої суспільної необхідності, яка б потребувала передачі відомостей, які становили медичну таємницю заявників. Національні суди Росії, з огляду на необмежені повноваження прокуратури щодо витребування особистої інформації про заявників, визнали законними такі дії. Однак, ЄСПЛ вказав про необхідність забезпечення справедливого балансу між правом заявників на приватне життя і діяльністю прокуратури, направлену на забезпечення захисту здоров'я і прав громадян. А тому, враховуючи, що крім прокурорського запиту про доступ до інформації, яка становила медичну таємницю заявників, існували інші можливості проведення перевірки звернення, зважаючи на надмірний об'єм запитуваної інформації та відсутність належних правових гарантій від свавілля, було порушено право заявників на приватне життя.[105]

2. Принцип законності обробки персональних даних

В ст. 32 Конституції України, а також в ст. 6 Закону України «Про захист персональних даних» міститься принцип законності обробки

[105] Рішення Європейського суду з прав людини від 06.06.2013 року у справі «Авілкіна проти Росії» (заява № 1585/09) [Електронний ресурс]. – Режим доступу: https://hudoc.echr.coe.int/fre#{%22itemid%22:[%22001-120071%22]}

персональних даних. Як вже зазначалось, обробка медичних даних особи можлива лише за наявності згоди, що відповідає усім законодавчим вимогам, окрім випадків, визначених законом, і лише в інтересах національної безпеки, економічного добробуту та прав людини.[106] Цілі обробки персональних даних повинні бути конкретними і законними, визначеними за згодою суб'єкта персональних даних, або у випадках, передбачених законами України, у порядку, встановленому законодавством.[107]

Окрім того, аби обробка персональних даних була законною, недостатньо лише вказівки в Законі. Згідно з узгодженою практикою ЄСПЛ, власне Закон теж повинен відповідати критеріям передбачуваності та доступності. Зокрема, у справі «L.H. проти Латвії» (заява №52019/07), збір медичної інформації про заявницю здійснювався Інспекцією по якості надання медичної допомоги аж через сім років після надання медичних послуг (проведення операції). Заявниця не надавала згоди на оцінку якості медичної допомоги, не була повідомлена про обробку своїх персональних даних. А тому, як зазначив суд, викликає сумніви, що обробка медичних даних заявниці здійснювалась із ціллю лікування або організації надання медичних послуг. І хоча, обробка персональних даних Інспекцією була дозволена законом, чинне на той час латвійське законодавство не було сформульоване з достатньою точністю та не забезпечувало належні правові гарантії від свавілля. Таким чином, ЄСПЛ констатував порушення статті 8 Конвенції.[108]

3. Принцип пропорційності

Так, відповідно до ч.3 ст. 6 Закону України «Про захист персональних даних», п. «с» ч. 4 ст. 5 Конвенції №108, склад та зміст персональних повинні бути «відповідними, адекватними та ненадмірними стосовно визначеної мети їх

[106] Конституція України: Верховна Рада України; Закон від 28.06.1996 р. № 254к/96-ВР // Відомості Верховної Ради України. – 1996. – № 30. – с.141.

[107] Закон України «Про захист персональних даних»: Верховна Рада України; Закон від 01.06.2010 № 2297-VI // Відомості Верховної Ради України. – 2010. – № 34. – с.481.

[108] Рішення Європейського суду з прав людини від 29/04/2014 року у справі «L.H. проти Латвії» (заява №52019/07) [Електронний ресурс]. – Режим доступу: https://hudoc.echr.coe.int/fre#{%22itemid%22:[%22001-142673%22]}

обробки».[109] А згідно з ч.1 ст. 5 Конвенції № 108, яка присвячена вимогам щодо легітимності обробки та якості інформації: «обробка даних повинна бути пропорційною щодо легітимної мети, яка переслідується, і відображати на всіх етапах обробки справедливий баланс між усіма зацікавленими інтересами, державними чи приватними, та відповідними правами та свободами».[110] Вказаний принцип передбачає, що обробляти потрібно саме ту інформацію та в саме тому обсязі, який відповідає законним цілям обробки, визначеним володільцем. Складовою цього принципу є також вимога щодо обмеження зберігання даних. Зокрема, «персональні дані обробляються у формі, що допускає ідентифікацію фізичної особи, якої вони стосуються, не довше, ніж це необхідно для законних цілей, у яких вони збиралися або надалі оброблялися.»[111]

У справі «С. та Марпер проти Сполученого Королівства» за заявою № 30562/04, обидва заявники були обвинувачені у кримінальному правопорушенні, але згодом виправдані. Попри закриття справи, відбитки пальців та зразки ДНК заявників продовжували зберігатись в поліції (що було дозволено законом). ЄСПЛ зазначив, що не зважаючи на передбаченість в законі (хоча й положення закону були недостатньо точними в частині визначених умов та порядку зберігання і використання інформації, і що було важливо мати чіткі правила, що регулюють обсяг та застосування таких заходів, а також мінімальні гарантії), попри наявність легітимної мети – запобігання злочинам, втручання в особисте життя заявників не відповідало критерію необхідності в демократичному суспільстві. Як зазначив суд, «всеосяжний та нерозбірливий характер повноважень із зберігання, як вони були застосовані у випадку заявників, не забезпечив знаходження справедливого балансу між

[109] Закон України «Про захист персональних даних»: Верховна Рада України; Закон від 01.06.2010 № 2297-VI // Відомості Верховної Ради України. – 2010. – № 34. – с.481.
[110] Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data Strasbourg, 10.X.2018 [Електронний ресурс]. – Режим доступу: https://rm.coe.int/16808ac918
[111] Закон України «Про захист персональних даних»: Верховна Рада України; Закон від 01.06.2010 № 2297-VI // Відомості Верховної Ради України. – 2010. – № 34. – с.481.

конкуруючими суспільними та приватними інтересами, а держава-відповідач вийшла за будь-які прийнятні межі розсуду в цьому відношенні»[112].

4. Принцип точності

Ч. 2 ст. 6 Закону України «Про захист персональних даних», п. «d» ч. 4 ст. 5 Конвенції № 108 передбачає вимогу, щоб персональні дані, які підлягають обробці були точними, достовірними та оновлювалися в міру потреби, визначеної метою їх обробки.[113]

Звісно, в реаліях сучасних правовідносин та швидкості зміни інформації, досягти стовідсоткової точності, особливо в сфері охорони здоров'я (наприклад, зміна стану здоров'я), є неможливо. Однак, володільці та розпорядники даних повинні докладати максимум зусиль, щоб зібрана ними інформація була актуальною.

5. Принцип справедливості обробки

Принцип справедливості обробки (fair processing) закріплений в ч.1 ст. 6 Закону України «Про захист персональних даних», п. «a» ч. 4 ст. 5 Конвенції № 108, де передбачено, що «обробка персональних даних здійснюється відкрито і прозоро зі застосуванням засобів та у спосіб, що відповідають визначеним цілям такої обробки».[114]

Насамперед, це положення передбачає вже проаналізований нами у п.1.4 обов'язок володільця інформувати суб'єкта персональних даних щодо збирання та передачу його персональних даних третім особам. Цьому обов'язку кореспондує право суб'єкта персональних даних мати доступ до своїх персональних даних (далі п.3.1), зокрема, знати хто, коли, яким чином, в якому обсязі обробляв його персональні дані.

Стосовно порядку обробки конкретно медичних даних, варто наголосити на європейських актах, а саме на Рекомендації Комітету Міністрів Ради Європи

---

[112] Рішення Європейського суду з прав людини від 4.12.2008 року у справі С. та Марпер проти Сполученого Королівства» за заявою № 30562/04 [Електронний ресурс]. – Режим доступу: https://hudoc.echr.coe.int/fre#{%22tabview%22:[%22document%22],%22itemid%22:[%22001-117816%22]}

[113] Закон України «Про захист персональних даних»: Верховна Рада України; Закон від 01.06.2010 № 2297-VI // Відомості Верховної Ради України. – 2010. – № 34. – с.481.

[114] Там само.

R (97) 5, що передбачає перелік гарантій щодо обробки медичних даних. У п.3.2 Рекомендації закріплений обов'язок медичної таємниці (див. п.3.1 нашої праці), а також у вказаному акті Ради Європи рекомендаційного характеру закріплені вимоги об'єктивності, законності та конкретності цілей для обробки медичних даних. У п.4.2 передбачена можливість збирання медичних даних лише від суб'єктів даних. Інформація може бути отримана з інших джерел виключно, якщо: (1) це відповідає принципам 4 (щодо збирання та обробки медичних даних), 6 (щодо згоди) та 7 (щодо розголошення даних) цієї Рекомендації і якщо це необхідно, щоб досягти мети обробки або (2) якщо суб'єкт даних не в змозі надати дані.[115]

Підстави збирання та обробки медичних даних передбачені п.4.3 Рекомендації. Порівнюючи з національним законодавством, рекомендація Ради Європи дає більш чіткий та розширений перелік підстав для законної обробки медичних даних, однак ключові положення є аналогічними. Пункт 4.4 Рекомендації корелюється із п.6 ч.2. ст.7 Закону України «Про захист персональних даних», а саме дозволяється обробка медичних даних для надання медичної допомоги без окремої згоди.

Окремо в Рекомендації R (97) 5 врегульовані питання медичних даних ненароджених дітей та генетичних даних. Зокрема, в п. 4.5-4.6 Рекомендації, правовий захист медичних даних ненароджених дітей прирівнюється до захисту неповнолітніх дітей, а також міститься положення про надання ненародженим дітям статусу суб'єкта права, а батькам та законним опікунам ненароджених дітей права розпоряджатися їхніми медичними даними, якщо інше не передбачено законодавством.[116] Загалом питання правосуб'єктності зачатих, однак ще ненароджених дітей відноситься до свободи розсуду держави. Відповідно до українського законодавства, ненароджена дитина не виступає окремим суб'єктом права, правоздатність (за винятком окремих аспектів спадкування) виникає лише з моменту народження дитини (ст. 25, 269

[115] Recommendation on the Protection of Medical Data: Council of Europe, Committee of Ministers; Feb. 13, 1997. № R (97) 5 [Електронний ресурс]. – Режим доступу : https://www.coe.int/en/web/data-protection/legal-instruments
[116] Там само.

Цивільного кодексу України).[117] Закон України «Про захист персональних даних» врегульовує питання захисту персональних даних, а отже ідентифікуючої інформації лише про живих осіб. Тому, в Україні медичні дані зачатих, однак ще ненароджених дітей, є складовою медичної інформації їхніх батьків, і саме останні є суб'єктами права щодо медичних даних їхніх зачатих, однак ненароджених дітей.

Щодо питання захисту генетичних даних, в пп. 4.7-4.9 Рекомендацій містяться положення про особливості захисту вказаного різновиду медичних даних. Зокрема, наголошується на обов'язку дотримання цілей збирання та обробки генетичних даних (для профілактики, діагностики,лікування суб'єкта даних або для наукових досліджень); на необхідності окремих законодавчих гарантій у разі обробки генетичних даних з метою судового розгляду або кримінального розслідування, а також на недопущенні зловживання обсягом та цілями обробки в останньому випадку.[118] Обробка генетичних даних в інших цілях, окрім вище перерахованих, можлива лише з метою охорони здоров'я і уникнення будь-якої серйозної шкоди для здоров'я суб'єкта даних або третіх осіб.[119] Однак в окремих випадках – за умови, що інтереси суб'єкта того вимагають, та відповідно до певних гарантій, передбачених законом, може бути дозволена обробка генетичних даних з метою попередження захворювання.[120]

Підсумовуючи, вважаємо за необхідне відзначити низку законодавчих колізій, зокрема між положеннями Закону України «Про захист персональних даних», Наказу МОЗ України № 503 та Закону України «Про державні фінансові гарантії медичного обслуговування населення» щодо необхідності одержання окремої згоди на обробку персональних даних закладами охорони здоров'я та фізичними особами - підприємцями, які одержали ліцензію на провадження господарської діяльності з медичної практики в цілях охорони здоров'я.

[117] Цивільний кодекс України: Верховна Рада України; Закон від 16.01.2003 № 435-IV // Інформаційний бюлетень НКРЕ. – 2003. – № 7.
[118] Recommendation on the Protection of Medical Data: Council of Europe, Committee of Ministers; Feb. 13, 1997. № R (97) 5 [Електронний ресурс]. – Режим доступу : https://www.coe.int/en/web/data-protection/legal-instruments
[119] Там само.
[120] Там само.

Наведений законодавчий дисонанс потребує, на нашу думку, негайного узгодження на користь Закону України «Про захист персональних даних», що є спеціальним. Загальні вимоги щодо обробки персональних, в тому числі, медичних даних, передбачені законодавством України, є аналогічними тим, що передбачені в Конвенції №108. Однак, формальне декларування принципів ще не означає дотримання їх в правозастосовній діяльності.

2.2. Система e-Health в Україні: переваги та ризики.

На виконання вимог ч.1 ст.11 Закону України «Про державні фінансові гарантії медичного обслуговування населення», Кабінет Міністрів України своєю постановою від 25.04.2018 р. № 411 затвердив Порядок функціонування електронної системи охорони здоров'я, яким визначив механізм функціонування електронної системи охорони здоров'я та її компонентів, реєстрації користувачів, внесення та обміну інформацією і документами в електронній системі охорони здоров'я.[121] Саме з цього моменту розпочалось впровадження електронної системи охорони здоров'я в Україні, взявши за приклад успішні закордонні практики. Ключові моменти функціонування системи e-Health в Україні, з визначенням безумовних переваг, а також слабких сторін цього процесу, розглянемо в цьому підпункті.

Насамперед, необхідно розібратись, що таке система «e-Health». У п.2 ч.1 ст. 2 Закону України «Про державні фінансові гарантії медичного обслуговування населення» міститься визначення, згідно з яким «електронна система охорони здоров'я – це інформаційно-телекомунікаційна система, що забезпечує автоматизацію ведення обліку медичних послуг та управління медичною інформацією шляхом створення, розміщення, оприлюднення та обміну інформацією, даними і документами в електронному вигляді, до складу якої входять центральна база даних та електронні медичні інформаційні системи, між якими забезпечено автоматичний обмін інформацією, даними та документами через відкритий програмний інтерфейс (API)».[122]

[121] Закон України «Про державні фінансові гарантії медичного обслуговування населення»: Верховна Рада України; Закон від 19.10.2017 № 2168-VIII// Відомості Верховної Ради України. – 2018. – № 5. – с.31.
[122] Там само.

У науковій літературі науковці пропонують власні дефінації поняття «e-Health». Зокрема, вдалим, на нашу думку, є визначення Нурені Азіз та Чарльза Вивера, які трактують поняття «e-Health» як використання інфраструктури інформаційних технологій та практики електронної комерції для обробки, обміну та управління операціями обробки медичної інформації.[123] Також, Ґ. Ейзенбах пропонує дефініцію поняття «e-Health» як нова сфера на перетині медичної інформатики, охорони здоров'я та бізнесу, яка стосується медичних послуг та інформації, що надається або поширюється через інтернет та пов'язані з ним технології. У більш широкому розумінні, на думку вченого, цей термін характеризує не лише технічний розвиток, але й спосіб мислення, ставлення та зобов'язання до мережевого глобального мислення для покращення охорони здоров'я на місцевому, регіональному та світовому рівнях за допомогою інформаційно-комунікаційних технологій.[124]

Електронна система охорони здоров'я в Україні – це не єдина база даних. E-health в Україні є складною багаторівневою системою, що складається з «центрального» компоненту - центральної бази даних, що включає в себе реєстри МОЗ та «периферійного» компоненту – електронних медичних інформаційних систем (далі – МІС), між якими забезпечено автоматизований обмін інформацією, даними та документами через відкритий програмний інтерфейс (API) (п.3 Порядку № 411).[125] Варто відзначити використання в українській системі e-Health новітніх міжнародних стандартів обміну інформацією HL7 FHIR (Fast Health care Interoperability Resources), які дозволяють збереження та миттєву, точну передачу медичних даних на основі міжнародних кодів. Для кращого розуміння, пропонуємо ознайомитись з Таблицею №1 (додаток 1).

У «центральному» компоненті - центральній базі даних ведуться реєстри, які ми зобразили в Таблиці №2 (додаток №2). Власником центральної бази

[123] Nureni Ayofe Azeez, Charles Vander Vyver. Security and privacy issues in e-health cloud-based system: a comprehensive content analysis. Egyptian Informatics Journal. Volume 20, Issue 2, July 2019, p. 97-108.
[124] Eysenbach, G. What is e-health? Journal of medical Internet research, 3(2), 2001. p.20.
[125] Порядок функціонування електронної системи охорони здоров'я, затверджений постановою Кабінету Міністрів України від 25 квітня 2018 р. № 411

даних, у тому числі майнових прав на програмне забезпечення центральної бази даних та володільцем відомостей є держава у особі Національної служби здоров'я України (НСЗУ). [126] Володільцем відомостей (який визначає мету та порядок обробки даних) Реєстру медичних спеціалістів, Реєстру суб'єктів господарювання у сфері охорони здоров'я та Реєстру медичних висновків є Міністерство охорони здоров'я (МОЗ).[127] Розпорядником Реєстру медичних спеціалістів, Реєстру суб'єктів господарювання у сфері охорони здоров'я та Реєстру медичних висновків (органом, який відповідальний за верифікацію інформації) є НСЗУ.[128] Розпорядником інших реєстрів та володільцем їх відомостей та іншої інформації у центральній базі даних є НСЗУ, якщо інше не визначено законодавством.[129]

Адміністратором центральної бази даних є державне підприємство «Електронне здоров'я», крім Інформаційної системи НСЗУ, адміністрування якої забезпечує НСЗУ.[130] Слід відзначити, що адміністратор лише здійснює організаційні, технічні та інші заходи, необхідні для того, аби забезпечити функціонування центральної бази даних електронної системи охорони здоров'я, він не уповноважений здійснювати обробку персональних даних пацієнтів.

Науковці зазначають, що різні домени, які використовуються під час обміну медичними даними, ускладнили застосування інформаційної системи, що призвело до необхідності у хмарному сховищі (cloud-based environment), яке б дозволило спільно обмінюватися інформацією між різними адміністративними доменами.[131] Безумовними перевагами використання хмарних сховищ є безперервна передача інформації, що, своєю чергою, дозволяє обмін медичними даними в реальному часі та забезпечує актуальність

[126] Порядок функціонування електронної системи охорони здоров'я, затверджений Постановою Кабінету Міністрів України від 25.04.2018 №411. [Електронний ресурс]. – Режим доступу: https://zakon.rada.gov.ua/laws/show/411-2018-%D0%BF#Text

[127] Там само.

[128] Там само.

[129] Там само.

[130] Порядок функціонування електронної системи охорони здоров'я, затверджений Постановою Кабінету Міністрів України від 25.04.2018 №411. [Електронний ресурс]. – Режим доступу: https://zakon.rada.gov.ua/laws/show/411-2018-%D0%BF#Text

[131] Zhang R, Liu L. Security models and requirements for healthcare application clouds. In: 3rd IEEE International Conference on Cloud Computing (CLOUD), Miami, FL, USA, USA, pp. 268–275 (2010).

медичної інформації. Також у науковій літературі відзначають економічну вигідність і збільшення гнучкості спільного обміну інформацією при використанні хмарних технологій.[132] Значною перевагою використання хмарних сховищ є можливість резервування інформації на додаткових серверах, що запобігає її випадковій втраті. Також, поряд із звичайною системою охорони здоров'я, e-health дозволяє вирішити низку проблем, серед яких низька ємність, високі витрати на експлуатацію та технічне обслуговування та інтеграцію системи.[133] Не слід забувати і про такі переваги e-Health, як забезпечення прозорості та відкритості при управлінні охороною здоров'я. Перехід на електронну систему охорону здоров'я в Україні є одним із ефективних заходів для боротьби з корупцією, що відповідає міжнародним зобов'язанням України.

Однак, використання системи e-Health породжує і низку ризиків, зокрема, щодо безпеки та конфіденційності персональних, в тому числі медичних, даних.[134] Європейська комісія зазначає: «У всіх країнах довіра до систем електронного охорони здоров'я як з боку громадян, так і медичних фахівців була визначена однією із, якщо не ключовою проблемою. Конфіденційність визнана найбільш чутливим аспектом електронних систем обліку здоров'я».[135] Серед головних питань конфіденційності варто зазначити: незаконне або недобровільне розкриття персональної інформації суб'єкта даних, порушення права пацієнта бути ознайомленим хто саме і коли мав доступ до його медичних даних, вразливість до атак. Окрім того, існує загроза веб-аналітики, здійсненої третіми особами, які використовують персональні дані користувачів для цільової реклами.[136] Для захисту інформації використовують як організаційні, так і технічні заходи для ефективного запобігання різноманітним загрозам,

[132] Abbas, A, Khan, M, Ali, M, Khan, S, Yang, L. A cloud based framework for identification of influential health experts from Twitter. In: Proceedings of the 15th International Conference on Scalable Computing and Communications (ScalCom) (2015), Beijing, China, pp.831-838 (2015).

[133] Rahimli A. A Review of Cloud Computing Technology Solution for Healthcare System. Research Journal of Applied Sciences, Engineering and Technology 2014 8(20):2150-2153.

[134] Zissis D, Lekkas D. Addressing cloud computing security issues. Future Generation Computer Systems. Volume 28, Issue 3, March 2012, Pages 583-592.

[135] Mahony, M. Trust remains key barrier to eHealth. Електронний ресурс: http://euobserver.com/ 893/31958.

[136] Eman Abukhousa, Nader Mohamed, Jameela Al-Jaroodi. e-Health Cloud: Opportunities and Challenges July 2012 Future Internet 4(4):621-645

таким як несанкціонований доступ, відмова в доступі, втрата всіх даних, фальсифікація, підробка особистих даних тощо. Окремого визначення міжнародних стандартів щодо механізмів захисту персональних даних в електронній системі даних немає. Однак, науковці пропонують наступні способи протидії незаконного розкриття інформації. Один із них - це надання пацієнтам, які є суб'єктами даних, повного контролю над обміном своєї конфіденційної інформації (пацієнто-орієнтований підхід). Тобто, замість того, щоб власник хмари шифрував дані пацієнтів, пацієнти можуть генерувати власні ключі шифрування, використовуючи атрибутивне шифрування, а потім розповсюджувати їх конкретним авторизованим користувачам.[137] В такому випадку, пацієнти мають змогу визначити чіткий перелік осіб, які уповноважені на обробку їх медичних даних, конкретний обсяг та необхідний строк розкриття персональних даних. Також, вартує уваги спосіб шифрування даних за допомогою криптографічних методів, щоб дозволити власнику даних делегувати більшість обчислювальних операцій власнику хмари, але без розкриття змісту, тобто без розкриття персональної інформації.[138] Інші аргументовані способи забезпечення безпеки даних - становлення реєстраторів даних, різні механізми автентифікації, авторизації та контролю доступу, періодична сертифікація стороннім аудитом (TPA), довірені домени конфіденційності.[139]

Варто відзначити дослідження Бехер С, Герл А та Бюлз Ф. щодо того, яким чином технології в e-health впливають на право на приватність. Зокрема, науковці обґрунтовано зауважують, що збір персональних, і в тому числі медичних даних, відбувається не лише медичними працівниками в рамках охорони здоров'я, але й з різних пристроїв нашого повсякденного життя, таких

[137] Li, M.; Yu, S.; Ren, K.; Lou, W. Securing Personal Health Records in Cloud Computing: Patient-centric and Fine-grained Data Access Control in Multi-owner Settings. In Proceedings of the 6th International ICST Conference on Security and Privacy in Communication Networks (SecureComm 2010), Singapore, 7–9 September 2010; pp. 89–106.

[138] Yu, S.; Wang, C.; Ren, K.; Lou, W. Achieving secure, scalable and fine-grained data access control in cloud computing. In Proceedings of INFOCOM 2010, San Diego, CA, USA, 15–19 March 2010; pp. 1–9.

[139] Eman Abukhousa, Nader Mohamed, Jameela Al-Jaroodi. e-Health Cloud: Opportunities and Challenges July 2012 Future Internet 4(4):621-645

як датчики та інтелектуальні пристрої в особистому просторі, наприклад, автомобіля, який відчуває стрес або втому водія або ж трекерів для фітнесу чи здоров'я, які постійно збирають дані про різні аспекти людини: від частоти пульсу, кількості щоденного сну, активності, місцезнаходження (відстеження) або рівня цукру в крові.[140] Науковці зазначають про необхідність суб'єкта даних контролювати збір та обробку своїх персональних даних, перш за все, за допомогою персоніфікованого визначення правил в політиці конфіденційності відповідних пристроїв та програм. Наприклад, беручи до уваги програми для відстеження COVID-19, користувач має право погодитись на надання доступу до GPS мобільного пристрою, однак відмовитись від надання додаткових даних, наприклад, щодо можливих хронічних захворювань, свого віку тощо. Вагомо, щоб дані були анонімними, а також були вжиті заходи щодо контролю доступу (науковці виділяють Рольовий контроль доступу (RBAC), Контроль доступу на основі атрибутів (ABAC) та Контроль доступу з урахуванням контексту (CAAC).[141] Окрім того, повинні бути створені відповідні механізми, що враховують аспекти конфіденційності протягом усього розвитку технічних систем (вищезгадана privacy by design).

Розглянемо конкретні організаційні та технічні заходи захисту персональних даних на прикладі української моделі e-Health. Для функціонування системи e-Health в Україні використовують приватну хмарну модель. Так, 27.09.2019 року між Національною службою охорони здоров'я України (Замовник) та Товариством з обмеженою відповідальністю «ДЕ НОВО» (Виконавець) було укладено договір №133 про надання послуг зі зберігання та обробки даних системи eHealth у формі хмарного (віртуального) датацентру.[142] У технічному завданні, яке розміщене в Додатку №1 до Договору №133,

[140] Becher S, Gerl A, Meier B, Bölz F. Big Picture on Privacy Enhancing Technologies in e-Health: A Holistic Personal Privacy Workflow. Information 2020, 11(7), 356; https://doi.org/10.3390/info11070356.

[141] Kayes, A.S.M.; Kalaria, R.; Sarker, I.; Islam, M.; Watters, P.; Ng, A.; Hammoudeh, M.; Badsha, S.; Kumara, I. A Survey of Context-Aware Access Control Mechanisms for Cloud and Fog Networks: Taxonomy and Open Research Issues. Sensors 2020, 20, 2464.

[142] Договір між Національною службою охорони здоров'я України (Замовник) та Товариством з обмеженою відповідальністю «ДЕ НОВО» (Виконавець) №133 від 27.09.2019 року [Електронний ресурс]. – Режим доступу: https://zakupki.com.ua/tender/5431754.

містяться вимоги до технічних та якісних характеристик предмета договору. Предметом договору є послуги зі зберігання та обробки даних системи eHealth у формі приватного хмарного (віртуального) датацентру (VPC), необхідні для розміщення потужностей інформаційних систем Національної служби охорони здоров'я України. Під приватною віртуальною хмарою (VPC) розуміють доступний на вимогу замовника об'єднаний на логічному рівні набір обчислювальних ресурсів Виконавця з пулу ресурсів ХЦОД (хмарного центру обробки даних) та призначених для надання послуг виключно Замовнику. ХЦОД – це хмарна інфраструктура, що на логічному рівні охоплює певний набір обчислювальних ресурсів Виконавця, яка є у володінні, керуванні та експлуатації Виконавця та призначена для спільного користування багатьма замовниками. ХЦОД розміщується в Центрі (ах) обробки даних (ЦОД) Виконавця. Під останнім слід розуміти спеціалізований технічний майданчик, підключений до мережі Інтернет в автономну систему (або мережі в її складі) по множині каналів зв'язку; це сукупність спланованих певним чином територій, будівель, приміщень, зі встановленими інженерними системами забезпечення та обслуговуючим персоналом, що утворюють загальний фізичний простір і технологічне середовище для розміщення комп'ютерів,електронних та інших засобів прийому, передачі, обробки, зберігання інформації і забезпечують задану ступінь доступності (готовності) розміщеного обладнання в заданому режимі функціонування.[143]

Приватне хмарне сховище вважається найбільш захищеним, оскільки дані повністю обмежені від загальнодоступного Інтернету.[144] До електронних медичних записів у приватній хмарі має доступ лише окремо визначений персонал закладів охорони здоров'я або ФОПів, які одержали ліцензію на провадження господарської діяльності з медичної практики, за умови

[143] Договір між Національною службою охорони здоров'я України (Замовник) та Товариством з обмеженою відповідальністю «ДЕ НОВО» (Виконавець) №133 від 27.09.2019 року [Електронний ресурс]. – Режим доступу: https://zakupki.com.ua/tender/5431754.

[144] Nureni Ayofe Azeez, Charles Vander Vyver. Security and privacy issues in e-health cloud-based system: a comprehensive content analysis. Egyptian Informatics Journal. Volume 20, Issue 2, July 2019, p. 97-108.

проходження авторизації та ідентифікації за допомогою цифрових підписів. Для кращого розуміння приватної хмари ми створили Таблицю №3 (додаток №3).

Важливо зазначити, що відповідно до п.11. Порядку №411, технічні засоби центральної бази даних повинні перебувати у межах території України.[145] Для виконання вказаної законодавчої вказівки, у вищезгаданому технічному завданні, що є в Додатку №1 до Договору №133, міститься вимога до усіх обчислювальних ресурсів ХЦОД та комп'ютерних шаф Виконавця щодо знаходження на території України в межах однієї локації.[146]

Щодо технічних вимог до української системи e-Health, хочемо відзначити деякі із них. Так, задля забезпечення цілісності усіх даних, фізичні ресурси зберігання даних для віртуальних дисків та хмарного сховища мають рівень резервування не гірше N+2, тобто вихід з ладу будь-яких двох фізичних дисків не призведе до зупинки сервісу та втрати даних; забезпечено фізичну охорону периметру ЦОД та контролю доступу, а також відео спостереження та зберігання відео-архіву не менше 15 днів; доступ у серверне приміщення строго обмежений; електроживлення приміщення дата центру реалізовано від двох незалежних джерел, використання лише ліцензійного програмного забезпечення тощо. Товариство з обмеженою відповідальністю «ДЕ НОВО», як виконавець договору №133, також забезпечує та гарантує повну ізоляцію даних, що зберігаються/обробляються у віртуальній приватній хмарі від інших користувачів ХЦОД та третіх осіб.

Організаційні заходи захисту інформації в електронній системі e-Health в повній мірі відповідають вимогам, передбаченим в Типовому порядку обробки персональних даних, проаналізованих нами в п.1.4 цієї праці. Окремо хочемо відзначити такий організаційний захід задля забезпечення безпеки в хмарній системі e-Health, як реєстрацію будь-яких дій користувачів, таких як авторизація, спроба авторизації, використання сервісів тощо, та процесів, яка

[145] Порядок функціонування електронної системи охорони здоров'я, затверджений постановою Кабінету Міністрів України від 25 квітня 2018 р. № 411

[146] Договір між Національною службою охорони здоров'я України (Замовник) та Товариством з обмеженою відповідальністю «ДЕ НОВО» (Виконавець) №133 від 27.09.2019 року [Електронний ресурс]. – Режим доступу: https://zakupki.com.ua/tender/5431754.

здійснюється безперервно цілодобово окремими програмними засобами захисту та збереження такої інформації протягом 3 місяців.

Іншим важливим організаційним заходом є кваліфікований електронний підпис (далі- КЕП) медичного працівника, лише за допомогою якого його власник має право доступу до електронної системи. Так, згідно із п.3.1. Регламенту функціонування компонентів електронної системи обміну медичною інформацією, що необхідні для запуску нової моделі фінансування на первинному рівні надання медичної допомоги внесення даних, «доступ до даних у компонентах електронної системи обміну медичною інформацією здійснюється користувачами виключно після їх реєстрації у Системі з застосуванням засобів електронної ідентифікації (електронним цифровим підписом) та наступної автентифікації - введення своїх ідентифікаційних даних, отриманих при реєстрації».[147]

КЕП прирівнюється до власноручного підпису та являє собою унікальний набір даних, який і дозволяє чітко ідентифікувати особу та відслідковувати її дії. При цьому, слід розмежовувати особистий КЕП та КЕП медичного працівника, оскільки саме останній повинен використовуватись працівниками для входу в систему e-Health. У разі ж втрати такого, особа повинна негайно повідомити про такий факт установу, де його було отримано, та подати відповідну заяву на зміну КЕП медичного працівника.

Загалом, варто відзначити достатньо високий рівень захисту персональних даних в українській системі e-Health, що відповідає національним та міжнародним вимогам . Використання приватної хмари, а саме G-cloud, що має сертифікацію Комплексної Системи Захисту Інформації (КСЗІ), належні та достатні організаційні та технічні заходи гарантують цілісність та запобігання несанкціонованому доступу третіх осіб. Окремо відзначимо зберігання

[147] Регламент функціонування компонентів електронної системи обміну медичною інформацією, що необхідні для запуску нової моделі фінансування на первинному рівні надання медичної допомоги. Електронний ресурс: https://ehealth.gov.ua/wp-content/uploads/2018/10/Rehlament_funktsionuvannia_komponentiv_elektronnoi_systemy.pdf

медичних даних у деперсоналізованому вигляді в основному кластері ЦБД, тоді як персональні дані у відокремленому кластері ЦБД.

Однак, хочемо наголосити на необхідності законодавчої зміни декількох аспектів української e-Health. Насамперед, фактично пацієнти як суб'єкти даних позбавлені можливості контролю щодо того, хто і коли мав доступ до їхніх персональних даних. Так, пацієнти не мають можливості ознайомитись із інформацією щодо обробки їхніх персональних даних на рівні НСЗУ (власника центральної бази даних). Також, викликає занепокоєння збереження усього об'єму інформації в ЦБД (разом із інформацією отриманою з периферійного компоненту – із різноманітних медичних інформаційних систем, підключених до системи e-Health). На нашу думку, такий великий обсяг інформації, збережений в одному місці є недоцільним та становить загрозу її безпеці, навіть попри належні організаційні та технічні заходи захисту. Також, це може спричинити в майбутньому перевантаженість системи і, відповідно, унеможливить нормальне функціонування системи. Тож, на нашу думку, необхідно зробити розподіл інформації з забезпеченням окремих надійно захищених серверів, які в сукупності складатимуть систему e-Health.

2.3. Правове регулювання транскордонної передачі медичних даних.

Вважаємо за необхідне окремо проаналізувати такий різновид обробки медичних даних, як транскордонна передача даних у сфері охорони здоров'я.

Поняття «передача» даних («transfer») вживається більше в міжнародному контексті, «розкриття» («disclosure») тяжіє до національної взаємодії і відбувається без згоди суб'єкта персональних даних та «поширення» («dissemination») відрізняється від останнього тим, що здійснюється за згодою суб'єкта персональних даних. Це терміни, що позначають передачу володільцем персональних даних третім особам. Щоправда в Законі України «Про захист персональних даних» міститься також поняття «надання доступу третім

особам» (ст. 16 Закону)[148], попри те що в міжнародних актах, в тому числі Директиві (EU) 2016/679, поняття «доступ» («access») стосується лише принагідного права суб'єкта даних (про це детальніше – в п.3.2 нашої роботи). Поширення персональних даних передбачає дії щодо передачі відомостей про фізичну особу за згодою суб'єкта персональних даних (ч.1 ст. 14 Закону)[149].

Визначення терміну «транскордонна передача даних» в національному законодавстві немає, однак згідно із п.23 ст. 4 Регламенту 2016/679:

«(23) «транскордонне опрацювання» означає або:

(a) опрацювання персональних даних, що відбувається у контексті діяльності осідків контролера чи оператора в Союзі у більше ніж одній державі-члені, ***якщо контролер або оператор мають осідки в більше ніж одній державі-члені****; або (b) опрацювання персональних даних, що здійснюють у контексті діяльності* ***єдиного осідку контролера або оператора в Союзі, але яке істотно впливає чи ймовірно істотно впливатиме на суб'єктів даних у декількох державах-членах****.»*[150]

Отож, транскордонною передачею даних слід вважати не лише обробку даних, коли володілець або розпорядник даних знаходяться у різних державах, а й ситуацію, коли обробка здійснюється в межах однієї держави, однак істотно впливає або ж схильна до істотного впливу на суб'єктів даних, що знаходяться за межами країни. Принагідно також зазначимо, що зберігання персональних даних на хмарах, сервери яких знаходяться на території іноземної держави, не охоплюється поняттям «транскордонна передача даних», однак така діяльність є різновидом обробки персональних даних.

Відповідно до ч.3 статті 29 Закону України «Про захист персональних даних», транскордонна передача даних (передача даних іноземним суб'єктам) дозволяється ***лише за умови забезпечення відповідною державою-контрагентом належного захисту персональних даних*** у випадках,

[148] Закон України «Про захист персональних даних»: Верховна Рада України; Закон від 01.06.2010 № 2297-VI // Відомості Верховної Ради України. – 2010. – № 34. – с.481.

[149] Закон України «Про захист персональних даних»: Верховна Рада України; Закон від 01.06.2010 № 2297-VI // Відомості Верховної Ради України. – 2010. – № 34. – с.481.

[150] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance)

встановлених законом або міжнародним договором України.[151] При цьому, визначення переліку держав, які відповідають наведеній вище вимозі - прерогатива Кабінету Міністрів України. Законодавчо закріплена також презумпція, що держави - учасниці Європейського економічного простору, а також держави, які підписали Конвенцію № 108 узгоджуються з такою вимогою навіть без окремого визнання такими рішенням Кабінету Міністрів України.[152]

Закон окремо наголошує на необхідності додержання принципу «конкретизації мети» та неможливість обробки даних з іншою метою, ніж та, з якою вони були зібрані. Зокрема, якщо медичні дані були зібрані з метою охорони здоров'я для встановлення медичного діагнозу та подальшого лікування, зокрема шляхом підписання декларації з лікарем (без одержання згоди суб'єкта даних на підставі п.6 ч.2. ст. 7 Закону України «Про захист персональних даних»), то такі дані не можуть бути передані іноземним суб'єктам в цілях охорони здоров'я без окремої згоди на це суб'єкта даних, оскільки мета транскордонної передачі не охоплюється п.6 ч.2. ст. 7 Закону України «Про захист персональних даних». Звісно ж, в такому випадку використовувати зібрані медичні дані не в цілях охорони здоров'я, а, наприклад, з метою маркетингу, є також протизаконно без окремої згоди на це суб'єкта даних.

Конкретизації змісту виразу «належний рівень захисту» в національному законодавстві немає, однак в оновленій версії ч.3 ст.14 Конвенції № 108 (відповідно до внесених змін протоколом CETS № 223 від травня 2018 року) міститься роз'яснення, що такий може бути забезпечений через:

1) закон держави-контрагента або міжнародної організації, включаючи відповідні міжнародні договори або угоди; або

2) ad hoc або затверджені стандартизовані гарантії, передбачені юридично обов'язковими та придатними до виконання документами, прийнятими та

[151] Закон України «Про захист персональних даних»: Верховна Рада України; Закон від 01.06.2010 № 2297-VI // Відомості Верховної Ради України. – 2010. – № 34. – с.481.

[152] Там само.

імплементованими особами, які беруть участь у передачі та подальшій обробці.[153]

Хочемо також звернути увагу на інші умови передачі медичних даних іноземним суб'єктам відносин, пов'язаних з персональними даними, передбачені в ч.4 статті 29 Закону України «Про захист персональних даних». А саме: 1) наявність однозначної згоди суб'єкта даних на таку передачу; 2) необхідність укладення чи виконання правочину між володільцем персональних даних та суб'єктом персональних даних, при цьому виключно на користь суб'єкта даних; 3) необхідність захисту життєво важливих інтересів суб'єктів персональних даних; 4) необхідність захисту суспільного інтересу або ж встановлення, виконання чи забезпечення правової вимоги; 5) надання володільцем персональних даних відповідних гарантій щодо невтручання в особисте і сімейне життя суб'єкта персональних даних.[154]

В оновленій версії Конвенції № 108, попри наведені вище підстави, також міститься додаткова – якщо така передача даних є необхідним і пропорційним заходом у демократичному суспільстві щодо свободи вираження поглядів. Щодо захисту суспільного інтересу, наголошується на можливості такої передачі лише за умов передбачення в законі та дотримання вимог необхідності та пропорційності такого втручання в демократичному суспільстві.

Важливим аспектом транскордонної передачі даних є належні органи нагляду. Так, згідно із оновленою версією ч. 6 ст.14 Конвенції № 108, кожна Сторона повинна забезпечити право наглядового органу вимагати, щоб особа, яка передає дані, продемонструвала ефективність гарантій або існування законних інтересів, що переважають, а також право наглядового органу забороняти, призупиняти або встановлювати умови такої передачі з метою захисту прав та основних свобод суб'єктів даних.[155]

---

[153] Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data Strasbourg, 10.X.2018 [Електронний ресурс]. – Режим доступу: https://rm.coe.int/16808ac918

[154] Закон України «Про захист персональних даних»: Верховна Рада України; Закон від 01.06.2010 № 2297-VI // Відомості Верховної Ради України. – 2010. – № 34. – с.481.

[155] Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data Strasbourg, 10.X.2018 [Електронний ресурс]. – Режим доступу: https://rm.coe.int/16808ac918

В Україні немає жодного органу, який би був наділений необхідними повноваженнями. Повідомлення Уповноваженого Верховної Ради України з прав людини, яке здійснюється вже постфактум (п.1.4 нашої роботи) не є належним механізмом захисту. Уповноважений не наділений всіма необхідними повноваженнями, передбаченими в Додатковому протоколі до Конвенції щодо органів нагляду та транскордонних потоків даних від 8 листопада 2001 року. Так, згідно з ст. 1 Додаткового протоколу, орган нагляду повинен мати повноваження стосовно розслідування та втручання в передачу даних, а також право брати участь у судовому розгляді або повідомляти компетентним судовим органам про порушення положень внутрішньодержавного права, що втілюють принципи, викладені в Конвенції та в цьому Протоколі. Також такий орган нагляду повинен бути повністю незалежним від будь-яких гілок влади, однак зацікавлені суб'єкти повинні мати право оскарження його рішень в суді.

На нашу думку, попри те, що незалежність інституції Уповноваженого ВР гарантується Конституцією, він не наділений достатніми повноваженнями для захисту персональних даних при транскордонній передачі персональних даних. Так, Уповноважений ВР у разі виявлення ознак кримінального правопорушення під час перевірки суб'єкта перевірки направляє необхідні матеріали до правоохоронних органів для відкриття кримінального правопорушення (п. 5.17 Порядку здійснення Уповноваженим Верховної Ради України з прав людини контролю за додержанням законодавства про захист персональних даних, затвердженого Наказом Уповноваженого Верховної Ради України з прав людини від 08.01.2014 року № 1/02-14).[156] Зауважимо, що таке повноваження Уповноваженого ВР передбачене не Законом, як вимагається п. 14 ст. 13 Закону України «Про Уповноваженого Верховної Ради України з прав людини»[157], а підзаконним нормативно-правовим актом, що створює сумніви у легітимності дій Уповноваженого. Окрім того, як вже було зазначено, він уповноважений

[156] Порядок здійснення Уповноваженим Верховної Ради України з прав людини контролю за додержанням законодавства про захист персональних даних, затвердженого Наказом Уповноваженого Верховної Ради України з прав людини від 08.01.2014 року № 1/02-14

[157] Закон України «Про Уповноваженого Верховної Ради України з прав людини»: Верховна Рада України; Закон від 23.12.1997 № 776/97-ВР// Відомості Верховної Ради України. – 1998. – № 20. – с.99.

складати протоколи про притягнення до адміністративної відповідальності та направляти їх до суду у випадках, передбачених законом, а також має право за підсумками перевірки, розгляду звернень видавати обов'язкові для виконання вимоги (приписи) про запобігання або усунення порушень законодавства про захист персональних даних.[158]

Однак, найчастіше Уповноважений ВР виступає як орган захисту, а не охорони законних прав та свобод суб'єктів персональних даних. Так, повідомлення Уповноваженого ВР вже про здійснювану обробку медичних даних може означати первинне порушення прав суб'єкта даних, та не є необхідним механізмом охорони. У такому випадку Уповноважений не наділений, передбаченим Конвенцією, *необхідним правом забороняти, призупиняти або встановлювати умови такої передачі* з метою захисту прав та основних свобод суб'єктів даних, а також необхідним *правом наглядового органу вимагати, щоб особа, яка передає дані, продемонструвала ефективність гарантій або існування законних інтересів, що переважають*.

Також, слід погодитись з Бем М. В., Городиським І. М., Саттоном Г. та іншими дослідниками, що станом на сьогодні особу, яка здійснює незаконне поширення персональних, в тому числі, медичних, даних у мережі Інтернет майже неможливо встановити та притягнути до відповідальності, оскільки реєстрація доменного ім'я сайту, де незаконно поширені персональні дані, зазвичай відбувається в іноземній державі.[159] А тому, існує гостра необхідність законодавчого запровадження ефективних механізмів блокування Уповноваженим розміщених в Інтернеті персональних, зокрема медичних даних, з можливістю попереднього або ретроспективного судового контролю.

Щодо законодавства Європейського Союзу, варто відзначити Директиву 2011/24/ЄС про застосування прав пацієнтів у транскордонній охороні здоров'я, яка спрямована на покращення співпраці та обміну інформацією між

[158] Закон України «Про захист персональних даних»: Верховна Рада України; Закон від 01.06.2010 № 2297-VI // Відомості Верховної Ради України. – 2010. – № 34. – с.481.

[159] Бем М. В., Городиський І. М., Саттон Г., Родіоненко О. М. Захист персональних даних: Правове регулювання та практичні аспекти: науково-практичний посібник. – К.: К.І.С., 2015. – 220 с. Електронний доступ : https://rm.coe.int/168059920c

державами-членами в галузі електронної охорони здоров'я для сприяння доступу до охорони здоров’я в державах-членах ЄС та водночас забезпечення захисту персональних даних.[160] Директива підлягає імплементації на локальному рівні кожною державою-членом ЄС. Сподіваємось на якнайшвидше визнання України повноцінним членом ЄС та, відповідно, поширення дії вищевказаної Директиви на територію України, оскільки це означатиме значний крок вперед у галузі транскордонного потоку даних, зокрема між електронними системами охорони здоров’я держав-членів ЄС та, відповідно, спростить процедуру «медичного туризму» в контексті передачі персональних даних між медичними закладами.

Варто наголосити на сфері дії Загального регламенту про захист даних Європейського Парламенту і Ради 2016/679. Окрім того, що вказаний нормативно-правовий акт поширюється і без спеціальної імплементації в національне законодавство на країн-членів Європи, до складу яких не відносять Україну, він також має екстериторіальну дію. Зокрема, організація, яка не створена в межах Європейського Союзу (далі – ЄС), потрапляє в сферу дії GDPR, якщо вона обробляє персональні дані суб'єктів даних, які перебувають у ЄС, коли діяльність щодо обробки пов'язана "з пропозицією товарів чи послуг" таким суб'єктам даних в ЄС або "моніторингом їх поведінки (дій)", якщо їх поведінка має місце в межах ЄС (стаття 3 Загального регламенту про захист даних).[161] Таким чином, гарантії захисту персональних даних, які передбачені Загальним регламентом про захист даних, можуть поширюватись і на український заклад охорони здоров’я, який є володільцем даних (контролером згідно із термінами Загального регламенту про захист даних) та використовує сервери, що знаходяться у межах Європейського Союзу. Зауважимо, що медичні заклади України, що здійснюють діяльність з цільового надання медичної

[160] Directive 2011/24/EU of the European Parliament and of the Council on the application of patients’ rights in cross-border healthcare, 9 March 2011. OJEU 2011;L88:45–65.

[161] Регламент Європейського Парламенту і Ради (ЄС) 2016/679 від 27 квітня 2016 року про захист фізичних осіб у зв’язку з опрацюванням персональних даних і про вільний рух таких даних, та про скасування Директиви 95/46/ЄС (Загальний регламент про захист даних). Офіційний вісник Європейського Союзу L 119/1 від 04.05.2016 (офіційний переклад).

допомоги громадянам ЄС в рамках медичного туризму, на нашу думку, теж підпадають під сферу дії Загального регламенту про захист даних.

Висновки до розділу 2

1. Термін «обробка» медичних даних означає будь-яку дію або сукупність дій, що виконуються із зазначеним різновидом персональних даних, у тому числі, «використання» таких даних. Натомість, «захист» персональних даних є окремою категорією, яку слід відмежовувати від поняття «обробки», оскільки він не передбачає вчинення окремих дій із персональними даними.

2. Обробка медичних даних здійснюється виняткова на підставі згоди особи, яка відповідає вимогам добровільності, поінформованості та однозначності, а також повинна бути конкретною (відповідати меті обробки), або в випадках, чітко окреслених в законі та лише в інтересах національної безпеки, економічного добробуту та прав людини.

3. У зв'язку з існуванням законодавчої колізії у правовому регулюванні підстав для обробки медичних даних, є необхідність законодавчо уніфікувати та узгодити Закон України «Про державні фінансові гарантії медичного обслуговування населення» та Порядок №411 відповідно до вимог спеціального Закону в системі захисту персональних даних, а саме – Закону України «Про захист персональних даних». Згідно з останнім, згода особи на обробку персональних даних для мети, визначеної в п.6 ч.2. ст. 7 Закону України «Про захист персональних даних». (в цілях охорони здоров'я), не потребується.

4. При обробці медичних даних необхідно дотримуватись загальних вимог до обробки персональних даних, а саме: принципу конкретизації мети; принципу законності обробки персональних даних; принципу пропорційності; принципу точності; принципу справедливості обробки. Окремо слід наголосити на важливості дотримання принципу «приватності за замовчуванням» та принципу «мінімізації даних».

5. Транскордонна передача медичних даних дозволяється лише за умови забезпечення відповідною державою-контрагентом належного рівня захисту персональних даних у випадках, встановлених законом або міжнародним договором України, та обов'язково за умов дотримання прав суб'єкта даних.

6. Українська система e-Health забезпечує достатньо високий рівень захисту персональних даних, що відповідає національним і міжнародним вимогам. Використання приватної хмари, а саме G-cloud, що має сертифікацію Комплексної Системи Захисту Інформації (КСЗІ), належні та достатні організаційні та технічні заходи гарантують цілісність і запобігання несанкціонованому доступу третіх осіб. Важливим є зберігання медичних даних у деперсоналізованому вигляді в основному кластері ЦБД, тоді як персональних даних - у відокремленому кластері ЦБД.

7. Однак, існує необхідність законодавчих змін декількох аспектів української e-Health. До таких відносимо, зокрема: 1) забезпечення пацієнтам як суб'єктам даних можливості контролю щодо доступу до їхніх персональних даних; 2) зробити розподіл інформації зі забезпеченням окремих надійно захищених серверів, які в сукупності складатимуть систему e-Health, оскільки недопустимо зберігати увесь об'єм інформації в ЦБД, що може становити загрозу її безпеці, навіть попри належні організаційні та технічні заходи захисту, а також призвести до перезавантаження системи.

РОЗДІЛ 3. Права суб'єкта медичних даних у сфері надання медичної допомоги та відповідальність за їх порушення

Перелік загальних прав суб'єкта даних у сфері захисту персональних даних передбачений в ч.2 ст. 8 Закону України «Про захист персональних даних».[162] Більшість з них ми вже згадували в пп 2.1нашого дослідження.

Оновлена версія Конвенції № 108 в статті 9 додатково виокремлює право на отримання вигоди від діяльності наглядового органу в контексті допомоги у здійсненні та захисті власних прав. А також, на відміну від Закону України «Про захист персональних даних», який передбачає максимально можливий строк 30 календарних днів (якщо інше не передбачено законом) на отримання відповіді на запит про деталі обробки персональних даних, Конвенція № 108 не передбачає чіткого строку для володільця даних для виконання передбаченого обов'язку, однак зазначає, що відповідь повинна бути отримана через розумний проміжок часу, без надмірних затримок чи витрат, при цьому наголошує на важливості подання інформації в зрозумілій для суб'єкта даних формі. Вважаємо, що максимально можливий строк у 30 календарних днів може бути надмірно довгим для суб'єкта даних та може мати наслідком неможливість реалізації та захисту ним своїх прав.

Відзначимо, що крім декларування відповідних прав у законі, законодавець повинен також і деталізувати порядок їх здійснення.

Вважаємо за необхідне розглянути спеціальні права суб'єкта медичних даних у сфері надання медичної допомоги.

3.1. Право фізичної особи на таємницю про стан здоров'я.

На жаль, в Україні відсутній спеціальний нормативний акт, присвячений правам пацієнтів, в тому числі щодо інформаційних прав. Однак, слід відмітити низку міжнародних актів, які врегульовують такі правовідносини. Зокрема, в Конвенції про захист прав та гідності людини щодо застосування біології та

[162] Закон України «Про захист персональних даних»: Верховна Рада України; Закон від 01.06.2010 № 2297-VI // Відомості Верховної Ради України. – 2010. – № 34. – с.481.

медицини 1997 р. Ради Європи (підписана Україною 22.03.2002 року, однак досі не ратифікована) міститься глава III «Приватне життя та право на інформацію», відповідно до ч. 1 ст. 10 якої кожна особа має право на повагу до її особистого життя стосовно інформації про її здоров'я.[163]. Щодо юридичних інструментів, які не є міжнародними договорами та ще не згадані нами в п.1.3 нашої праці, вважаємо за необхідне зазначити Декларацію про політику в галузі дотримання прав пацієнта в Європі (1994), згідно із п. 4.1 якої вся інформація про стан здоров'я пацієнта, його медичний стан, діагноз, прогноз та лікування, а також інша особиста інформація повинна зберігатися в таємниці навіть після смерті.[164]

Генезис поняття «медична таємниця» сягає ще 1948 року, з моменту закріплення в Женевській декларації та в 1949 р. в Міжнародному кодексі медичної етики обов'язку лікаря тримати в таємниці всю відому йому інформацію про пацієнта (див. п.1.3 нашої праці).

ЄСПЛ також неодноразово акцентував увагу на важливості дотримання конфіденційності медичних даних та необхідності передбачення в національному законодавстві гарантій від зловживання, зокрема, в справі «I проти Фінляндії», «Z проти Фінляндії».[165]

Відповідно до ст. 40 (Лікарська таємниця) Закону Основ, «медичні працівники та інші особи, яким у зв'язку з виконанням професійних або службових обов'язків стало відомо про хворобу, медичне обстеження, огляд та їх результати, інтимну і сімейну сторони життя громадянина, не мають права розголошувати ці відомості, крім передбачених законодавчими актами випадків».[166]

---

[163] Конвенція про захист прав та гідності людини щодо застосування біології та медицини 1997 р: Рада Європи. Підписано Україною 22.03.2002. Станом на період написання роботи, не ратифікована. [Електронний ресурс]. – Режим доступу : conventions.coe.int/Treaty/EN/Treaties/Html/164.htm.

[164] Декларація про політику в галузі дотримання прав пацієнта в Європі: Всесвітня організація охорони здоров'я від 28.06.1994. [Електронний ресурс]. – Режим доступу: https://www.who.int/genomics/public/eu_declaration1994.pdf.

[165] Рішення Європейського суду з прав людини від 17.10.2008 року у справі «I проти Фінляндії»» (заява № 20511/03) [Електронний ресурс]. – Режим доступу: http://hudoc.echr.coe.int/eng?i=001-87510

[166]Основи законодавства України про охорону здоров'я: Верховна Рада України; Закон від 19.11.1992 р. № 2801-XII // Відомості Верховної Ради України. – 1993. – № 4. – с.19

В окремих законодавчих актах України фігурує також поняття «медична таємниця». Зокрема, п.2.5 Наказу МОЗ України від 01.08.2005 № 385 «Про інфекційну безпеку донорської крові та її компонентів», де зазначено необхідність дотримання чинних вимог законодавства щодо медичної таємниці до інформації про захворювання осіб (ВІЛ, вірусні гепатити, сифіліс та інші інфекції, визначені МОЗ України)[167], п.1.5 Порядку медичного обстеження донорів крові та (або) її компонентів, затвердженого наказом МОЗ України від 01.08.2005 № 385, відповідно до якого відомості, отримані від донора, складають медичну таємницю.[168]

Варто окремо наголосити, що невдалим є законодавче закріплення дефініції «лікарська таємниця», оскільки така наводить на думку, що обов'язок дотримання конфіденційності відомостей, які є об'єктом медичної таємниці, носять виключно лікарі. Насправді, суб'єктний склад осіб, які підпадають під сферу дії цієї статті є значно ширшим. Так, якщо звернутись до міжнародного законодавства, в п.3.2 Рекомендації Комітету Міністрів Ради Європи R (97) 5 закріплений обов'язок медичної таємниці. Характерно, що такий обов'язок покладений на медичних фахівців, а також на інших фізичних чи юридичних осіб, які працюють від імені медичних фахівців. При цьому, особа-розпорядник інформації, яка не є медичним працівником, повинна збирати та обробляти медичні дані лише відповідно до положень про конфіденційність, що є аналогічними тим, які покладені на медичного працівника, або відповідно до гарантій, передбачених національним законодавством, що мають таку ж силу.[169]

Так, обов'язок додержання медичної таємниці покладений не лише на медичних працівників, але й на будь-яких осіб, яким у зв'язку з виконанням своїх професійних або службових обов'язків чи громадською діяльністю стало відомо про такі відомості. Серед них: інтерни та студенти, які отримали доступ

[167] Наказ МОЗ України від 01.08.2005 № 385 «Про інфекційну безпеку донорської крові та її компонентів», зареєстрований в Міністерстві юстиції України 16 серпня 2005 р. за № 895/11175.

[168] Порядок медичного обстеження донорів крові та (або) її компонентів, затверджений наказом МОЗ України від 01.08.2005 № 385. Зареєстрований в МОЗ України від 16 серпня 2005 р. за № 896/11176.

[169] Recommendation on the Protection of Medical Data: Council of Europe, Committee of Ministers; Feb. 13, 1997. № R (97) 5 [Електронний ресурс]. – Режим доступу : https://www.coe.int/en/web/data-protection/legal-instruments

до відомостей, які об’єктом медичної таємниці під час проходження практики або навчання; фармацевтичні працівники; працівники страхових компаній; водії швидкої медичної допомоги; медичні реєстратори; інші особи, яким надали доступ до відомостей, що становлять медичну таємницю у встановленому законом порядку тощо.

При цьому, питання стосовно того, чи мають право студенти та інтерни завжди в повній мірі ознайомлюватись з інформацією, що є об’єктом медичної таємниці є доволі дискусійним. Насамперед, необхідно звернути увагу на ч.2 ст.40 Закону України «Основи законодавства України про охорону здоров'я», де зазначено: «При використанні інформації, що становить лікарську таємницю, в навчальному процесі, науково-дослідній роботі, в тому числі у випадках її публікації у спеціальній літературі, повинна бути забезпечена анонімність пацієнта».[170] Одними із механізмів охорони та захисту, як ми вже зазначали в п.1.4. є облік працівників, які мають доступ до персональних даних суб’єктів та визначення рівня доступу зазначених працівників до відповідної персональної інформації. Кожен із цих працівників користується доступом лише до тих персональних даних суб’єктів, які необхідні йому у зв’язку з виконанням своїх професійних чи службових або трудових обов’язків.[171] Саме тому, студенти, інтерни та інші особи в межах наукової діяльності можуть отримати доступ до інформації, яка є складовою медичної таємниці лише в тому обсязі, який необхідний для навчальних, наукових, службових цілей та зберігаючи при цьому, за можливості, анонімність пацієнта. Досить проблематичним є визначення, хто в цьому випадку є розпорядником персональних даних пацієнта та має право надавати доступ до такої інформації – заклад охорони здоров’я чи заклад вищої освіти. Найкраще, задля уникнення суперечностей, на нашу думку, письмово зафіксувати це в договорі про співпрацю між закладом вищої освіти та закладом охорони здоров’я. Також, не варто забувати і про письмове

[170] Основи законодавства України про охорону здоров'я: Верховна Рада України; Закон від 19.11.1992 р. № 2801-XII // Відомості Верховної Ради України. – 1993. – № 4. – с.19

[171] Типовий порядок обробки персональних даних, затверджений наказом Уповноваженого від 08.01.2014 № 1/02–14 [Електронний ресурс]. – Режим доступу: https://zakon.rada.gov.ua/laws/show/v1_02715-14#Text

зобов'язання з боку студентів та інтернів про нерозголошення персональних даних.

Законність ознайомлення медиків-інтернів з процедурою надання медичної допомоги пацієнтам в контексті дотримання права на приватність полягає не лише в наявності формального законодавчого врегулювання, але й забезпеченні конкретних гарантій захисту від втручання в законне право пацієнта на конфіденційність. Зокрема, ЄСПЛ у справі «Коновалова проти Російської Федерації» (заява № 37873/04) наголосив, що присутність медиків-інтернів під час пологів у заявниці хоча і мала правове підґрунтя (Основи законодавства Російської Федерації про охорону здоров'я громадян, чинні на той час, не вимагали письмової згоди пацієнта на присутність студентів-медиків), однак не відповідала вимогам законності за змістом п. 2 ст. 8 Конвенції через відсутність у національному праві на момент подій, які розглядаються, достатніх процесуальних гарантій захисту від свавільного втручання у права заявниці, закріплені в ст. 8 Конвенції.[172]

Не менш важливим є питання, яка інформація входить до обсягу поняття «медична таємниця». Хочемо наголосити, що варто розмежовувати терміни «медичні дані» та «медична таємниця», оскільки останнє – ширше за обсягом. Так, у вищезгаданому рішенні Конституційного Суду України у справі К. Г. Устименка від 30.10.1997 р. (справа № 18/203-97), суд зазначив, що всі дані, які становлять зміст поняття «медична інформація» є конфіденційними. А також, що необхідно розрізняти лікарську таємницю - інформацію про пацієнта та медичну інформацію - інформацію для пацієнта. Як влучно зазначає І. Сенюта, об'єктом лікарської таємниці є не лише медична інформація, але й уся інформація, отримана в процесі надання медичної допомоги, в тому числі і інформація про інтимну та сімейну сторону пацієнта. Таким чином, за змістом медичну таємницю та медичну інформацію можна співвіднести як ціле і

[172] Рішення Європейського суду з прав людини від 09.10.2014 року у справі «Коновалова проти Російської Федерації» (заява № 37873/04) [Електронний ресурс]. – Режим доступу: http://medicallaw.org.ua/fileadmin/user_upload/pdf/12_rishenja.pdf

частину відповідно.[173] Також, ми солідарні з позицією Антонова С.В., який вважає, що доцільно використовувати поняття "медична таємниця", що охоплює не лише медичну складову взаємовідносин лікар – пацієнт, а й усю сукупність інформації, яку лікарі, медсестри чи обслуговуючий персонал одержують від пацієнта у процесі спілкування з ним.[174]

Варто наголосити, що не лише розголошення медичного діагнозу чи історії хвороби, а й факту звернення до медичного закладу та будь-якої іншої медичної інформації про особу становить порушення медичної таємниці. Зокрема, в справі № 487/1982/17, позивач, яка працювала на посаді сестри медичного стаціонару відділення загальної хірургії Миколаївської обласної клінічної лікарні Миколаївської обласної ради, звернулася до суду з позовом до роботодавця про скасування наказу про застосування дисциплінарного стягнення (догани) за розголошення медичної таємниці. Обґрунтовуючи позовні вимоги вказувала на те, що не озвучувала історію хвороби пацієнта. Матеріалами справи було встановлено, що догана застосована за «надання інтерв`ю сторонній особі і розголошення відомостей про пацієнта із зазначенням його прізвища, проведення операції, знеболення сибазоном, вживання твердження, що пацієнт є наркоманом, вживає наркотичні засоби і в нього були ломки.» [175]

Рішенням Заводського районного суду м. Миколаєва від 26 березня 2018 року позовні вимоги задоволені. Суд визнав недопустимим доказом відеозапис, на якому було зафіксовано надання сестрою медичної інформації в інтерв'ю, оскільки він отриманий з порушенням порядку, встановленого законом, а саме у зв'язку з його публікацією в інтернет-мережі сторонньою особою. Однак, постановою Апеляційного суду Миколаївської області від 23 травня 2018 року,

[173] Сенюта І.Я. Цивільні правовідносини у сфері надання медичної допомоги в Україні: питання теорії та практики. Дисертація на здобуття наукового ступеня доктора юридичних наук: 12.00.03 – цивільне право і цивільний процес; сімейне право; міжнародне приватне право. — Львівський національний медичний університет імені Данила Галицького; Науково-дослідний інститут приватного права і підприємництва імені академіка Ф. Г. Бурчака Національної академії правових наук України. — Київ, 2018. — 500 с. (с.194)

[174] Антонов С. В. Цивільно-правова відповідальність за заподіяння шкоди здоров'ю при наданні платних медичних послуг : дис. ... канд. юрид. наук : 12.00.03 / Антонов Сергій Володимирович. – К., 2006. – 206 с. С.33.

[175] Постанова Верховного Суду від 20 травня 2019 року в справі № 487/1982/17 [Електронний ресурс]. – Режим доступу: http://reyestr.court.gov.ua/Review/81925629.

залишеною без змін постановою Верховного суду від 20 травня 2019 року, вказане рішення було скасовано та відмовлено у задоволенні позовних вимог. Так, апеляційний суд врахував, що позивач не заперечувала ні факт інтерв'ю сторонній особі, ні факт поширення інформації, що міститься в медичній документації хворого, а тому названі докази створюють сукупність та є належними та достатніми для висновку про безпідставність позову.

На нашу думку, Апеляційний суд Миколаївської області та Верховний Суд дійшли правильного висновку про відмову в задоволенні позову, оскільки позивач, як працівник медичного закладу (розпорядник медичних даних), порушила медичну таємницю, вимоги професійної етики, деонтології та посадової інструкції, надавши третій особі інтерв`ю із зазначенням медичних даних пацієнта, які вона отримала під час виконання своїх посадових обов`язків. Щодо процесуально-правових аспектів, ми також вважаємо за необхідне враховувати визнання особою - позивачем факту розкриття інформації, що становила медичну таємницю.

Як ми вже зазначали неодноразово в пп.2.1 нашої праці, випадки правомірності розкриття відомостей, що становлять медичну таємницю, без згоди особи повинні бути чітко передбачені законом і здійснюватись лише в інтересах національної безпеки, економічного добробуту та прав людини.

Наприклад, один із таких передбачений статтею 6 Закону України «Про психіатричну допомогу», яка дозволяє передачу інформації про стан психічного здоров'я пацієнта для провадження досудового розслідування за письмовим запитом слідчого, прокурора, суду та представника уповноваженого органу з питань пробації.[176]

Однак, варто наголосити на рішенні ЄСПЛ у справі «Заїченко проти України (№ 2)» (заява № 45797/09), де заявник скаржився на порушення пункту 1 статті 5 Конвенції у зв'язку з поміщенням та примусовим триманням його у психіатричній лікарні, а також на порушення статті 8 Конвенції у зв'язку зі

[176] Закон України «Про психіатричну допомогу»: Верховна Рада України; Закон від 22.02.2000 № 1489-III // Відомості Верховної Ради України. – 2000. – № 19. – с.143.

збиранням органами внутрішніх справ відомостей про заявника без його згоди. Суд зауважив - для того, щоб втручання в приватне життя особи було правомірним, недостатньо лише законодавчого підгрунтя. Важливо, щоб закон був сумісним з принципом «верховенства права» та відповідав вимогам доступності та передбачуваності. Тобто, закон повинен бути сформульованим достатньо чітко, щоб забезпечити особі можливість регулювати свою поведінку. Для того, щоб відповідати вказаним вимогам, національне законодавство повинно встановлювати адекватні юридичні гарантії від свавілля та чітко визначати межі повноважень, наданих компетентним органам влади, та способи їхнього здійснення, які в конкретному випадку були відсутніми.[177]

У справі «Пантелеєнко проти України» (заява № 11901/02), заявник посилався на порушення статті 8 Конвенції через розголошення на судовому слуханні конфіденційної інформації про стан його психічного здоров'я і психіатричне лікування. Суд зазначив, що таке втручання в особисте життя було незаконним заявника оскільки такі зібрані медичні дані жодним чином не могли вплинути на результат судового процесу, зокрема на встановлення того, чи особа здійснила наклеп. А тому, запит суду на отримання такого виду чутливої інформації, що не була «важлива для розслідування, досудового слідства чи судового слухання" є незаконним.[178]

Окремо хочемо акцентувати ***на балансі права особи на конфіденційність медичних даних та праві на охорону громадського здоров'я*** на прикладі поширеної на момент написання роботи пандемії коронавірусної хвороби (COVID-19).

Станом на 13.11.2020 року в світі підтверджено понад 52,8 млн випадків інфікування COVID-19 та зафіксовано 1 295 613 смертей. Оскільки дотепер не винайдено дієвих вакцин чи ліків від коронавірусної хвороби, держави активно вживають заходів щодо охорони здоров'я людей та мінімізації контактів з

[177] Рішення Європейського суду з прав людини від 06.07.2015 року у справі ««Заїченко проти України (№ 2)» (Заява № 45797/09) [Електронний ресурс]. – Режим доступу: https://zakon.rada.gov.ua/laws/show/974_a87#Text.
[178] Рішення Європейського суду з прав людини від 29.06.2006 року у справі «Пантелеєнко проти України» (заява № 11901/02) [Електронний ресурс]. – Режим доступу: https://zakon.rada.gov.ua/laws/show/974_274#Text

носіями вірусу. Однак, важливо розмежовувати виправдані та дозволені законом випадки обмеження прав людей та масові порушення прав людей, в тому числі і в сфері захисту персональних даних, зумовлені такими заходами.

Так, багато країн розробили власні мобільні додатки для відстеження ланцюгів зараження COVID-19. Наприклад, в Ізраїлі таке відстеження здійснюється під контролем Ізраїльського агентства безпеки (ISA) за допомогою даних про місцезнаходження їх телефону, використання додатку має примусовий, а не добровільний характер[179]. Тоді як в країнах західної демократії (наприклад, додаток Stopp Corona (Відень, Австрія) прийнято програми відстеження контактів, які використовують технологію Bluetooth, щоб слідувати ланцюгу зараження COVID-19. Такі дані декодуються та аналізуються безпосередньо на пристроях кожної людини або централізовано в органах охорони здоров'я.[180] В межах європейського законодавства із захисту персональних даних, зокрема GDPR, встановлення додатків повинно було відповіти низці вимогам. Зокрема, необхідними умовами є явно виражена чітка згода на обробку персональних даних, таких як дані про місцезнаходження (GPS) або телефонні номери, з певною метою, такою як медичне дослідження або відстеження, яка чітко сформульована в Політиці конфіденційності. Також, дані необхідно видаляти одразу після досягнення мети обробки, а тому термін зберігання даних повинен бути обмежений (здебільшого до 30 днів), при цьому дані повинні бути анонімними. Наголошується, що користувач програми повинен мати можливість висловити власні уподобання щодо згоди на цілі обробки або дані, які збираються та передаються.[181] Політика конфіденційності не тільки повинна бути персоніфікованою та сформульованою прозоро і

[179] Amit, M., Kimhi, H., Bader, T. et al. Mass-surveillance technologies to fight coronavirus spread: the case of Israel. Nat Med 26, 1167–1169 (2020). [Електронний ресурс]. – Режим доступу: https://doi.org/10.1038/s41591-020-0927-z .

[180] Li, J.; Guo, X. COVID-19 Contact-tracing Apps: A Survey on the Global Deployment and Challenges. 2020. [Електронний ресурс]. – Режим доступу: arXiv:2005.03599.

[181] Becher S, Gerl A, Meier B, Bölz F. Big Picture on Privacy Enhancing Technologies in e-Health: A Holistic Personal Privacy Workflow. Information 2020, 11(7), 356; https://doi.org/10.3390/info11070356

зрозуміло для користувача, але й зобов'язана виконуватись відповідальними особами.

У квітні 2020 року в Україні також було запроваджено власний додаток «Дій вдома» для моніторингу дотримання режиму обсервації та самоізоляції осіб, хворих на COVID-19. Цікавим фактом є те, що скачування додатку є добровільним, однак в описі додатку на Google Play Market міститься наступне положення: «Застосунок встановлюється у смартфони осіб, які можуть бути потенційними носіями вірусу COVID-19 та яких зареєстровано у медзакладах як тих, що потребують самоізоляції або обсервації.»[182]. У політиці конфіденційності додатку вказано, що метою обробки даних є протидія поширенню коронавірусної хвороби (COVID-19) відповідно до Закону України «Про внесення змін до Закону України «Про захист населення від інфекційних хвороб» щодо запобігання поширенню коронавірусної хвороби (COVID-19)».[183] Зауважимо, що порядку передачі володільцем даних (Міністерство цифрової трансформації України) або розпорядником (Державне підприємство "Дія") третім особам, передбаченим в Політиці конфіденційності (зокрема, Міністерству внутрішніх справ України, Національній поліції та її територіальним органам) досі немає, що унеможливлює використання зібраної персональної інформації в цілях, відмінних від статистичних.

Окремо слід наголосити на Законі України «Про внесення змін до Закону України «Про захист населення від інфекційних хвороб» щодо запобігання поширенню коронавірусної хвороби (COVID-19)», п. 2 Перехідних положень якого було дозволено обробку персональних даних (у тому числі, медичних) без згоди особи за умови використання таких даних виключно з метою здійснення протиепідемічних заходів та в порядку, визначеному рішенням про

[182] Додаток «Дій вдома» : Google Play Market. Електронний ресурс: https://play.google.com/store/apps/details?id=ua.gov.diia.quarantine&hl=uk&gl=US.

[183] Політика конфіденційності додатку «Дій вдома» [Електронний ресурс]. – Режим доступу: https://diia.gov.ua/policy_covid.

встановлення карантину.[184] Зауважимо, що законодавець вказує лише правомірну мету для використання персональних даних без згоди особи, при цьому умовчує перелік уповноважених суб'єктів. Жодної згадки Закон не містить про коло осіб, персональні дані яких підлягають примусовій обробці даних. Як вже зазначалось раніше, в ст. 32 Конституції України міститься гарантія невтручання в особисте і сімейне життя особи, крім випадків, передбачених Основним Законом. Обробка персональних даних неможлива без згоди особи, крім випадків, визначених законом, і лише в інтересах національної безпеки, економічного добробуту та прав людини.[185] Відповідно до ст. 64 Конституції України, конституційні права і свободи людини і громадянина не підлягають обмеженню, крім випадків, передбачених Конституцією України.[186] Зокрема, наприклад, в умовах воєнного або надзвичайного стану можуть встановлюватися окремі обмеження прав і свобод із обов'язковим зазначенням строку дії цих обмежень. Варто зазначити, що надзвичайного стану у зв'язку з COVID-19 в Україні введено не було. Однак, 25.03.2020 р. прийнято рішення про запровадження режиму надзвичайної ситуації на всій території України, який за своєю правовою природою не є еквівалентним режиму надзвичайного стану, а отже не передбачає тимчасового обмеження прав та свобод людини. Саме тому, сумнівним з точки зору законності положення про доповнення конституційної норми про примусову обробку персональних даних додатковою метою – задля здійснення протиепідемічних заходів шляхом прийняття Закону України «Про внесення змін до Закону України «Про захист населення від інфекційних хвороб» щодо запобігання поширенню коронавірусної хвороби (COVID-19)».

Викликає здивування також законодавче положення вищезгаданого п. 2 Перехідних положень про те, що протягом 30 днів після закінчення карантину

[184] Закон України «Про внесення змін до Закону України «Про захист населення від інфекційних хвороб» щодо запобігання поширенню коронавірусної хвороби (COVID-19)»: Верховна Рада України; Закон від 13.04.2020 № 555-IX // Відомості Верховної Ради України. – 2020. – № 19. – с.127.
[185] Конституція України: Верховна Рада України; Закон від 28.06.1996 р. № 254к/96-ВР // Відомості Верховної Ради України. – 1996. – № 30. – с.141.
[186] Там само.

такі дані мають бути знеособленими, а у разі неможливості цього – знищені. З наведеного можна дійти висновку, що дані підлягатимуть зберіганню протягом всієї дії карантину, термін дії якого може тривати декілька років. Викликає питання доцільність такого тривалого зберігання медичних даних, у разі досягнення мети їх обробки, та, послідовно, питання дотримання принципу обмеження зберігання даних, як складової частини принципу пропорційності.

Резюмуючи, медична таємниця є ширшим за обсягом поняттям, аніж «медичні дані», оскільки включає в себе також інформацію про інтимну та сімейну сторону пацієнта, а також будь-яку іншу інформацію, отриману в процесі надання медичної допомоги. Потребує законодавчих змін формулювання поняття «лікарська таємниця», оскільки обов'язок додержання медичної таємниці покладений не лише на медичних працівників, але й на будь-яких осіб, яким у зв'язку з виконанням своїх професійних або службових обов'язків чи громадською діяльністю стало відомо про таку інформацію. Для того, аби втручання в особисте життя особи шляхом розкриття медичних даних про неї без її згоди було правомірним, такі випадки повинні бути передбаченими в законі, який повинен бути доступним та передбачуваним, а також відповідати критерію необхідності у демократичному суспільстві та здійснюватись в інтересах національної безпеки, економічного добробуту або захисту прав і свобод суб'єктів персональних даних чи інших осіб.

3.2. Право фізичної особи на інформацію про стан свого здоров'я.

Відповідно до частини 2 статті 10 Конвенції про захист прав і гідності людини щодо застосування біології та медицини: Конвенція про права людини та біомедицину від 04.04.1997 р. (підписана з боку України 22.03.2002 р., проте досі не ратифікована), кожна особа має право на

ознайомлення із будь-якою зібраною про її здоров'я інформацією. *Однак бажання осіб не отримувати таку інформацію має також поважатися*.[187]

Важливі положення щодо права на інформацію також закріплені в Лісабонській декларації про права пацієнтів (1981). Зокрема, згідно з пунктом 7 вказаного міжнародно-правового акту:

«пацієнт має право бути повністю поінформований щодо стану свого здоров'я, включаючи медичні факти щодо свого стану. Однак конфіденційна інформація щодо третіх осіб, яка міститься у записах пацієнта, не повинна надаватися пацієнтові без дозволу такої третьої особи. У виняткових випадках інформація може бути прихована від пацієнта за наявності достатніх підстав для припущення, що така інформація створить серйозну загрозу його життю чи здоров'ю. Інформацію необхідно повідомляти відповідно до особливостей місцевої культури й так, аби вона була зрозумілою пацієнту. На пряме прохання пацієнта інформація може йому не надаватися, якщо тільки цього не потрібно для врятування життя іншої особи. Пацієнт має право обирати особу, якій необхідно повідомляти відомості про нього»[188].

В частині 2 статті 2 Декларації про політику в галузі дотримання прав пацієнта в Європі вказано, що «пацієнти мають право бути повністю проінформованими про стан свого здоров'я, зокрема і медичні факти про свій стан, про потенційні ризики і переваги кожного пропонованого методу лікування, про альтернативні методи лікування, про можливі наслідки відмови від лікування, про діагноз, прогноз та хід лікувальних заходів».[189]

Щодо національного законодавства, в статті 285 ЦК України передбачено «право на інформацію про стан свого здоров'я», відповідно до змісту якого повнолітня фізична особа має право на достовірну і повну інформацію про стан свого здоров'я, у тому числі на ознайомлення з

[187] Конвенція про захист прав і гідності людини щодо застосування біології та медицини: Конвенція про права людини та біомедицину від 04.04.1997 (підписана Україною 22.03.2002 р, але не ратифікована). URL: https://zakon.rada.gov.ua/laws/show/994_334#Text.

[188] Лісабонська декларація стосовно прав пацієнта: Міжнародний документ Всесвітньої медичної асоціації від 01.10.1981 [Електронний ресурс]. – Режим доступу : https://www.wma.net/policies-post/wma-declaration-of-lisbon-on-the-rights-of-the-patient/.

[189] Декларація про політику в галузі дотримання прав пацієнта в Європі: Всесвітня організація охорони здоров'я від 28.06.1994. [Електронний ресурс]. – Режим доступу : https://www.who.int/genomics/public/eu_declaration1994.pdf.

відповідними медичними документами, що стосуються її здоров'я.[190] Аналогічні положення містяться у статті 39 Основ.

Перш за все, вважаємо за необхідне наголосити, що дефініція статті є значно вужчою за обсяг відповідного права особи. Адже, як з'ясовано в п.1.2 нашої роботи, до складу медичної інформації входить значно ширше коло інформації, а не лише стан здоров'я особи. Саме тому, вважаємо за необхідно законодавчо усунути дисонанс між формулюванням статті та її обсягом.

Також, аналізуючи вищенаведені положення ЦК України, доходимо висновку, що реалізація права на медичну інформацію в Україні прив'язана до наявності у суб'єкта такої ознаки як повноліття (18 років). Законні представники, тобто батьки (усиновлювачі), опікуни, піклувальники, мають право на отримання інформації про стан здоров'я дитини або підопічного. При цьому, як слушно зазначає І. Сенюта, навіть набуття або надання особі повної цивільної дієздатності не вплине на віковий ценз здійснення права на медичну інформацію, адже це різні правові конструкції.[191] Ми погоджуємось з думкою, що доцільніше було б прив'язувати право на інформацію до такої ознаки суб'єкта як повна цивільна дієздатність.

Також звертаємо увагу, що реалізація права на отримання об'єктивної інформації про щеплення, наслідки відмови від них та можливі поствакцинальні ускладення можлива з досягненням особою 15 років (ч.6 ст.12 Закону України «Про захист населення від інфекційних хвороб»). Вважаємо за необхідне узгодити між собою положення Цивільного кодексу України та Закону України «Про захист населення від інфекційних хвороб».

Питанням залишається чи необхідно надавати дітям доступ до медичної інформації і якщо так, то в якому обсязі. Вік згоди на медичну допомогу згідно з законодавством України становить 14 р. (ст. 284 Цивільного кодексу України, ст. 38

[190] Цивільний кодекс України: Верховна Рада України; Закон від 16.01.2003 № 435-IV // Інформаційний бюлетень НКРЕ. – 2003. – № 7.

[191] Сенюта І.Я. Цивільні правовідносини у сфері надання медичної допомоги в Україні: питання теорії та практики. Дисертація на здобуття наукового ступеня доктора юридичних наук: 12.00.03 – цивільне право і цивільний процес; сімейне право; міжнародне приватне право. — Львівський національний медичний університет імені Данила Галицького; Науково-дослідний інститут приватного права і підприємництва імені академіка Ф. Г. Бурчака Національної академії правових наук України. — Київ, 2018. — 500 с.

Основ). Таким чином, виникає парадоксальна ситуація, коли неповнолітня особа уповноважена на надання згоди на медичну допомогу, однак не може отримати доступ до власної медичної інформації до 18 років. Під критичним сумнівом в наведеній ситуації поінформованість такої згоди, що є неприпустимим на нашу думку. Вважаємо за доцільно законодавчо узгодити положення щодо вікового цензу на доступ до медичної інформації та згоди на медичну допомогу.

Відповідно до п. 2.4 (Право бути почутим) Рекомендації CM/Rec (2018)7 Комітету міністрів державам-членам про принципи дотримання, захисту та реалізації прав дитини в цифровому середовищі: «6. Держави та інші відповідні зацікавлені сторони повинні надавати дітям інформацію про їх права, включаючи права участі, у зрозумілий спосіб, що відповідає їхній зрілості та обставинам. Вони повинні розширювати можливості для їх вираження через ІКТ, як доповнення до особистої участі. Діти повинні бути поінформовані про механізми та послуги, що надають належну підтримку, а також про процедури подання скарг, поновлення прав або відшкодування, якщо їх права порушуються. Така інформація повинна бути також доступна їхнім батькам або опікунам, щоб вони могли підтримувати дітей у здійсненні їхніх прав.»[192]

Ми вважаємо за необхідне імплементувати наведені вище положення в законодавство України. Доцільно закріпити положення про можливість надання інформації неповнолітній особі в зрозумілій для неї формі враховуючи вік та рівень її розвитку. Це уможливить прийняття нею інформованого рішення щодо згоди або відмови від медичної допомоги. Також вважаємо, що законодавчі положення про повідомлення медичної інформації дітей їхнім батькам (усиновлювачів) є виправданими, за винятком набуття або надання неповнолітній особі повної цивільної дієздатності. Адже, в останньому випадку, особа вправі самостійно усвідомлено розпоряджатись своїми немайновими правами.

Необхідно розглянути питання доступу суб'єкта даних до своєї медичної інформації та поширення такої інформації третім особам. Відповідно до ст. 16

[192] Рекомендація CM/Rec (2018)7 Комітету міністрів державам-членам про принципи дотримання, захисту та реалізації прав дитини в цифровому середовищі [Електронний ресурс]. – Режим доступу : https://mvs.gov.ua/upload/file/rekomendac_ya_schodo_zahistu_d_tey_u_cifrovomu_seredovisch_2018.pdf

Закону «Про захист персональних даних», порядок доступу третіх осіб до персональних даних, які перебувають у володінні розпорядника публічної інформації, визначається Законом України «Про доступ до публічної інформації».[193]

Ч.4 ст. 16 Закону України «Про захист персональних даних» містить обов'язкові реквізити такого запиту, серед них і мета та/або правові підстави для запиту.[194] Відповідно до ч.5 цієї ж статті, строк вивчення запиту на предмет його задоволення не може перевищувати десяти робочих днів з дня його надходження.[195] Тобто, протягом цього строку володілець/розпорядник даних повинні повідомити особу, що її запит буде задоволено або ж відмовлено із зазначенням відповідних правових підстав. У першому випадку (якщо запит задовільний), відповідь на запит особи по суті повинна бути надана протягом тридцяти календарних днів з дня його надходження, якщо інше не передбачено законом.

Щодо права суб'єкта даних на доступ до медичних даних, ч. 6 ст. 16 Закону України «Про захист персональних даних» передбачає право суб'єкта персональних даних на одержання будь-яких відомостей про себе у будь-якого суб'єкта відносин, пов'язаних з персональними даними (тобто у володільця, розпорядника інформації чи у третьої особи), за умови зазначення прізвища, ім'я та по батькові, місця проживання і реквізитів документа, що посвідчує його особу.[196] У такому випадку, вказувати мету чи правові підстави для запиту не потрібно. Однак, попри відсутність окремого законодавчого положення, запит суб'єкта даних повинен також містити перелік персональних даних, що запитуються, адже в протилежному випадку, такий запит не зможе бути опрацьованим. Також, до запиту суб'єкта даних повинен бути долучений документ, що засвідчує його особу, зокрема копія паспорта, посвідчена власним підписом суб'єкта даних.

Окремо варто звернути увагу на отримання медичної інформації законними представниками та представниками (адвокатами) суб'єкта даних. З метою

[193] Закон України «Про захист персональних даних»: Верховна Рада України; Закон від 01.06.2010 № 2297-VI // Відомості Верховної Ради України. – 2010. – № 34. – с.481.
[194] Там само.
[195] Там само.
[196] Там само.

підтвердження права батьків (усиновлювачів), опікунів, піклувальників представляти інтереси дитини необхідно надати документи, що підтверджують їхні повноваження, зокрема, копію свідоцтва про народження дитини, рішення суду про усиновлення або рішення суду чи органу опіки та піклування про встановлення опіки над особою.

Щодо представників на договірних засадах, Закон України «Про адвокатуру та адвокатську діяльність» визначає правові засади організації і діяльності адвокатури та провадження адвокатської діяльності в Україні та є спеціальним по відношенню до Закону України «Про захист персональних даних». Саме тому, використання адвокатського запиту, як спеціального юридичного інструменту для виконання обов'язків адвоката є доцільним для одержання ним медичної інформації про особу, яку він/вона представляє. Як слушно зазначає Х. Терешко, Закон України «Про адвокатуру і адвокатську діяльність» не передбачає подання додаткових документів до адвокатського запиту, крім ордера та свідоцтва про право на провадження адвокатської діяльності. З огляду на це, погоджуємось з позицією, що вимагати від адвоката інших документів, окрім тих, що чітко передбачені спеціальним законом, неправомірно.[197] У разі, якщо ж суб'єкт даних хоче обмежити повноваження особи, яка його представляє, зокрема щодо отримання медичної інформації, він вправі зазначити такі обмеження у договорі та/чи згоді на обробку даних, яку надає адвокатові.

Як зазначено в ч.5 ст. 39 Основ, у разі смерті пацієнта члени його сім'ї або інші уповноважені ними фізичні особи мають право бути присутніми при дослідженні причин його смерті та ознайомитися з висновками щодо причин смерті, а також право на оскарження цих висновків до суду.[198] Як ми вже зазначали в пп.1.1 нашої роботи, інформація медичного характеру після смерті особи вже не є персональними даними про особу, оскільки Закон України «Про захист персональних даних» поширюється лише на живих осіб. Однак, в такому випадку,

[197] Терешко Х. Доступ адвоката до персональних даних свого клієнта у сфері надання медичної допомоги // Медичне право,2019 [Електронний ресурс]. – Режим доступу :https://doi.org/10.25040/medicallaw2019.02.057

[198] Основи законодавства України про охорону здоров'я: Верховна Рада України; Закон від 19.11.1992 р. № 2801-XII // Відомості Верховної Ради України. – 1993. – № 4. – с.19

члени сім'ї померлого або інші уповноважені ними фізичні особи мають право на доступ до такої інформації на підставі належно оформленої заяви відповідно до Закону України «Про інформацію». При цьому, до заяви необхідно долучати документи, що підтверджують особу (зокрема, копію паспорта), а також ті, які підтверджують сімейний зв'язок (свідоцтво про шлюб, свідоцтво про народження, довідка про склад сім'ї тощо). На жаль, законодавство України про охорону здоров'я не містить спеціального визначення поняття «член сім'ї», що викликає чимало питань в правозастосуванні. Варто наголосити на роз'ясненні Уповноваженого Верховної Ради України з прав людини від 25.01.2018 № 2/9-К306655 17/26-138, де зазначено: «інформація про померлу особу може надаватись членам її сім'ї, близьким особам та родичам, якщо така інформація необхідна їм для реалізації їх прав, свобод і законних інтересів, за умови надання копій документів, які підтверджують їх родинний зв'язок».[199]У роз'ясненні значно розширено коло осіб, які можуть вимагати право на доступ до конфіденційної інформації про померлу особу, порівняно із ч.5 ст. 39 Основ та ч.4 ст. 285 Цивільного кодексу України. Формулювання «близькі особи» не нечітким та таким, що може спричинити низку зловживань, а тому, на нашу думку, інформація медичного характеру про померлу особу може надаватись виключно членам сім'ї та уповноваженим ними особам, за умови надання підтверджуючий сімейний зв'язок документів.

Щодо права на ознайомлення з відповідними документами, що містить медичну інформацію, ЄСПЛ у справі «К.Х. та інші проти Словаччини» зазначив, що позитивний обов'язок держави повинен бути розширений шляхом не лише надання можливості ознайомлення з інформацією, але й забезпечення можливості отримання копій документів, які містять персональні дані особи. Суд зауважив, що «уникнути ризику зловживань можна й іншим способом, аніж забороняти заявницям виготовляти копії. Наприклад, розголошенню персональних даних про стан здоров'я, яке може суперечити ст. 8 Конвенції, можна було б запобігти

[199] Щодо доступу до інформації про померлого членами сім'ї та близькими родичами: лист Уповноваженого Верховної Ради України з прав людини від 25.01.2018 № 2/9-К306655 17/26-138. Медичне право. 2018. № 1 (21). С. 159–163.

шляхом інкорпорації (включення) у національне законодавство відповідних засобів безпеки з мотивів обмеження умов, за яких окреслені дані можуть бути розголошені, та кількості осіб, які мають право доступу до цих файлів»[200]

Варто також наголосити на закріпленому в ч. 4 ст. 39 Основ (а також ч. 3 ст.285 Цивільного кодексу) праві медичного працівника надати неповну інформацію про стан здоров'я пацієнта, обмежити можливість їх ознайомлення з окремими медичними документами у випадку, якщо інформація про хворобу пацієнта може погіршити стан його здоров'я або погіршити стан здоров'я його законних представників.[201] Таке обмеження обумовлює певну дискрецію дій медичних представників, при чому законодавець встановлює не об'єктивні чітко визначені критерії, а лише суб'єктивну позицію медичного працівника щодо можливості на його думку погіршити стан його здоров'я або погіршити стан здоров'я його законних представників в конкретному випадку. Так, в літературі існують різні погляди щодо можливості та доцільності застосування «медичної таємниці» до власне пацієнта. Одні науковці, зокрема, С. П. Боткін, Г. А. Захар'їн, стійко підтримують утримання окремих медичних даних від самого пацієнта, навіть якщо це пов'язано з обманом.[202] На думку В. П. Осипової, неповідомлення відомостей особі про стан її здоров'я лише створює атмосферу недовіри до лікаря.[203] Ми вважаємо, що при реалізації медичним працівником вказаного вище права, слід враховувати, що таке суб'єктивне рішення медичного працівника, на нашу думку, повинно ґрунтуватися на об'єктивних обставинах, сукупність яких вказує, що існує не просто ризик, а обґрунтовані підстави вважати, що така інформація може завдати особі серйозної шкоди. Це, зокрема, психічний та психологічний стан особи, рівень розвитку, характер відомостей, що повідомляються. При цьому, на нашу думку, лікар ніколи не повинен говорити

[200] Рішення Європейського суду з прав людини від 28.04.2009 року у справі «К.Х. та інші проти Словаччини» (заява № 32881/04) [Електронний ресурс]. – Режим доступу: https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-92418%22]}.

[201] Основи законодавства України про охорону здоров'я: Верховна Рада України; Закон від 19.11.1992 р. № 2801-XII // Відомості Верховної Ради України. – 1993. – № 4. – с.19

[202] Сук И. С. Врачебная тайна. — К.: Здоров'я, 1981. — 39 с.

[203] Коробцова Н.В. Деякі проблеми правової охорони медичної таємниці / Коробцова Н.В., Печений О.П. // Медичне право України: проблеми становлення та розвитку. Матеріали І Всеукраїнської науково-практичної конференції 19–20.04.2007. – С. 165-172.

неправду пацієнту. Навіть при вкрай несприятливому для пацієнта діагнозі, медичний працівник повинен надати особі правдиву інформацію в обережній та делікатній формі.

Підсумовуючи, вважаємо за необхідне узгодити формулювання статті 285 Цивільного кодексу України «право на інформацію про стан свого здоров'я» із обсягом статті, який охоплює значно ширше коло інформації, аніж «стан здоров'я. Також, варто законодавчо узгодити положення щодо вікового цензу на доступ до медичної інформації (18 років) та згоди на медичну допомогу (14 р.). На нашу думку, право на доступ до достовірної та повної медичної інформації повинно стосуватись такої ознаки суб'єкта як повна цивільна дієздатність, замість вікового критерію. Запит на одержання інформації медичної інформації повинен містити всі необхідні реквізити, а законні представники/представники повинні надати підтверджуючі їх повноваження документи. Право на ознайомлення з відповідними документами медичного характеру включає в себе також і можливість отримання копій документів, які містять персональні дані особи.

3.3. Відповідальність за порушення інформаційних прав у сфері надання медичної допомоги.

Відповідальність за порушення інформаційних прав у сфері надання медичної допомоги можна поділити на: дисциплінарну, цивільно-правову, адміністративну та кримінальну. Окремо слід відмітити відповідальність у зв'язку з винесенням Уповноваженим ВР, за підсумком перевірки або ж відразу після розгляду звернення заінтересованої особи, приписів про запобігання або усунення порушень законодавства про захист персональних даних (проблематика притягнення до адміністративної відповідальності Уповноваженим ВР проаналізована нами в п.1.4 нашої праці). Невиконання законних приписів Уповноваженого ВР та його представників є складом адміністративного правопорушення, передбаченого ч.2 ст.188-39 КУпАП.

Дисциплінарна відповідальність у формі догани або звільнення виникає в разі вчинення дисциплінарного проступку, тобто невиконання чи неналежного виконання працівником своїх трудових обов`язків відповідно до посадової інструкції відповідного медичного закладу, зокрема, в разі порушення лікарської таємниці, вимог професійної етики та деонтології. При цьому, відповідно до ст. 148 КЗпП України дисциплінарне стягнення застосовується власником або уповноваженим ним органом безпосередньо за виявленням проступку, але не пізніше одного місяця з дня його виявлення.[204] Крім того, воно не може бути накладене пізніше шести місяців з дня вчинення проступку. Зауважимо принагідно, що обов'язок доказування правомірності застосування дисциплінарного стягнення покладається саме на роботодавця.

Для притягнення особи до дисциплінарної відповідальності невід'ємним є доведення конкретних фактичних обставин допущеного порушення трудової дисципліни. Неможливо притягнути особу до відповідальності за положення, які не прописані в жодному документі. Як слушно зазначив Компаніївський районний суд Кіровоградської області в своєму рішенні від 25 червня 2009 року у справі № 2-190/2009, «поняття «деонтологія» слід розуміти в двох аспектах. По-перше, це професійна етика медичних працівників, принципи поведінки медичного персоналу з пацієнтами, спрямовані на максимальне підвищення ефективності лікування.[205] По-друге, це розділ етики, що вивчає проблеми обовязку, сферу обовязкового, моральні вимоги та співвідношення між ними. Таким чином, суд дійшов висновку, що, накладаючи дисциплінарне стягнення, керівництво лікарні враховувало перший аспект поняття «деонтологія».»[206] Оскільки в медичному закладі не затверджувались деонтологічні норми, неможливо було довести які саме норми порушив позивач, а тому суд дійшов висновку, що наказ в оскаржуваній частині є безпідставним та задовольнив

[204] Кодекс законів про працю: Верховна Рада УРСР від 10.12.1971 № 322-VIII. Відомості Верховної Ради УРСР, 1971, додаток до № 50, ст. 375.
[205] Рішення Компаніївського районного суду Кіровоградської області від 25 червня 2009 року у справі № 2-190/2009. [Електронний ресурс]. – Режим доступу: https://reyestr.court.gov.ua/Review/5987869.
[206] Там само.

позовні вимоги про скасування наказу щодо накладення дисциплінарного стягнення.

Відповідно до статті 55 Конституції України, кожен має право будь-якими не забороненими законом засобами захищати свої права і свободи від порушень і протиправних посягань[207]. Щодо *цивільно-правової відповідальності*, то особа вправі сама визначати спосіб захисту свого порушеного інформаційного права на у сфері надання медичної допомоги. Доцільним у разі порушення медичної таємниці є формулювання позивних вимог про визнання протиправними дій відповідача (що є необхідним для подальшої можливості відшкодування шкоди) та відшкодування завданої матеріальної та/або моральної шкоди.

Важливе процесуальне питання у справах про розголошення медичної таємниці – чи обов'язкове в таких категоріях справ доведення факту ознайомлення з матеріалами медичної документації чи достатньо самого факту розголошення інформації, що є об'єктом медичної таємниці? В справі № 460/1849/15, відповідач методом таємної відеозйомки та шляхом спілкування з медсестрою незаконно зібрав медичну інформацію про позивача, яка містилася в медичних документах останнього, зокрема, в історії хвороби та згодом оприлюднив її.[208] Відеоматеріали, що містили інформацію, що була об'єктом медичної таємниці позивача були прокоментовані відповідачем і розміщені ним у соціальних мережах. Яворівський районний суд Львівської області дійшов висновку про відсутність правових підстав для задоволення позову щодо відшкодування моральної шкоди, завданої розголошенням лікарської таємниці, оскільки відповідач був позбавлений можливості ознайомитися з медичними документами позивача під час перебування в офтальмологічному відділенні лікарні, де позивач перебував на стаціонарному лікуванні, а тому - не міг розголосити лікарську таємницю. Однак Апеляційний суд Львівської області, а

[207] Конституція України: Верховна Рада України; Закон від 28.06.1996 р. № 254к/96-ВР // Відомості Верховної Ради України. – 1996. – № 30. – с.141.
[208] Постанова Верховного суду від 20 червня 2018 року у справі № 460/1849/15 [Електронний ресурс]. – Режим доступу: https://reyestr.court.gov.ua/Review/75099468

згодом і Верховний суд не погодилися зі зазначеним вище висновком суду першої інстанції, оскільки в матеріалах справи містились докази розголошення інформації, що становила медичну таємницю.[209] Ми повністю підтримуємо таку позицію касаційного суду, адже в аналогічних категоріях справ саме встановлення факту незаконного поширення медичної таємниці, інформації про стан здоров'я вже означає порушення немайнового права особи та є підставою для відшкодування їй моральної шкоди. При цьому, факт незаконного поширення такої інформації може встановлюватися як в рішенні суду про притягнення особи до адміністративної або кримінальної відповідальності, так і безпосередньо згідно з приписом Уповноваженого ВР.

У спорах щодо відшкодування моральної шкоди, зокрема і в справах про розголошення персональних даних, необхідно пам’ятати про презумпцію спричинення особі моральної шкоди відповідачем. Так, в постанові Верховного Суду України від 27.09.2017 справі № 6-1435цс17 щодо захисту прав споживача та відшкодування моральної шкоди, завданої у зв’язку з поширенням конфіденційної інформації про відповідача шляхом поширення його особистої розмови в мережі інтернет, Верховний Суд України заперечив правомірність трактування нищестоячими судами закону, зокрема щодо «недоведення позивачем заподіяння йому моральної шкоди, оскільки сам по собі факт розповсюдження персональних даних не може бути підтвердженням завдання моральної шкоди, а Законом України «Про захист персональних даних» не передбачено відшкодування моральної шкоди».[210] Натомість, Верховний Суд України обґрунтовано зазначив, що у деліктних зобов'язаннях саме на відповідача покладено обов'язок спростування презумпції вини шляхом доведення відсутності його вини у завданні шкоди позивачу.

Важливим є і питання юрисдикції щодо визнання незаконними дій прокурора у разі збирання медичних даних про особу без ухвали суду, а також

[209] Постанова Верховного суду від 20 червня 2018 року у справі № 460/1849/15 [Електронний ресурс]. – Режим доступу: https://reyestr.court.gov.ua/Review/75099468

[210] Постанова Верховного суду від 27 вересня 2017 року у справі № 6-1435цс17[Електронний ресурс]. – Режим доступу: https://reyestr.court.gov.ua/Review/70427210

ненадання суб’єкту даних на його вимогу копії такого запиту прокурора про витребування медичних даних (в порядку цивільного чи адміністративного судочинства). У справі № 474/424/18 щодо визнання незаконними дій прокурора щодо збирання медичних даних позивача; визнання незаконною бездіяльність прокурора щодо ненадання копії запиту про надання інформації про стан здоров'я та лікування позивача, Верховний Суд в своїй постанові від 27 лютого 2019 року зауважив, попри те що прокурор витребував медичну інформацію від Врадіївської центральної районної лікарні, а не від позивача, подаючи запит щодо прав позивача, він вступив із нею (позивачкою) у правовідносини, реалізовуючи публічно-владну управлінську функцію.[211] А тому, такий спір за предметним і суб'єктним критеріями підпадає під адміністративну юрисдикцію.[212]

Ми згідні з позицією суду щодо того, що при розмежуванні юрисдикції в подібних спорах слід брати не лише суб'єктний критерій (те, що суб’єктом подання запиту на витребування медичної інформації був прокурор), але і той факт, чи виникнення таких правовідносин відбулось у зв’язку з виконанням чи невиконання суб'єктом владних повноважень його публічно-владних управлінських функцій (те, чи діяв прокурор як фізична особа чи користувався наділеними публічно-владними повноваженнями). У конкретній справі, прокурор, за його словами, звертався із запитом для обґрунтування у суді позиції держави стосовно відстрочення виконання рішення Врадіївського районного суду Миколаївської області від 8 вересня 2017 року у справі № 474/192/17, а отже, реалізовував передбачену законом публічно-владну управлінську функцію. Якби прокурор діяв з власного розсуду, як приватна особа, поза межами будь-якого кримінального розслідування чи судового провадження, юрисдикція, на нашу думку, була б цивільно-правова.

Щодо ненадання позивачеві копії запиту прокурора про витребування її медичної інформації у відповідь на її звернення, Верховний суд зазначив, що у

[211] Постанова Верховного суду від 27 лютого 2019 року в справі № 474/424/18 [Електронний ресурс]. – Режим доступу: https://reyestr.court.gov.ua/Review/80522357.
[212] Там само.

правовідносинах щодо надання відповідей на звернення громадян, які подані згідно з законом «Про звернення громадян», прокурор діє як суб'єкт владних повноважень, здійснюючи публічно-владні управлінські функції.[213] А тому, суд, обґрунтовано на нашу думку, зазначив, що спір і в цій частині повинен розглядатися за правилами адміністративного судочинства.

Також виникає питання юрисдикції у справах щодо визнання незаконними дій , що полягають у розголошенні свідком медичної таємниці під час допиту в кримінальному провадженні – цивільна чи кримінальна юрисдикція. Так, згідно з п.4 ч.2 ст. 65 Кримінального процесуального кодексу України, «не можуть бути допитані як свідки медичні працівники та інші особи, яким у зв'язку з виконанням професійних або службових обов'язків стало відомо про хворобу, медичне обстеження, огляд та їх результати, інтимну і сімейну сторони життя особи - про відомості, які становлять лікарську таємницю».[214] Верховний Суд в своїй постанові від 23 вересня 2020 року у справі № 761/29995/17 обгрунтовано вказав, що суди попередніх інстанцій дійшли помилкового висновку про те, що спірні правовідносини в частині визнання незаконними дій, що полягають у розголошенні свідком медичної таємниці стосовно позивача під час надання показань як свідка під час допиту в кримінальному провадженні та відшкодування моральної шкоди, пов`язаної із розголошенням такої інформації є цивільними.[215] Такі відносини виникли у зв'язку зі збиранням й оцінкою на предмет належності та допустимості доказів, отриманих у кримінальному провадженні. А тому розгляд заявлених вимог як позовних не може відбуватися за правилами жодного з видів судочинства.[216]

Щодо адміністративної відповідальності, яка покладається на володільців та розпорядників інформації за порушення прав суб'єктів персональних даних, у тому числі у сфері охорони здоров'я, склади

[213] Постанова Верховного суду від 27 лютого 2019 року в справі № 474/424/18 [Електронний ресурс]. – Режим доступу: https://reyestr.court.gov.ua/Review/80522357.
[214] Кримінальний процесуальний кодекс України: Верховна Рада України; Закон від 13.04.2012 р. № 4651-VI// Відомості Верховної Ради України. – 2013. – № 9-10, №11-12, №13. – с. 88.
[215] Постанова Верховного суду від 23 вересня 2020 року у справі № 761/29995/17 [Електронний ресурс]. – Режим доступу: https://reyestr.court.gov.ua/Review/91818619.
[216] Там само.

адміністративних правопорушень передбачені в ст.ст. 188-39, 188-40 КУпАП. Зокрема:

1. *Неповідомлення або несвоєчасне повідомлення* Уповноваженого Верховної Ради України з прав людини *про обробку персональних даних або про зміну відомостей*, які підлягають повідомленню згідно із законом, *повідомлення неповних чи недостовірних відомостей* (ч.1 ст. 188-39 КУпАП).[217]

2. *Невиконання законних вимог (приписів) Уповноваженого* Верховної Ради України з прав людини *або визначених ним посадових осіб секретаріату* Уповноваженого Верховної Ради України з прав людини *щодо запобігання або усунення порушень законодавства про захист персональних даних* (ч.2 ст.188-39 КУпАП).[218]

3. *Недодержання* встановленого законодавством про захист персональних даних *порядку захисту персональних даних, що призвело до незаконного доступу до них або порушення прав суб'єкта персональних даних* (ч.4 ст.188-39 КУпАП).[219]

4. *Невиконання законних вимог Уповноваженого* Верховної Ради України з прав людини *або представників Уповноваженого* Верховної Ради України з прав людини (ч.1 ст.188-40 КУпАП).[220]

Слід окремо проаналізувати склад правопорушення, передбачений ч.4 ст.188-39 КУпАП. У законодавстві немає чіткого визначення поняття «порядок захисту персональних даних». Ми схильні погодитись з Бем М. В., Городиським І. М., Саттоном Г. та іншими дослідниками, що визначити таке поняття можна через 2 складові. Перша – це зобов'язання володільця вживати організаційних та технічних заходів з метою запобігання їх випадкової втрати або знищення, незаконної обробки, у тому числі незаконного знищення чи доступу до персональних даних (стаття 24 Закону України «Про захист персональних

[217] Кодекс України про адміністративні правопорушення: Верховна Рада УРСР; Закон від 07.12.1984 р. № 8073-X// Відомості Верховної Ради Української РСР. – 1984. – № 51. – с. 1122.
[218] Там само.
[219] Там само.
[220] Там само.

даних»).[221] А також, це зобов'язання кожного працівника володільця та розпорядника виконувати зобов'язання конфіденційності, тобто розголошувати персональні дані, що стали йому/їй відомі у зв'язку з виконанням трудових, службових або ж професійних обов'язків (стаття 10 Закону України «Про захист персональних даних»)[222].

Одним із недоліків законодавчого формулювання ч.4 ст.188-39 КУпАП є матеріальний склад правопорушення, тобто відповідальність настає не лише за недодержання встановленого законодавством порядку захисту персональних даних, але й обов'язково таких діянь, що призвели до незаконного доступу до персональних даних або порушення прав суб'єкта персональних даних. На практиці, попри те, що в такому випадку практично завжди відбувається порушення прав суб'єкта персональних даних, довести причинно-наслідковий зв'язок між діянням та протиправними наслідками є дуже важко. Згідно з таким формулюванням, відповідальність настає не тоді коли був порушений порядок захисту персональних даних, а коли вже відбулося розкриття персональної, в тому числі, чутливої, інформації або ж порушення інших прав суб'єкта даних. На нашу думку, такі положення аж ніяк не стимулюють володільців та розпорядників до дотримання норм законодавства про захист персональних даних та, на нашу думку, критично потребують законодавчих змін в інтересах суб'єктів даних.

Також ми поділяємо думку Бема М. В., Городиського І. М., Саттона Г. та інших учених, що в наведеній вище статті мова йде не про доступ «третіх осіб», оскільки у статті 16 Закону України «Про захист персональних даних» йдеться про порядок доступу третіх осіб до персональних даних в форматі «запит-відповідь», а саме про незаконне розголошення, поширення відповідних

[221] Закон України «Про захист персональних даних»: Верховна Рада України; Закон від 01.06.2010 № 2297-VI // Відомості Верховної Ради України. – 2010. – № 34. – с.481.

[222] Бем М. В., Городиський І. М., Саттон Г., Родіоненко О. М. Захист персональних даних: Правове регулювання та практичні аспекти: науково-практичний посібник. – К.: К.І.С., 2015. – 220 с. Електронний доступ : https://rm.coe.int/168059920c.

відомостей.[223] Як ми вже відзначали раніше, загальноприйнятим в міжнародній практиці є відношення поняття «доступ» лише для суб'єктів даних, тоді як дії з персональними даних у випадку надання третім особам вже мають назву «поширення», «розкриття», «розголошення».

Ще одним суттєвим недоліком закону є неможливість притягнення до адміністративної відповідальності юридичних осіб. Коли відбулось розкриття персональних даних,наприклад, медичних даних, а вололодільцем є юридична особа (заклад охорони здоров'я), неооподинокими є випадки, коли встановити конкетну особу-працівника володільця, винну в розголошенні медичних даних пацієнта є неможливо (наприклад, коли медичний заклад порушив вимоги щодо обліку осіб що мають доступ до персональних даних). У такому випадку, притягнути до адміністративної відповідальності заклад охорони здоров'я як володільця даних є неможливим, оскільки такий є юридичною особою.

На нашу думку, лакуною в КУпАП є те, що не передбачено відповідальності за неповідомлення суб'єкта про збір його персональних даних (адже ч.1 ст. 188-39 КУпАП стосується неповідомлення або несвоєчасного повідомлення саме Уповноваженого ВР про обробку персональних, в тому числі медичних, даних або про зміну такої інформації).

Варто наголосити, що одним із труднощів притягнення до відповідальності за адміністративні правопорушення щодо захисту персональних даних є законодавче обмеження строків притягнення до відповідальності (протягом 3 місяців з дня вчинення правопорушення, а при триваючому правопорушенні – не пізніш як через три місяці з дня його виявлення).[224] Згідно з даними ЄДРСР за 2019 рік (протягом 01.01.2019-01.01.2020) винесено лише 10 постанов про притягнення до адміністративної відповідальності за ч.4 ст. 188-39 КУпАП, 51 постанову про притягнення до адміністративної відповідальності за ч.1 ст. 1-40 КУпАП (невиконання приписів

[223] Бем М. В., Городиський І. М., Саттон Г., Родіоненко О. М. Захист персональних даних: Правове регулювання та практичні аспекти: науково-практичний посібник. – К.: К.І.С., 2015. – 220 с. Електронний доступ : https://rm.coe.int/168059920c.

[224] Кодекс України про адміністративні правопорушення: Верховна Рада УРСР; Закон від 07.12.1984 р. № 8073-X// Відомості Верховної Ради Української РСР. – 1984. – № 51. – с. 1122.

Уповноваженого) та жодної постанови щодо притягнення до адміністративної відповідальності за ч.1-ч.3 ст. 188-39 КУпАП. На нашу думку, ситуація щодо притягнення винних до відповідальності є критичною та спричинена в тому числі низькою ефективністю роботи Уповноваженого (зокрема і через незначну чисельність штатних працівників Департаменту у сфері захисту персональних даних Секретаріату Уповноваженого).

Кримінальна відповідальність є найбільш суворим різновидом санкцій щодо правопорушника та передбачена ст.ст. 132, 145 та 182 Кримінального кодексу України (далі – КК України).

У ч.1 ст. 182 КК України передбачено кримінальну відповідальність за порушення недоторканності приватного життя, зокрема за «*незаконне збирання, зберігання, використання, знищення, поширення конфіденційної інформації про особу або незаконна зміна такої інформації, крім випадків, передбачених іншими статтями цього Кодексу*».[225] Злочин, передбачений ч.1 ст. 182 КК України є формальним, а отже, закінченим одразу з моменту вчинення (початку вчинення для триваючого правопорушення) одного із діянь, передбачених у диспозиції статті. У ч.2 цієї ж статті передбачено здійснення однієї із дій, передбачених ч. 1 повторно (також формальний склад злочину) або ж у разі заподіяння істотної шкоди охоронюваним законом правам, свободам та інтересам особи (матеріальний склад злочину – а отже для закінчення злочину потрібне настання злочинних наслідків).[226] Під істотною шкодою законодавець має на увазі шкоду, якщо вона полягає у заподіянні матеріальних збитків, що в сто і більше разів перевищують неоподатковуваний мінімум доходів громадян.[227] Ця стаття є загальною щодо інших складів злочину про незаконне поширення конфіденційної інформації, в тому числі, медичних даних. Так, в разі поширення медичної інформації, що є складовою лікарської таємниці суб'єктом, який не підпадає під сферу дію ст. 145 КК України («незаконне

[225] Кримінальний кодекс України: Верховна Рада України; Закон від 05.04.2001 р. № 2341-III // Відомості Верховної Ради України. – 2001. – № 25–26. – с. 131.
[226] Там само.
[227] Там само.

розголошення лікарської таємниці»), зокрема, у разі розголошення зазначеної інформації третіми особами, а не спеціальним суб'єктом, кримінальна відповідальність наставатиме за ст. 182 КК України.

Згідно з диспозицією ст. 145 КК України, криміналізовано «*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*».[228] Предмет злочину (лікарська таємниця) проаналізований нами в п.3.1. Важливим для кваліфікації за цією статтею є наявність умислу (прямого/непрямого), наявність спеціального суб'єкта (особа, якій інформація стала відомою саме через виконання її професійних чи службових, трудових обов'язків). Окремо слід наголосити на матеріальному складі наведеного злочину, оскільки кримінально- караним є діяння передбачене в диспозиції статті лише у разі спричинення ним тяжких наслідків. Законодавець не визначив зміст поняття «тяжкі наслідки», що становить труднощі в правозастосовній практиці. Також проблематичним на практиці є доведення причинно-наслідкового зв'язку.

Ми згідні з твердженням Антонова С. В., що розголошенням медичної таємниці є в тому числі й обговорення медичними працівниками із своїми друзями чи колегами в неформальній обстановці перебігу лікування окремого пацієнта або його особистих проблем у випадку не дотримання анонімності суб'єкта даних.[229] Так, для вчинення зазначеного злочину, не важливі умови кому та за яких умов було незаконно передано інформацію, що є об'єктом медичної таємниці, необхідним є лише сам факт розголошення такої за відсутності підстав, передбачених Конституцією України (умови правомірності розголошення медичних даних проаналізовані нами в п.2.1 роботи).

Спеціальною статтею до попередньо проаналізованої статті, є стаття 132 КК, яка передбачає кримінальну відповідальність за *«розголошення службовою*

[228] Кримінальний кодекс України: Верховна Рада України; Закон від 05.04.2001 р. № 2341-III // Відомості Верховної Ради України. – 2001. – № 25–26. – с. 131.

[229] Антонов С. В. Цивільно-правова відповідальність за заподіяння шкоди здоров'ю при наданні платних медичних послуг : дис. ... канд. юрид. наук : 12.00.03 / Антонов Сергій Володимирович. – К., 2006. – 206 с.

особою лікувального закладу, допоміжним працівником, який самочинно здобув інформацію, або медичним працівником відомостей про проведення медичного огляду особи на виявлення зараження вірусом імунодефіциту людини чи іншої невиліковної інфекційної хвороби, що є небезпечною для життя людини, або захворювання на синдром набутого імунодефіциту (СНІД) та його результатів, що стали їм відомі у зв'язку з виконанням службових або професійних обов'язків».[230]Адже, згідно з ст. 13 Закону України «Про запобігання захворюванню на синдром набутого імунодефіциту (СНІД) та соціальний захист населення», відомості про результати тестування особи з метою виявлення ВІЛ, про наявність або відсутність в особи ВІЛ-інфекції є конфіденційними та становлять лікарську таємницю.[231] Так, наведений склад злочину є формальним, тобто закінченим з моменту розголошення відповідної інформації, а отже для кваліфікації за вказаною статтею не потрібно додатково доводити настання тяжких наслідків для суб'єкта даних (на відміну від попередньої статті 145 КК України). Суб'єкт спеціальний - службова особа лікувального закладу, допоміжний працівник, який самочинно здобув інформацію, або медичний працівник. Якщо ж правопорушник не підпадає під ознаки зазначеного спеціального суб'єкта, або ж отримав доступ до конкретних медичних даних особи не у зв'язку з виконанням службових або професійних обов'язків, в такому випадку, такі діяння повинні кваліфікуватись за ст. 182 КК України.

Принагідно зазначимо, що згідно з статистичними даними Державної судової адміністрації України, Касаційного кримінального суду у складі Верховного Суду за 2019 рік, кількість засуджених осіб за вчинення злочинів, передбачених ст. 132 та 145 КК України у 2018—2019 роках становить 0 осіб.[232] Згідно з даними ЄДРСР, протягом 01.01.2020 року- 01.10.2020 року жодну особу

[230] Кримінальний кодекс України: Верховна Рада України; Закон від 05.04.2001 р. № 2341-III // Відомості Верховної Ради України. – 2001. – № 25–26. – с. 131.

[231] Про запобігання захворюванню на синдром набутого імунодефіциту (СНІД) та соціальний захист населення: закон України від 12 грудня 1991 року № 1972XII // Відомості Верховної Ради України. – 1992. – № 11. – Ст. 152.

[232] Стан здійснення правосуддя у кримінальних провадженнях та справах про адміністративні правопорушення судами загальної юрисдикції у 2019 році. Верховний Суд. 17 [Електронний ресурс]. – Режим доступу: https://supreme.court.gov.ua/userfiles/media/Zbirka_analit_tablic_2019.pdf

не засуджено за наведеними нище статтями. На нашу думку, причиною є приватний характер обвинувачення, правова необізнаність населення, а також недотримання передбачених законодавством гарантій охорони та захисту персональних, у тому числі, медичних даних, що призводить до неможливості встановлення винних осіб та притягнення їх до відповідальності.

Висновки до розділу 3

1. До спеціальних прав суб'єкта медичних даних у сфері надання медичної допомоги належать: право на таємницю про стан здоров'я та право на інформацію про стан свого здоров'я.

2. Медична таємниця є ширшим за обсягом поняттям, аніж «медичні дані», оскільки включає в себе також інформацію про інтимну та сімейну сторону життя пацієнта, а також будь-яку іншу інформацію, отриману в процесі надання медичної допомоги.

3. Потребує законодавчих змін позначення юридичної конструкції «лікарська таємниця», оскільки обов'язок додержання медичної таємниці покладений не лише на медичних працівників, але й на будь-яких осіб, яким у зв'язку з виконанням своїх професійних або службових обов'язків чи громадською діяльністю стало відомо про таку інформацію.

4. Втручання в особисте життя особи шляхом розкриття медичних даних про неї без її згоди буде правомірним, якщо такі випадки передбачені в законі, який повинен бути доступним та передбачуваним, а також відповідати критерію необхідності в демократичному суспільстві та здійснюватись в інтересах національної безпеки, економічного добробуту або захисту прав і свобод суб'єктів персональних даних чи інших осіб.

5. Запит щодо доступу до медичних даних повинен містити всі необхідні реквізити, передбачені ст. 16 Закону України «Про захист персональних даних», а законні представники повинні надати підтверджуючі їхні повноваження документи. При зверненні адвоката за отриманням медичних даних про його клієнта, адвокатський запит

повинен відповідати вимогам ст. 24 Закону України «Про адвокатуру та адвокатську діяльність».

6. Неефективність роботи органів Національної поліції та Уповноваженого Верховної Ради України з прав людини має наслідком відсутність санкцій кримінального та адміністративного характеру для порушників прав суб'єкта медичних даних у сфері надання медичної допомоги.

7. Відшкодування суб'єктом медичних даних, права якого порушені, завданої йому матеріальної та моральної шкоди є більш проблематичним, адже доводити склад цивільного правопорушення непросто. Рішення суду про притягнення особи до адміністративної або кримінальної відповідальності або ж припис Уповноваженого Верховної Ради України з прав людини значно спрощує механізм справедливої сатисфакції у такій чуттєвій сфері.

ВИСНОВКИ

Належне правове дослідження тематики уможливило сформулювати низку висновків, що спрямовані на досягнення мети дослідження.

1. Запропоновано авторське визначення поняття «медичні дані», а саме це: інформація про стан здоров'я пацієнта(ки), його/її діагноз, історію його/її хвороби, про запропоновані дослідження і лікувальні заходи, прогноз можливого розвитку захворювання, інші дані, які безпосередньо пов'язані із станом здоров'я пацієнта(ки) та процесом надання йому/їй медичної допомоги, а також, його/її генетичні дані.

2. До особливостей медичних даних належать поширення на них законодавства про захист персональних даних; «чутливість» їх обробки та конфіденційність за замовчуванням.

3. Медичні дані є особливою категорією персональних даних та, з огляду на віднесення їх обробки до такої, що становить особливий ризик для прав і свобод, потребують додаткових механізмів охорони та захисту. До механізмів охорони зачисляємо: 1) наявність однозначної, добровільної, поінформованої згоди суб'єкта даних на обробку його/її даних, поданої в формі, що дозволяє дійти висновку про її надання (окрім випадків, коли згода на обробку персональних даних не потребується, в тому числі, в цілях охорони здоров'я); 2) обов'язок володільця медичних даних повідомляти суб'єкта даних про збирання його персональних даних, про їх передачу третім особам та інші дії (про кожну зміну, видалення чи знищення персональних даних або обмеження доступу до них); 3) обов'язок повідомлення Уповноваженого Верховної Ради України з прав людини про обробку медичних даних; 4) визначення відповідальної(их) особи(іб) в закладі охорони здоров'я щодо обробки медичних даних; 5) положення про обробку персональних даних на локальному рівні.

4. До механізмів захисту зачисляємо: 1) превентивні, що безпосередньо випливають із обов'язку володільця медичних даних здійснювати організаційні та технічні заходи з метою запобігання їх випадкової втрати або знищення,

незаконної обробки (приміром, визначення окремого обліку працівників, що мають доступ до персональних даних; визначення різних рівнів доступу працівників до медичних даних; письмове зобов'язання осіб про нерозголошення такої інформації; ведення обліку операцій щодо обробки персональних даних суб'єкта та доступом до них); 2)відновлювальні, що здійснюються через діяльність Уповноваженого Верховної Ради України з прав людини або суду (наприклад, обов'язкові для виконання вимоги (приписи) Уповноваженого Верховної Ради України з прав людини про усунення порушень законодавства про захист персональних даних).

5. Необхідно законодавчо уніфікувати та узгодити через існування колізії у правовому регулюванні підстав для обробки медичних даних Закон України «Про державні фінансові гарантії медичного обслуговування населення» та Порядок функціонування електронної системи охорони здоров'я, затверджений Постановою Кабінету Міністрів України від 25.04.2018 №411, відповідно до вимог спеціального Закону в системі захисту персональних даних, а саме – Закону України «Про захист персональних даних». Згідно з останнім, згода особи на обробку персональних даних для мети, визначеної в п.6 ч.2. ст. 7 Закону (в цілях охорони здоров'я), не потребується.

6. При обробці медичних даних необхідно дотримуватись загальних вимог до обробки персональних даних, а саме: принципу конкретизації мети; принципу законності обробки персональних даних; принципу пропорційності; принципу точності; принципу справедливості обробки. Окремо слід наголосити на важливості дотримання принципу «приватності за замовчуванням» та принципу «мінімізації даних».

7. Існує необхідність законодавчих змін декількох аспектів української e-Health. До таких відносимо, зокрема: 1) забезпечення пацієнтам як суб'єктам даних можливості контролю щодо доступу до їхніх персональних даних; 2) розподілення інформації зі забезпеченням окремих надійно захищених серверів, які в сукупності складатимуть систему e-Health, оскільки недопустимо зберігати увесь об'єм інформації в ЦБД, що може ставновити загрозу її безпеці,

навіть попри належні організаційні та технічні заходи захисту, а також призвести до перезаванатаження системи.

8. Медична таємниця є ширшим за обсягом поняттям, аніж «медичні дані», оскільки включає в себе також і інформацію про інтимну та сімейну сторону пацієнта, а також будь-яку іншу інформацію, отриману в процесі надання медичної допомоги.

9. Втручання в особисте життя особи шляхом розкриття медичних даних про неї без її згоди буде правомірним, якщо такі випадки передбачені в законі, який повинен бути доступним та передбачуваним, а також відповідати критерію необхідності в демократичному суспільстві та здійснюватись в інтересах національної безпеки, економічного добробуту або захисту прав і свобод суб'єктів персональних даних чи інших осіб.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

Міжнародно-правові акти

1. Дванадцять принципів організації охорони здоров'я для будь-якої національної системи охорони здоровя: Міжнародний документ Всесвітньої медичної асоціації від 01.10.1963 [Електронний ресурс]. – Режим доступу : http://zakon4.rada.gov.ua/laws/show/990_004.
2. Декларація про політику в галузі дотримання прав пацієнта в Європі: Всесвітня організація охорони здоров'я від 28.06.1994. [Електронний ресурс]. – Режим доступу : https://www.who.int/genomics/public/eu_declaration1994.pdf.
3. Директива 95/46/ ЄС Європейського Парламенту та Ради «Про захист фізичних осіб при обробці персональних даних і про вільне переміщення таких даних» від 24 жовтня 1995 року [Електронний ресурс]. – Режим доступу: https://zakon.rada.gov.ua/laws/show/994_242#Text.
4. Європейська хартія прав пацієнтів: Активна громадська мережа у співпраці з громадськими організаціями з 12 різних країн ЄС від 15.11.2002 [Електронний ресурс]. – Режим доступу : http://meduniv.lviv.ua/files/press-centre/2014/n180414/evropejska_ hartiya_prav_pacientiv.pdf.
5. Женевська декларація: Міжнародний документ Всесвітньої медичної асоціації від 01.09.1948 [Електронний ресурс]. – Режим доступу : http:// zakon3.rada.gov.ua/laws/show/990_001.
6. Конвенція про захист осіб у зв'язку з автоматизованою обробкою персональних даних : Міжнародний документ Ради Європи від 28.01.1981 №108. Дата ратифікації Україною: 06.07.2010. Дата набрання чинності для України: 01.01.2011. [Електронний ресурс]. – Режим доступу : https://zakon.rada.gov.ua/laws/show/994_326#Text.
7. Конвенція про захист прав та гідності людини щодо застосування біології та медицини (1997): Рада Європи. Підписано Україною 22.03.2002.

Станом на період написання роботи, не ратифікована. [Електронний ресурс]. – Режим доступу : conventions.coe.int/Treaty/EN/Treaties/Html/164.htm.

8. Лісабонська декларація стосовно прав пацієнта: Міжнародний документ Всесвітньої медичної асоціації від 01.10.1981 [Електронний ресурс]. – Режим доступу : http://zakon3.rada.gov.ua/laws/show/990_016.
9. Міжнародний кодекс медичної етики: Міжнародний документ Всесвітньої медичної асоціації від 01.10.1949 [Електронний ресурс]. – Режим доступу: http://zakon2.rada.gov.ua/laws/show/990_002.
10. Положення про медичне обстеження, «телемедицину» та медичну етику: Міжнародний документ Всесвітньої медичної асоціації від 01.09.1992 [Електронний ресурс]. – Режим доступу : https://zakon.rada.gov.ua/laws/show/990_049#Text.
11. Регламент Європейського Парламенту і Ради (ЄС) 2016/679 від 27 квітня 2016 року про захист фізичних осіб у зв'язку з опрацюванням персональних даних і про вільний рух таких даних, та про скасування Директиви 95/46/ЄС (Загальний регламент про захист даних). Офіційний вісник Європейського Союзу L 119/1 від 04.05.2016 (офіційний переклад).
12. Рекомендація CM/Rec (2018)7 Комітету міністрів державам-членам про принципи дотримання, захисту та реалізації прав дитини в цифровому середовищі [Електронний ресурс]. – Режим доступу : https://mvs.gov.ua/upload/file/rekomendac_ya_schodo_zahistu_d_tey_u_cifrovomu_seredovisch_2018.pdf.
13. Directive 2011/24/EU on the application of patients' rights in cross-border healthcare, Amended by Council Directive 2013/64/EU of 17 December 2013: the European Parliament and the Council; 9 March 2011.
14. Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data Strasbourg, 10.X.2018 [Електронний ресурс]. – Режим доступу: https://rm.coe.int/16808ac918.

15. Recommendation on the Protection of Medical Data: Council of Europe, Committee of Ministers; Feb. 13, 1997. № R (97) 5 [Електронний ресурс]. – Режим доступу: https://www.coe.int/en/web/data-protection/legal-instruments.

Рішення Європейського суду з прав людини

16. Рішення Європейського суду з прав людини від 04.12.2008 у справі «С. та Маргер проти Сполученого Королівства» (заяви № 30562/04 та 30566/04) [Електронний ресурс]. – Режим доступу: https://hudoc.echr.coe.int/fre#{%22itemid%22:[%22001-90051%22]}.
17. Рішення Європейського суду з прав людини від 06.06.2013 у справі «Авілкіна проти Росії» (заява № 1585/09) [Електронний ресурс]. – Режим доступу: https://hudoc.echr.coe.int/fre#{%22itemid%22:[%22001-120071%22]}.
18. Рішення Європейського суду з прав людини від 06.07.2015 у справі ««Заїченко проти України (№ 2)» (Заява № 45797/09) [Електронний ресурс].–Режим доступу: https://zakon.rada.gov.ua/laws/show/974_a87#Text.
19. Рішення Європейського суду з прав людини від 09.10.2014 у справі «Коновалова проти Російської Федерації» (заява № 37873/04) [Електронний ресурс]. – Режим доступу: http://medicallaw.org.ua/fileadmin/user_upload/pdf/12_rishenja.pdf.
20. Рішення Європейського суду з прав людини від 17.10.2008 у справі «І проти Фінляндії»» (заява № 20511/03) [Електронний ресурс]. – Режим доступу: http://hudoc.echr.coe.int/eng?i=001-87510.
21. Рішення Європейського суду з прав людини від 23.02.2016 у справі «Й.Й. проти Росії» (заява № 40378/06) [Електронний ресурс]. – Режим доступу: https://hudoc.echr.coe.int/eng#{%22fulltext%22:[%22\%22CASE%20OF%20Y.Y.%20v.%20RUSSIA\%22%22],%22documentcollectionid2%22:[%22GRANDCHAMBER%22,%22CHAMBER%22],%22itemid%22:[%22001-161048%22]}.

22. Рішення Європейського суду з прав людини від 26.05.11 у справі «Р. Р. проти Польщі» (заява № 27617/04) [Електронний ресурс]. – Режим доступу: https://hudoc.echr.coe.int/eng#{%22display%22:[%220%22],%22languageisocode%22:[%22UKR%22],%22appno%22:[%2227617/04%22],%22documentcollectionid2%22:[%22CHAMBER%22],%22itemid%22:[%22001-145424%22]}.
23. Рішення Європейського суду з прав людини від 27.01.2017 у справі «Суріков проти України» (заява № 42788/06) [Електронний ресурс]. – Режим доступу: https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-170462%22]}.
24. Рішення Європейського суду з прав людини від 28.04.2009 у справі «К.Х. та інші проти Словаччини» (заява № 32881/04) [Електронний ресурс]. – Режим доступу: https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-92418%22]}.
25. Рішення Європейського суду з прав людини від 29.04.2014 у справі «L.H. проти Латвії» (заява №52019/07) [Електронний ресурс]. – Режим доступу: https://hudoc.echr.coe.int/fre#{%22itemid%22:[%22001-142673%22]}.
26. Рішення Європейського суду з прав людини від 29.06.2006 у справі «Пантелеєнко проти України» (заява № 11901/02) [Електронний ресурс]. – Режим доступу: https://zakon.rada.gov.ua/laws/show/974_274#Text.

Національне законодавство

27. Деякі питання електронної системи охорони здоров’я: Постанова Кабінету Міністрів України від 25.04.2018 № 411. [Електронний ресурс]. – Режим доступу: https://zakon.rada.gov.ua/laws/show/411-2018-%D0%BF#Text.
28. Закон України «Про внесення змін до Закону України «Про захист населення від інфекційних хвороб» щодо запобігання поширенню коронавірусної хвороби (COVID-19)»: Верховна Рада України; Закон від

13.04.2020 № 555-IX // Відомості Верховної Ради України, 2020, № 19. с.127.

29. Закон України «Про державні фінансові гарантії медичного обслуговування населення»: Верховна Рада України; Закон від 19.10.2017 № 2168-VIII// Відомості Верховної Ради України, 2018, № 5, с.31.
30. Закон України «Про електронні документи та електронний документообіг»: Верховна Рада України; Закон від 22.05.2003 № 851-IV // Відомості Верховної Ради України, 2003, № 36, с.275.
31. Закон України «Про захист персональних даних»: Верховна Рада України; Закон від 01.06.2010 № 2297-VI // Відомості Верховної Ради України, 2010, № 34, с.481.
32. Закон України «Про інформацію»: Верховна Рада України; Закон від 02.10.1992 № 2657-XII // Відомості Верховної Ради України, 1992, № 48, с.650.
33. Закон України «Про поховання та похоронну справу»: Верховна Рада України; Закон від 10.07.2003 № 1102-IV // Відомості Верховної Ради України, 2004, № 7, с. 47.
34. Закон України «Про психіатричну допомогу»: Верховна Рада України; Закон від 22.02.2000 № 1489-III // Відомості Верховної Ради України, 2000, № 19, с.143.
35. Кодекс законів про працю: Верховна Рада УРСР від 10.12.1971 № 322-VIII. Відомості Верховної Ради УРСР, 1971, додаток до № 50, ст. 375.
36. Кодекс України про адміністративні правопорушення: Верховна Рада УРСР; Закон від 07.12.1984 р. № 8073-X// Відомості Верховної Ради Української РСР, 1984, № 51, ст. 1122.
37. Конституція України: Верховна Рада України; Закон від 28.06.1996 р. № 254к/96-ВР // Відомості Верховної Ради України. – 1996. – № 30. – с.141.
38. Кримінальний кодекс України: Верховна Рада України; Закон від 05.04.2001 р. № 2341-III // Відомості Верховної Ради України, 2001, № 25–26, с. 131.

39. Кримінальний процесуальний кодекс України: Верховна Рада України; Закон від 13.04.2012 р. № 4651-VI// Відомості Верховної Ради України. 2013, № 9-10, №11-12, №13, с. 88.
40. Наказ Міністерства охорони здоров’я України від 01.08.2005 № 385 «Про інфекційну безпеку донорської крові та її компонентів», зареєстрований в Міністерстві юстиції України 16 серпня 2005, № 895/11175.
41. Наказ Міністерства охорони здоров’я України від 19.03.2018 № 503 "Про затвердження Порядку вибору лікаря, який надає первинну медичну допомогу, та форми декларації про вибір лікаря, який надає первинну медичну допомогу" [Електронний ресурс]. – Режим доступу: https://moz.gov.ua/article/ministry-mandates/nakaz-moz-ukraini-vid-19032018--503-pro-zatverdzhennja-porjadku-viboru-likarja-jakij-nadae-pervinnu-medichnu-dopomogu-ta-formi-deklaracii-pro-vibir-likarja-jakij-nadae-pervinnu-medichnu-dopomogu?preview=1.
42. Основи законодавства України про охорону здоров'я: Верховна Рада України; Закон від 19.11.1992 р. № 2801-XII // Відомості Верховної Ради України, 1993, № 4, с.19.
43. Порядок здійснення Уповноваженим Верховної Ради України з прав людини контролю за додержанням законодавства про захист персональних даних, затверджений Наказом Наказ Уповноваженого Верховної Ради України з прав людини від 08.01.2014 № 1/02-14. [Електронний ресурс]. – Режим доступу: https://zakon.rada.gov.ua/laws/show/v1_02715-14#Text.
44. Порядок медичного обстеження донорів крові та (або) її компонентів, затверджений наказом Міністерства охорони здоров’я України від 01.08.2005 № 385. Зареєстрований в МОЗ України від 16 серпня 2005 р. за № 896/11176.
45. Порядок повідомлення Уповноваженого Верховної Ради України з прав людини про обробку персональних даних, яка становить особливий ризик для прав і свобод суб’єктів персональних даних, про структурний

підрозділ або відповідальну особу, що організовує роботу, пов’язану із захистом персональних даних при їх обробці, а також оприлюднення вказаної інформації: Наказ Уповноваженого Верховної Ради України з прав людини від 08.01.2014 № 1/02-14 [Електронний ресурс]. – Режим доступу: https://zakon.rada.gov.ua/laws/show/v1_02715-14#n218.

46. Порядок функціонування електронної системи охорони здоров’я, затверджений Постановою Кабінету Міністрів України від 25.04.2018 №411. [Електронний ресурс]. – Режим доступу: https://zakon.rada.gov.ua/laws/show/411-2018-%D0%BF#Text.
47. Про запобігання захворюванню на синдром набутого імунодефіциту (СНІД) та соціальний захист населення: закон України від 12 грудня 1991 року № 1972XII // Відомості Верховної Ради України, 1992, № 11, ст. 152.
48. Проект Закону України «Про права пацієнтів» від 01.03.2013 № 2438 [Електронний ресурс]. – Режим доступу: http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=45938.
49. Роз'яснення до Типового порядку обробки персональних даних: Уповноважений Верховної Ради з прав людини, 08.01.2014. База даних «Законодавство України»/ВР України. Режим доступу: https://zakon.rada.gov.ua/laws/show/n0001715-14#Text.
50. Роз'яснення основних положень Порядку повідомлення Уповноваженого щодо визначення обробки персональних даних, яка становить особливий ризик для прав і свобод суб'єктів персональних даних : Уповноважений Верховної Ради України з прав людини; Роз’яснення від 08.01.2014 [Електронний ресурс]. – Режим доступу: https://zakon.rada.gov.ua/laws/show/n0003715-14#Text.
51. Типовий порядок обробки персональних даних, затверджений наказом Уповноваженого від 08.01.2014 № 1/02–14 [Електронний ресурс]. – Режим доступу: https://zakon.rada.gov.ua/laws/show/v1_02715-14#Text.
52. Цивільний кодекс України: Верховна Рада України; Закон від 16.01.2003 № 435-IV // Інформаційний бюлетень НКРЕ, 2003, № 7.

Національні судові рішення

53. Постанова Верховного Суду від 20 травня 2019 року в справі № 487/1982/17 [Електронний ресурс]. – Режим доступу: http://reyestr.court.gov.ua/Review/81925629.
54. Постанова Верховного суду від 20 червня 2018 року у справі № 460/1849/15 [Електронний ресурс]. – Режим доступу: https://reyestr.court.gov.ua/Review/75099468.
55. Постанова Верховного суду від 21 серпня 2019 року в справі № 712/3841/17 [Електронний ресурс]. – Режим доступу: https://reyestr.court.gov.ua/Review/84005754.
56. Постанова Верховного суду від 23 вересня 2020 року у справі № 761/29995/17 [Електронний ресурс]. – Режим доступу: https://reyestr.court.gov.ua/Review/91818619
57. Постанова Верховного суду від 27 вересня 2017 року у справі № 6-1435цс17[Електронний ресурс]. – Режим доступу: https://reyestr.court.gov.ua/Review/70427210.
58. Постанова Верховного суду від 27 лютого 2019 року в справі № 474/424/18 [Електронний ресурс]. – Режим доступу: https://reyestr.court.gov.ua/Review/80522357.
59. Постанова Вінницького апеляційного суду від 10.12.2019 року у справі № 127/2999/19 [Електронний ресурс]. – Режим доступу: https://reyestr.court.gov.ua/Review/86324230.
60. Постанова Полтавського апеляційного суду від 01 липня 2020 року у справі № 554/4546/19 [Електронний ресурс]. – Режим доступу: https://reyestr.court.gov.ua/Review/90614697.
61. Рішення Компаніївського районного суду Кіровоградської області від 25 червня 2009 року у справі № 2-190/2009. [Електронний ресурс]. – Режим доступу: https://reyestr.court.gov.ua/Review/5987869.
62. Рішення Конституційного Суду України у справі щодо офіційного тлумачення ст. 3, 23, 31, 47, 48 Закону України «Про інформацію» та ст. 12

Закону України «Про прокуратуру» (справа К. Г. Устименка) від 30.10.1997 (справа № 18/203-97). [Електронний ресурс]. – Режим доступу: http://zakon3.rada.gov.ua/laws/show/v005p710-97.

Наукова література

63. Антонов С. В. Цивільно-правова відповідальність за заподіяння шкоди здоров'ю при наданні платних медичних послуг : дис. ... канд. юрид. наук : 12.00.03 / Антонов Сергій Володимирович. – К., 2006. – 206 с.
64. Бем М. В., Городиський І. М., Саттон Г., Родіоненко О. М. Захист персональних даних: Правове регулювання та практичні аспекти: науково-практичний посібник. – К.: К.І.С., 2015.
65. Бєлова Ю. Умови дійсності згоди на обробку персональних даних / Ю. Бєлова // Підприємництво, господарство і право. — 2017. —№ 11. — Р. 14–18.
66. Гуйван П.Д. Юридичне обґрунтування електронної обробки персональних даних. Актуальні проблеми вітчизняної юриспруденції № 6. Том 1.- 2018 – с. 92-96.
67. Коробцова Н.В. Деякі проблеми правової охорони медичної таємниці / Коробцова Н.В., Печений О.П. // Медичне право України: проблеми становлення та розвитку. Матеріали І Всеукраїнської науково-практичної конференції 19–20.04.2007. – С. 165-172.
68. Кохановська О.В. До питання про захист персональних даних в Україні // Вісник Верховного Суду України. - 2011. - № 6. - С. 28-33. URL: http://nbuv.gov.ua/UJRN/vvsu_2011_6_8.
69. Сенюта І. Я. Скрипець Н. Хрестоматія Рішень Європейського суду з прав людини у сфері охорони здоров'я (окремі аспекти) // Юридична газета. – № 21 (311). – 2012. – С. 15–16. [Електронний ресурс]. – Режим доступу: https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-60564%22]}.
70. Сенюта І.Я. Цивільні правовідносини у сфері надання медичної допомоги в Україні: питання теорії та практики. Дисертація на здобуття наукового ступеня доктора юридичних наук: 12.00.03 – цивільне право і

цивільний процес; сімейне право; міжнародне приватне право. — Львівський національний медичний університет імені Данила Галицького; Науково-дослідний інститут приватного права і підприємництва імені академіка Ф. Г. Бурчака Національної академії правових наук України. — Київ, 2018. — 500 с.

71. Сук И. С. Врачебная тайна. — К.: Здоров'я, 1981. — 39 с.
72. Терешко Х. Я. Доступ адвоката до персональних даних свого клієнта у сфері надання медичної допомоги // Медичне право,2019 [Електронний ресурс]. – Режим доступу :https://doi.org/10.25040/medicallaw2019.02.057.
73. Терешко Х. Я. Інформація як об'єкт цивільних правовідносин у сфері медичного обслуговування: дис. канд. юрид. наук: 12.00.03. Київ, 2019. 227 с.
74. Тихонова Б. Ю. Субъективные права советских граждан, их охрана и защита :Автореферат диссертации на соискание ученой степени кандидата юридических наук. Специальность 710 - Теория и история государства и права /Б. Ю. Тихонова ; Науч. рук. Ю. Г. Ткаченко ; Министерство высшего и среднего спеціального образования СССР. Всесоюзный юридический заочный институт. -М.,1972. – с. 11.
75. Abbas, A, Khan, M, Ali, M, Khan, S, Yang, L. A cloud based framework for identification of influential health experts from Twitter. In: Proceedings of the 15th International Conference on Scalable Computing and Communications (ScalCom) (2015), Beijing, China, pp.831-838 (2015).
76. Amit, M., Kimhi, H., Bader, T. et al. Mass-surveillance technologies to fight coronavirus spread: the case of Israel. Nat Med 26, 1167–1169 (2020). [Електронний ресурс]. – Режим доступу: https://doi.org/10.1038/s41591-020-0927-z.
77. Becher S, Gerl A, Meier B, Bölz F. Big Picture on Privacy Enhancing Technologies in e-Health: A Holistic Personal Privacy Workflow. Information 2020, 11(7), 356; https://doi.org/10.3390/info11070356.

78. Eman Abukhousa, Nader Mohamed, Jameela Al-Jaroodi. e-Health Cloud: Opportunities and Challenges July 2012 Future Internet 4(4):621-645.
79. Eysenbach, G. What is e-health? Journal of medical Internet research, 3(2), 2001. p.20.
80. Kayes, A.S.M.; Kalaria, R.; Sarker, I.; Islam, M.; Watters, P.; Ng, A.; Hammoudeh, M.; Badsha, S.; Kumara, I. A Survey of Context-Aware Access Control Mechanisms for Cloud and Fog Networks: Taxonomy and Open Research Issues. Sensors 2020, 20, 2464.
81. Li, J.; Guo, X. COVID-19 Contact-tracing Apps: A Survey on the Global Deployment and Challenges. 2020. [Електронний ресурс]. – Режим доступу: arXiv:2005.03599.
82. Li, M.; Yu, S.; Ren, K.; Lou, W. Securing Personal Health Records in Cloud Computing: Patient-centric and Fine-grained Data Access Control in Multi-owner Settings. In Proceedings of the 6th International ICST Conference on Security and Privacy in Communication Networks (SecureComm 2010), Singapore, 7–9 September 2010; pp. 89–106.
83. Mahony, M. Trust remains key barrier to eHealth. Електронний ресурс: https://euobserver.com/health/31958.
84. Nureni Ayofe Azeez, Charles Vander Vyver. Security and privacy issues in e-health cloud-based system: a comprehensive content analysis. Egyptian Informatics Journal. Volume 20, Issue 2, July 2019, p. 97-108.
85. Rahimli A. A Review of Cloud Computing Technology Solution for Healthcare System. Research Journal of Applied Sciences, Engineering and Technology 2014 8(20):2150-2153.
86. Yu, S.; Wang, C.; Ren, K.; Lou, W. Achieving secure, scalable and fine-grained data access control in cloud computing. In Proceedings of INFOCOM 2010, San Diego, CA, USA, 15–19 March 2010; pp. 1–9.
87. Zhang R, Liu L. Security models and requirements for healthcare application clouds. In: 3rd IEEE International Conference on Cloud Computing (CLOUD), Miami, FL, USA, USA, pp. 268–275 (2010).

88. Zissis D, Lekkas D. Addressing cloud computing security issues. Future Generation Computer Systems. Volume 28, Issue 3, March 2012, Pages 583-592.

Інші джерела

89. Договір між Національною службою охорони здоров'я України (Замовник) та Товариством з обмеженою відповідальністю «ДЕ НОВО» (Виконавець) №133 від 27.09.2019 року [Електронний ресурс]. – Режим доступу: https://zakupki.com.ua/tender/5431754.
90. Додаток «Дій вдома» : Google Play Market. [Електронний ресурс]. – Режим доступу: https://play.google.com/store/apps/details?id=ua.gov.diia.quarantine&hl=uk&gl=US.
91. Політика конфіденційності додатку «Дій вдома» [Електронний ресурс]. – Режим доступу: https://diia.gov.ua/policy_covid.
92. Офіційний сайт державного підприємства «Електронне здоров'я» https://ehealth.gov.ua/pidklyucheni-do-ehealth-mis/.
93. Сенюта І. Чому надані Омбудсманом роз'яснення породжують правову невизначеність? 2020 р. [Електронний ресурс]. – Режим доступу: https://advokatpost.com/advokat-seniuta-chomu-nadani-ombudsmanom-roz-iasnennia-porodzhuiut-pravovu-nevyznachenist/?fbclid=Iw.
94.Стан здійснення правосуддя у кримінальних провадженнях та справах про адміністративні правопорушення судами загальної юрисдикції у 2019 році. Верховний Суд. 17 [Електронний ресурс]. – Режим доступу: https://supreme.court.gov.ua/userfiles/media/Zbirka_analit_tablic_2019.pdf.
95. Щодо доступу до інформації про померлого членами сім'ї та близькими родичами: лист Уповноваженого Верховної Ради України з прав людини від 25.01.2018 № 2/9-К306655 17/26-138. Медичне право. 2018. № 1 (21). С. 159–163.
96. Щорічна доповідь Уповноваженого Верховної Ради України з прав людини про стан додержання та захисту прав і свобод людини і громадянина

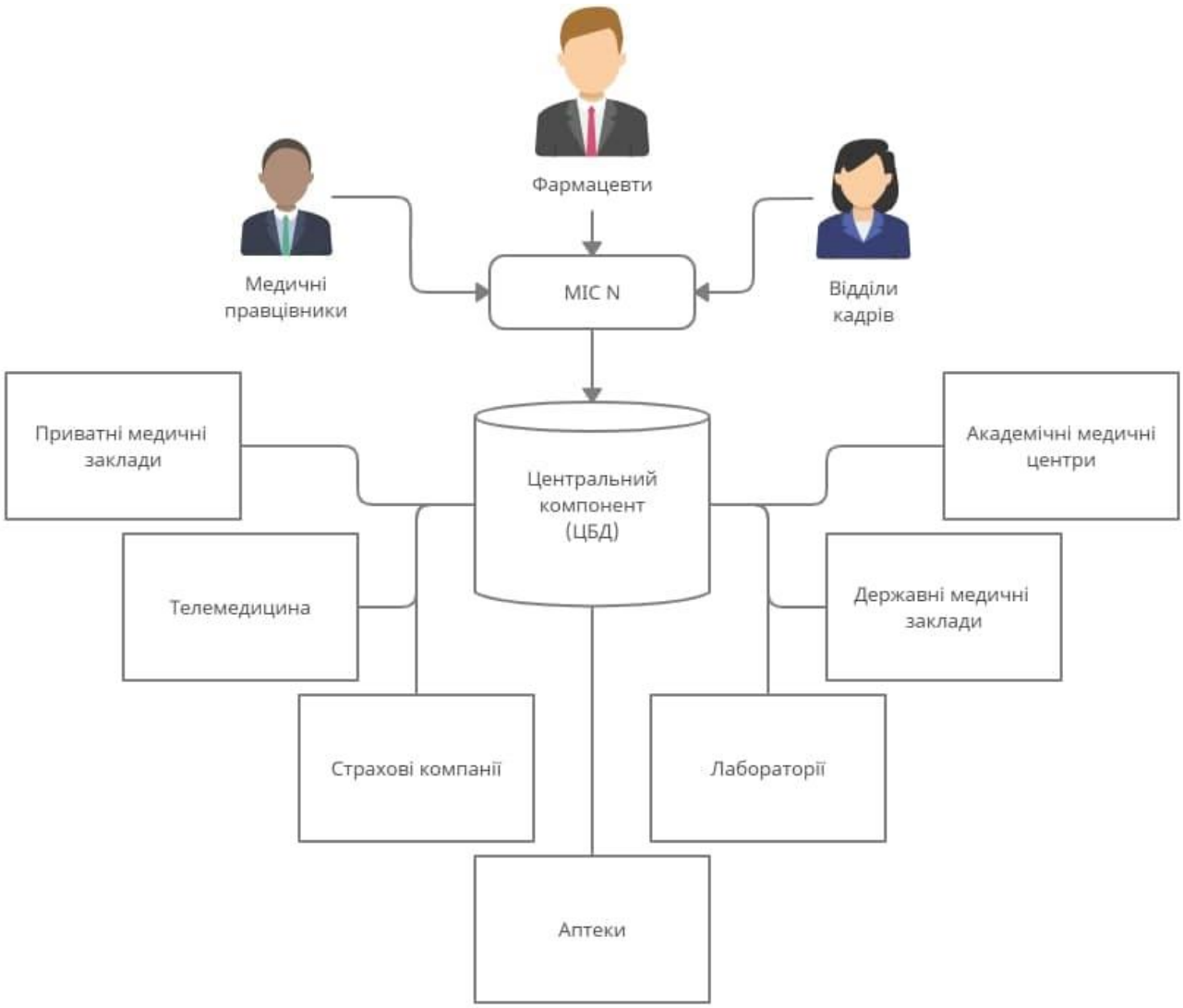
в Україні за 2019 рік. [Електронний ресурс]. – Режим доступу: https://dpsu.gov.ua/upload/zvit_za_2019.pdf.

97.Fitness tracking app Strava gives away location of secret US army bases. The Guardian. 2018. [Електронний ресурс]. – Режим доступу: https://www.theguardian.com/world/2018/jan/28/fitness-tracking-app-gives-away-location-of-secret-us-army-bases.

ДОДАТКИ

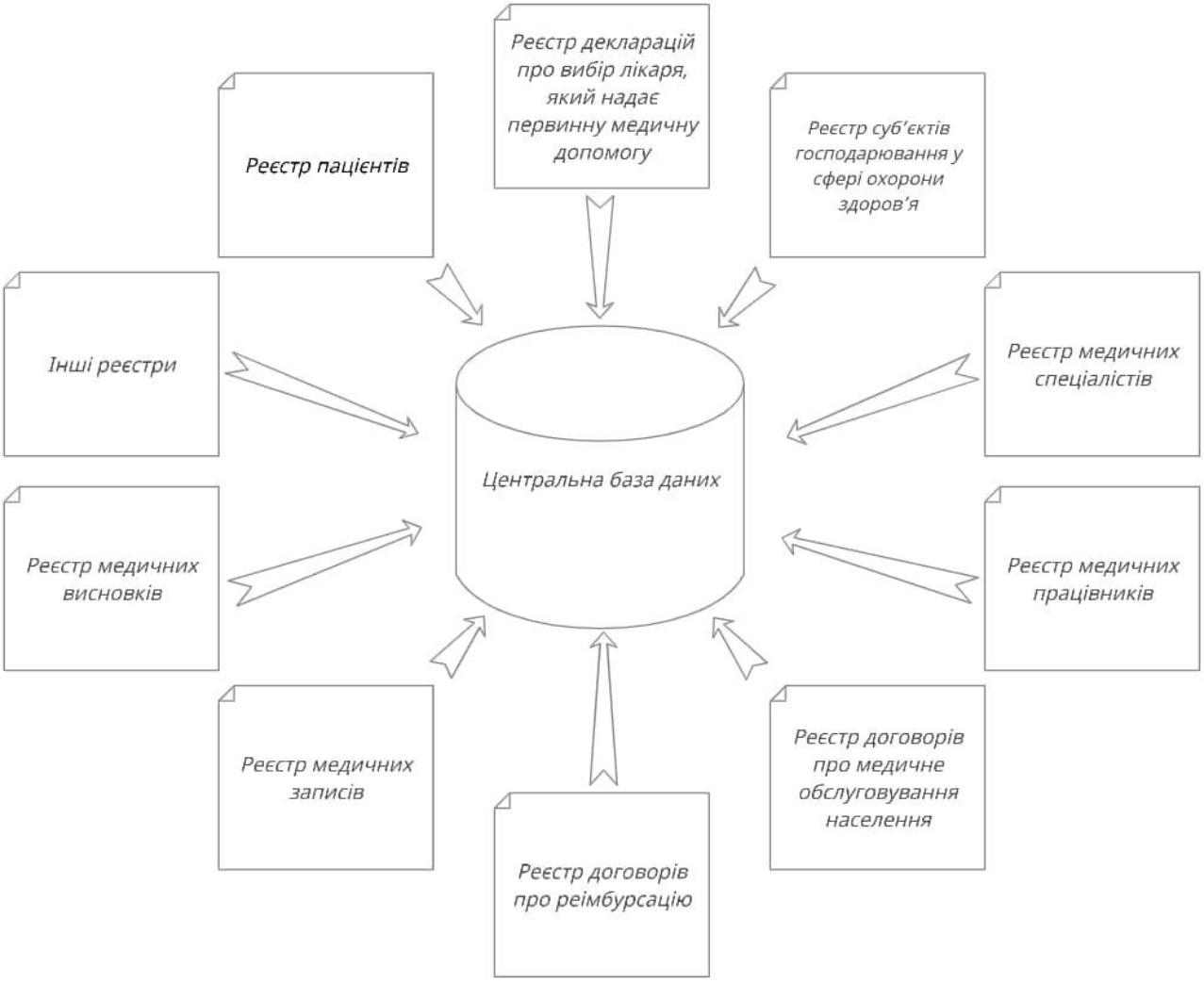
Додаток №1

Таблиця 1 «Система e-health в Україні»



Додаток №2

Таблиця 2 «Центральний компонент системи e-health в Україні»



Додаток №3

Таблиця 3 «Характеристика приватної хмари»