МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
КИЇВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ ІМЕНІ ТАРАСА ШЕВЧЕНКА
Навчально-науковий інститут права
кафедра інтелектуальної власності та інформаційного права

«До захисту у ЕК допустити»
Завідувач кафедри
інтелектуальної власності
та інформаційного права
д.ю.н., доц. Кодинець А.О.
_____

МАГІСТЕРСЬКА РОБОТА
на тему:
«Правове регулювання персональних даних у сфері охорони здоров'я»

студента 2 року навчання ОР «Магістр»
група № 2 (ІТ-право)
Спеціальність: 081 «Право»
Освітня програма «Інтелектуальна власність»
Навчально-наукового інституту права
денної форми навчання
Дрозда Владислава Руслановича

Науковий керівник:
професор, д.ю.н.,
Кулініч Ольга Олексіївна

Рецензент:
доцент, к.ю.н.,
Кашинцева Оксана Юріївна

_____

Київ - 2022

ПЛАН

ЗАТВЕРДЖЕНО:

Науковий керівник:

професор, д.ю.н.,

Кулініч Ольга Олексіївна

_____

«_____»_____ 2021 року

МАГІСТЕРСЬКЕ ЗАВДАННЯ

Дрозда Владислава Руслановича, студента 2 курсу магістратури, денної форми навчання, за спеціальністю «Право», ОНП «Інтелектуальна власність», спеціалізація «ІТ-право»

1. **Тема роботи:** «Правове регулювання персональних даних у сфері охорони здоров'я»**.**
2. **Термін здачі роботи керівнику для підготовки відгуку:** «10» травня 2022 року.
3. **Робота виконується на базі:** Інституту права Київського національного університету імені Тараса Шевченка.
4. **Теоретичне завдання:** аналіз спеціальної юридичної наукової літератури, законодавства України, дослідження досвіду зарубіжних країн; дослідження поняття, правової природи персональних даних у сфері охорони здоров'я, а також особливостей їх правового регулювання.
5. **Практичне завдання:** правовий аналіз поняття персональних даних, підстав, мети та межі їх обробки; дослідження чутливої категорії персональних даних – медичних даних; розробка можливих шляхів удосконалення законодавства про захист персональних даних та подолання колізій; аналіз та вивчення електронної системи E-Health в Україні.
6. **Сфера застосування результатів роботи:** наукова діяльність, навчальний процес, правотворчість, правозастосовна діяльність.
7. **Завдання вручено студенту:** «26» жовтня 2021 року.

ЗАТВЕРДЖЕНО:

Науковий керівник:

професор, д.ю.н.,

Кулініч Ольга Олексіївна

_____

«_____»_____ 2021 року

КАЛЕНДАРНИЙ ПЛАН

Дрозда Владислава Руслановича, студента 2 курсу магістратури, денної форми навчання, за спеціальністю «Право», ОНП «Інтелектуальна власність», спеціалізація «ІТ-право»

Тема роботи: «Правове регулювання персональних даних у сфері охорони здоров'я».

№	Види робіт	План	Фактично
1.	Підбір наукової літератури та нормативних актів за темою роботи	**08.11.2021**	**10.11.2021**
2.	Розробка плану роботи та його погодження	**25.11.2021**	**01.12.2021**
3.	Підготовка першого розділу роботи та подання його на перевірку керівнику	**26.01.2022**	**31.01.2022**
4.	Підготовка другого розділу роботи та подання його на перевірку керівнику	**12.03.2022**	**14.03.2022**
5.	Доопрацювання роботи на підставі зауважень керівника. Написання анотацій	**29.03.2022**	**01.04.2022**

6.	Написання вступу, висновків, додатків, списку використаних джерел	**06.04.2022**	**07.04.2022**
7.	Підготовка остаточного варіанту роботи та її технічне оформлення.	**09.04.2022**	**09.04.2022**
8.	Здача роботи керівнику для підготовки відгуку	**21.04.2022**	**21.04.2022**

Студент: Дрозд Владислав Русланович

АНОТАЦІЯ

У даній магістерській роботі автором розглянуто правове регулювання захисту та обробки персональних даних у сфері охорони здоров'я, визначено колізії між нормативно-правовими актами у сфері персональних даних та запропоновано шляхи їх подолання. Здійснено співставлення між наданням згоди на обробку персональних даних та договором про надання медичних послуг як підстава обробки персональних даних. Досліджено питання національної електронної системи E-Health та відповідальність за порушення законодавства у сфері персональних даних.

Ключові слова: правове регулювання, персональні дані, сфера охорони здоров'я, E-Health, згода на оброку персональних даних, договір.

Annotation

In this master's thesis, the author considers the legal regulation of protection and processing of personal data in the field of health care, identifies conflicts between regulations in the field of personal data and suggests ways to overcome them. A comparison was made between the consent to the processing of personal data and the contract for the provision of medical services as a basis for the processing of personal data. The issues of the national electronic system E-Health and the responsibility for violating the legislation in the field of personal data have been studied.

Keywords: legal regulation, personal data, health care, E-Health, consent to the processing of personal data, contract.

Анотація (розширена)

Автором у першому розділі магістерської роботи було приділено увагу загальним питання персональних даних, як: поняття персональних даних, обробка персональних даних. Разом із тим, автором дослідження було здійснено спробу визначити межі обробки персональних даних: коли законна обробка чи то на підставі Закону, чи то на підставі Згоди, перетворюється на незаконну обробку персональних даних.

При вивченні питання співвідношення персональної та конфіденційної інформації, автором було порівняно нормативно-правову базу, визначено

нормативні акти, що надають визначення «конфіденційна інформація», досліджено наукові погляди щодо цього питання та висловлено власну думку, що, при обробці персональних даних необхідно керуватися положеннями саме Закону України «Про захист персональних даних», оскільки особливості обробки та спеціальний статус персональних даних визначається цим Законом.

Автором було аргументовано та висловлено думку, чому формулювання «укладення та виконання правочину, стороною якого є суб'єкт персональних даних або який укладено на користь суб'єкта персональних даних» стосується саме договору як правочину, а не будь-якого іншого правочину.

Більш того, розмежовано порядок припинення обробки персональних даних у сфері охорони здоров'я при наданні згоди на обробку персональних даних та укладенні договору про надання медичних послуг.

Доводиться, що межами обробки персональних даних, які обробляються на підставі укладеного договору є предмет договору, однак, у разі, якщо обробка персональних даних потребується із іншою ціллю, ніж з тою, з якою укладався договір, то є необхідність в отриманні окремої згоди на обробку персональних даних або укладення нового договору.

Окрему увагу автором приділено питанню національній електронній системі E-Health. Визначено плюси даної системи та шляхи вдосконалення захисту персональних даних, які обробляються, у т.ч. зберігаються через національну систему E-Health. Досліджено питання визначення поняття E-Health та як це розуміють різні науковці. Автором підтримано загальну думку, що запровадження національної електронної системи E-Health є загалом позитивним явищем в системі охорони здоров'я так і новими можливостями для розвитку різних аспектів персональних даних.

Автором магістерської роботи було здійснено аналіз різних видів відповідальності за порушення законодавства у сфері персональних даних. Проведено градацію відповідальності за критерієм суворості відповідальності: від цивільно-правової до кримінальної відповідальності.

ВСТУП

На сьогоднішній день важко допустити думку про те, що існує людина, персональні дані, якої б не оброблялися в силу пришвидшеної глобалізації та інформатизації світу і технологій. Не могли зазнати впливу глобалізації і медичні дані як чутлива категорія персональних даних. Короновірнуса хвороба (COVID-19) звернула особливо гостру увагу на дотримання законності обробки медичних даних, порядок обробки та баланс дотримання приватного та публічного інтересів.

Затвердження постановою Кабінету Міністрів України від 25.04.2018 р. № 411 Порядок функціонування електронної системи охорони здоров'я призвело до формування національної електронної системи охорони здоров'я а отже фіксування персональних даних осіб в електронній системі охорони здоров'я з етапу підписання декларації щодо вибору сімейного лікаря та, як наслідок наступна обробка персональних даних. Запровадження електронної системи охорони здоров'я призводить до видозміни охорони медичних даних як чутливої категорії персональних даних і створення нових гарантій обробки (захисту) персональних даних пацієнтів.

Питання оброки персональних даних як і медичних даних вивчали С. В. Антонов, П. П. Андрушко, М. В. Бем, , В. В. Валах, З. С. Гладун, І. М. Городиський, 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 і т.д., проте це не применшує актуальність даної теми. 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 охорони здоров'я.

Актуальність даної теми проявляється в особливості правового регулювання персональних даних у сфері охорони здоров'я та впровадження електронної системи охорони здоров'я і її вплив на обробку персональних даних.

Визначення межі обробки персональних даних в контексті надання згоди на обробку персональних даних та договору.

Основною метою даної роботи є визначення кращих механізмів захисту медичних даних як персональних даних. Дослідження основних недоліків в національному законодавства у сфері персональних даних. Ефективність притягнення до різного виду відповідальності за порушення законодавства про захист персональних даних.

Завданням даної роботи є:

- дослідити визначення поняття «персональні дані»;
- проаналізувати обробку персональних даних та її види;
- з'ясувати межі обробки персональних даних;
- розмежувати обробку персональних даних на підставі згоди;
- провести аналіз згоди на обробку персональних даних та договору на підставі якого здійснюється обробка персональних даних;
- дослідити механізми захисту медичних даних як чутливу категорію персональних даних за законодавством України;
- порівняти персональні дані та конфіденційну інформацію;
- дослідити функціонування системи E-Health в Україні в контексті захисту персональних даних;
- визначити особливості притягнення до відповідальності за порушення законодавства України про захист персональних даних;

Об'єктом дослідження є правовідносини, що виникають під час здійснення обробки персональних даних суб'єктами та їх правове регулювання у сфері охорони здоров'я.

Предметом дослідження є правове регулювання персональних даних у сфері охорони здоров'я: зміни та розвиток, беручи до уваги аналіз нормативно-правових актів як національних так і міжнародно-правових, судової практики, наукових позицій та досліджень.

При дослідженні правового регулювання обробки персональних даних у сфері охорони здоров'я було використано такі методи дослідження, як:

- системний метод, для з’ясування місця персональних даних у сфері правового регулювання, їх вплив та взаємозв’язок із сферою охорони здоров’я;
- формально-юридичний метод використовувався для дослідження нормативно-правової бази у сфері персональних даних, як національної так і міжнародно-правової; досліджено національну та міжнародну судову практику щодо обробки персональних даних;
- метод системного аналізу застосовувався для вивчення та виявлення ефективних механізмів захисту персональних даних, у т.ч. у електронній системі охорони здоров’я;
- звернення до методу тлумачення норм права тісно пов’язане із застосуванням формально-юридичного методу, що проявлялося у розумінні справжнього сенсу норм права;

Таким чином, у даній магістерській роботі було ґрунтовно та всебічно досліджено аспекти правового регулювання персональних даних у сфері охорони здоров’я, виявлено недоліки та, як наслідок, перспективи удосконалення і розвитку правового регулювання.

У силу глобальної та швидкої інформатизації суспільства, дослідження питання захисту персональних даних залишатиметься й досі відкритим, оскільки розвиток технологій, швидкість обробки та обміну інформації (даних) постійно кидатимуть виклик праву як суспільному регулятору щодо захисту персональних даних суб’єкта, у тому числі у сфері охорони здоров’я.

РЕФЕРАТИВНИЙ ОГЛЯД ВИКОРИСТАНИХ ДЖЕРЕЛ

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.

При написанні магістерської роботи була опрацьована докторська дисертація І. Я. Сенюти «Цивільні правовідносини у сфері надання медичної допомоги в Україні: питання теорії та практики» (2018), де було досліджено питання право на інформацію суб'єкта персональних даних в контексті медичних даних, у тому числі, особливості обробки медичних даних та надання до них доступу студентам до, право на медичну таємницю.

Досліджено науково-практичний посібник Бема М. В., Городиського І. М., Саттона Г., Родіоненко О. М. «Захист персональних даних: Правове регулювання та практичні аспекти» (2015), у якому висвітлюється питання захисту персональних даних, межі обробки персональних даних, розмежовуються підстави для обробки персональних даних.

Науково-практичний посібник Бема. М.В., Городиського І.М. «Захист персональних даних: правове регулювання та практичні аспекти» (2021), який є оновленою версією посібника 2015 року, що ґрунтовно доповню зміст посібника 2015 року, тим самим виступаючи ще одним ключовим джерелом при розумінні досліджуваної теми та аналізу необхідної інформації.

Посібник з європейського права у сфері захисту персональних даних у якому представлено огляд права Європейського Союзу та Ради Європи з питань захисту персональних даних із посиланням та аналізом відповідної судової практики – як Європейського суду з прав людини так і Європейського суду справедливості та коментарями європейських нормативно-правових актів у сфері персональних даних.

Поряд із науковими джерелами, було досліджено правові висновки Верховного Суду щодо питання обробки персональних даних (в контексті отримання згоди на обробку персональних даних) – а саме постанова ВС/КЦС від 06.12.2019 № 664/1261/160, постанова ВС/КЦС від 16.10.2019 №

752/10234/16, у яких зазначено, що встановлення режиму «безвідкличної» згоди є таким, що не відповідає положенням Закону України «Про захист персональних даних» та Закону України «Про захист прав споживачів».

Рішення Європейського суду з прав людини та суду ЄС щодо меж обробки персональних даних та їх законності (медичних даних), підстав обробки персональних даних. - Рішення Суду ЄС, C-212/13, «Франтішек Ринеш проти Офісу захисту персональних даних», (František Ryneš v. Úřad pro ochranu osobních údajů), від 11 грудня 2014 р., п. 25., Справа «Боділ Ліндквіст», («L. H. v. Latvia», заява № 52019/07.

Більш того, автором дослідження здійснено аналіз нормативно-правових актів, як національних: Закону України «Про захист персональних даних», що є основним національним актом у сфері персональних даних, Закону України «Про інформацію», у якому здійснено, із врахуванням наукових позицій, співвідношення конфіденційної інформації та персональних даних, Конституція України та інші відомчі нормативно-правові акти, що прямо чи опосередковано стосуються сфери персональних даних; так і нормативно-правові акти ЄС: Конвенція про захист осіб у зв'язку з автоматизованою обробкою персональних даних Страсбург, 28 січня 1981 року, конвенція про захист прав людини і основоположних свобод 1950 року.

РОЗДІЛ 1. ЗАГАЛЬНІ ПОЛОЖЕННЯ ПРО ПЕРСОНАЛЬНІ ДАНІ

1.1. Поняття персональних даних.

Персональні дані оточують нас повсюди, розпочинаючи із ініціалів особи (П.І.Б.) закінчуючи даними з медичної картки, політичними поглядами та релігійними вподобаннями тому перед тим, як перейти до питань, які безпосередньо стосуються правового регулювання захисту персональних даних, необхідно визначитися, що саме собою являє поняття «персональних даних».

Поняття «персональні дані», перш за все міститься у Законі України «Про захист персональних даних», де зазначено, що персональними даними є відомості чи сукупність відомостей про фізичну особу, яка ідентифікована або може бути конкретно ідентифікована (ст. 2 Закону України «Про захист персональних даних»).[1]

Загальний регламент (ЄС) 2016/679 захисту фізичних осіб в зв'язку з обробкою персональних даних та вільних рух таких даних (Regulation (EU) 2016/679 (General Data Protection Regulation), у розділі I, ст. 4 визначається, що під персональними даними розуміється будь-яка інформація, що стосується фізичної особи, яку ідентифіковано чи можна ідентифікувати («суб'єкт даних»);[2]

У Конвенції про захист осіб у зв'язку з автоматизованою обробкою персональних даних від 28.01.1981, закріплено, що термін "персональні дані" означає будь-яку інформацію, яка стосується конкретно визначеної особи або особи, що може бути конкретно визначеною (далі - суб'єкт даних)[3]

Разом із тим, необхідно звернути увагу на ще один нормативно-правовий акт: законопроект 5628 (Проект Закону України «Про захист персональних даних»), яким надається визначення, що персональні дані — будь-яка

[1] Про захист персональних даних: Закон України від 01 червня 2010 року № 2297-VI// Відомості Верховної Ради України (ВВР) – 2010. - № 34. - ст. 481;

[2] Регламент Євопейського 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). Офіційна інтернет-сторінка Верховної Ради України – Режим доступу: https://zakon.rada.gov.ua/laws/show/984_008-16#Text;

[3] Конвенція про захист осіб у зв'язку з автоматизованою обробкою персональних даних від 28.01.1981. Конвенцію ратифіковано із заявами згідно із Законом N 2438-VI (2438-17) від 06.07.2010.). Офіційна інтернет-сторінка Верховної Ради України – Режим доступу: https://zakon.rada.gov.ua/laws/show/994_326#Text

інформація, що стосується фізичної особи, яку ідентифіковано або може бути ідентифіковано.[4]

Тобто поняття «персональних даних», у Конвенції про захист осіб у зв'язку з автоматизованою обробкою персональних даних від 28.01.1981, Загальному регламенті (ЄС) 2016/679 захисту фізичних осіб в зв'язку з обробкою персональних даних та вільних рух таких даних та законопроекті 5628 є ідентичними.

Разом із тим, із цих визначень вбачається словосполучення «фізична особа, яка може бути ідентифікована». Розкриття цього словосполучення міститься у Загальний регламент (ЄС) 2016/679 захисту фізичних осіб в зв'язку з обробкою персональних даних та вільних рух таких даних (Regulation (EU) 2016/679, якою роз'яснюється, що фізична особа, яку можна ідентифікувати, є такою особою, яку можна ідентифікувати, прямо чи опосередковано, зокрема, за такими ідентифікаторами як ім'я, ідентифікаційний номер, дані про місцеперебування, онлайн-ідентифікатор або за одним чи декількома факторами, що є визначальними для фізичної, фізіологічної, генетичної, розумової, економічної, культурної чи соціальної сутності такої фізичної особи (5.)[5] Тобто, ідентифікована – особа, яку за наявною в розпорядженні володільця інформацією можна безпомилково виділити з-посеред інших осіб.

Отже, наявність певного обсягу та кількості інформації, за складених умов та для відповідної особи, може бути достатньо, щоб вважати фізичну особу такою, що може бути ідентифікованою. Як приклад, у науково-практичному посібнику «Захист персональних даних: Правове регулювання та практичні аспекти», наводиться наступне: «У районному відділі соціального захисту розвішується інформація щодо надання конкретним жителям району соціальних послуг і соціального обслуговування з вказівкою прізвища, ініціалів особи та

[4] Про захист персональних даних. Законопроект № 5628 від 07.06.2021. Офіційна інтернет-сторінка Верховної Ради України - http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=72160;

[5]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). Офіційна інтернет-сторінка Верховної Ради України – Режим доступу: https://zakon.rada.gov.ua/laws/show/984_008-16#Text;

виду наданої послуги. Такої інформації в багатьох випадках буде достатньо для того, щоб провести ідентифікацію особи.»[6]

Коли питання стосується «особи, яка може бути ідентифіковано», то є необхідним не лише інформація особи про її ім'я та інші «прийнятні/широко розповсюджені» ознаки, а й безапеляційне виокремлення такої особи з невизначеного кола інших осіб, за допомогою додаткових відомостей.

Часто мається на увазі ідентифікація особи на базі відомостей, які, якщо взяті окремо, не дають можливості ідентифікувати особу, однак у поєднанні уможливлюють це[7].

Персональні даній вміщують у собі певну категорію персональних даних, які називаються спеціальні (або більш характерно – чутливі категорії персональних даних):

Расове або етнічне походження; політичні, релігійні або світоглядні переконання; членство в політичних партіях і професійних спілках; засудження до кримінального покарання; стан здоров'я, статеве життя; біометричні або генетичні дані.

Обробка таких даних, перш за все, має відбуватися із дотриманням певних механізмів та стандартів захисту, що передбачаються вищеназваним як міжнародно-правовими актами так і на національному рівні.

В основі такого поділу лежить те, що вказані категорії персональних даних мають у собі інформацію щодо ознак, які часто можуть стати підставою для дискримінаційного ставлення до відповідного суб'єкта персональних даних[8].

1.2. Обробка персональних даних. Особливості обробки медичних даних.

Відповідно до Закону України «Про захист персональних даних» обробка персональних даних - будь-яка дія або сукупність дій, таких як збирання, реєстрація, накопичення, зберігання, адаптування, зміна, поновлення,

[6] Захист персональних даних: Правове регулювання та практичні аспекти: науково-практичний посібник./ Бем М. В., Городиський І. М.– К.: К.І.С., 2021. – с. 20.
[7] Захист персональних даних: Правове регулювання та практичні аспекти: науково-практичний посібник./ Бем М. В., Городиський І. М.– К.: К.І.С., 2021. – с. 20.
[8] Захист персональних даних: Правове регулювання та практичні аспекти: науково-практичний посібник./ Бем М. В., Городиський І. М.– К.: К.І.С., 2021. – с. 20.

використання і поширення (розповсюдження, реалізація, передача), знеособлення, знищення персональних даних, у тому числі з використанням інформаційних (автоматизованих) систем [9].

Обробка персональних даних може здійснюватися як з використанням автоматизованих систем (автоматизована обробка) так і в ручну (неавтоматизована обробка).

Автоматизована обробка зачіпає операції, що здійснюються щодо персональних даних повністю або частково автоматизованими засобами.

У практичному вимірі це означає, що будь-яка обробка персональних даних за допомогою автоматизованих засобів, наприклад, персонального комп'ютера, мобільного додатку або роутера охоплюється як правилами захисту персональних даних ЄС, так і правилами РЄ [10].

У справі «Франтішек Ринеш» проти Офісу захисту персональних даних пан Ринеш за допомогою домашньої системи ТВ-спостереження записав зображення двох осіб, які розбили вікна в його будинку. Суд зазначив, що спостереження у формі відеозйомки осіб, як у справі, яка перебуває на розгляду у суді, який зберігається на пристрої безперервного запису — жорсткому диску — становить, відповідно до Стаття 3(1) Директиви 95/46, автоматична обробка персональних даних[11].

Справа «Боділ Ліндквіст» стосувалася посилання на веб-сторінці на різних осіб шляхом зазначення їхніх імен або іншим чином, наприклад шляхом зазначення їхніх телефонних номерів або інформації про їхні хобі. Суд підкреслив, що «акт посилання на Інтернет-сторінці, різним особам та ідентифікувати їх по імені чи іншим чином означає, наприклад, вказавши свій номер телефону або інформацію щодо їх умови роботи та захоплення, становить

[9] Про захист персональних даних: Закон України від 01 червня 2010 року № 2297-VI// Відомості Верховної Ради України (ВВР) – 2010. - № 34. - ст. 481

[10] Посібник з європейського права у сфері захисту персональних даних./ Переклад В. Костеллі — К.: К.І.С., - с. 111

[11] Рішення Суду ЄС, С-212/13, «Франтішек Ринеш проти Офісу захисту персональних даних» (František Ryneš v. Úřad pro ochranu osobních údajů), від 11 грудня 2014 р., п. 25. – Режим доступу: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:62013CJ0212

«обробку персональних даних повністю або частково автоматичними засобами» в сенсі статті 3 (1) Директиви 95/46.[12]

Одночасно із цим, слід зазначити, що дія Закону України «Про захист персональних даних не поширюється (не застосовується) під час обробки персональних даних, що використовуються у приватних цілях, журналістських та або/творчих цілях (ч.ч. 2,3 ст. 25).

Тобто, у Законі України «Про захист персональних даних» містяться прямі імперативні виключення, до процесів та сфер діяльності/життя, на які не поширюється дія Закону України «Про захист персональних даних».

Таким чином, можна дійти до висновку, що положення Закону України «Про захист персональних даних» у будь-якому разі поширюються на сферу охорони здоров'я , і така обробка може здійснюватися як в автоматизованому режимі (автоматизована обробка) так і в неавтоматизованому.

Однак, межі обробки персональних даних обмежуються метою їх обробки. У разі, якщо обробка персональних даних виходитиме за межі мети обробки, така обробка вважатиметься незаконною.

Так відповідно до справа «L. H. v. LATVIA» 1997 року заявниці довелося терміново робити кесарів розтин. У ході операції хірург без згоди на те заявниці провів стерилізацію. Інспекція, що вела контроль за якістю надання медичної допомоги, провела перевірку щодо цього інциденту. З цією метою вона зібрала відомості щодо надання заявниці медичної допомоги з 1996 по 2003 роки. Заявниця оскаржила факт збору чутливої інформації щодо неї інспекцією, однак суди відмовили в задоволенні її позову. Досліджуючи питання необхідності збору інформації щодо заявниці, Суд, серед іншого, звернув увагу на те, що інспекція зібрала непропорційно великий обсяг інформації (за період тривалістю сім років (за рік до операції та 6 після) з 3-х установ), щоб оцінити одне хірургічне втручання в 1997 році. Цьому не надано жодного обґрунтування.

[12] Суд ЄС, C-101/01, Кримінальне провадження проти Bodil Lindqvist (Criminal proceedings against Bodil Lindqvist), від 6 листопада 2003 р., п. 27. – Режим доступу: https://eur-lex.europa.eu/legal content/EN/TXT/?qid=1512480526556&uri=CELEX:62001CJ0101

Тому Суд констатував непропорційність втручання в права заявниці, гарантовані статтею 8 Конвенції. («L. H. v. Latvia», заява № 52019/07)[13]

За Конвенцією 108 (Конвенція про захист осіб у зв'язку з автоматизованою обробкою персональних даних Страсбург, 28 січня 1981 року - із внесенням змін (протокол протоколом CETS № 223 від травня 2018 року) обробка персональних даних - «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».[14]

Необхідно звернути увагу на проблематику, що прослідковується через системне вивчення положень Закону України «Про захист персональних даних» - а саме співвідношення понять: «обробка», «використання» та «захист».

Частиною 1 ст. 10 Закону України «Про захист персональних даних» до використання персональних даних віднесено дії щодо захисту персональних даних. Однак, в ст. 2 Закону України «Про захист персональних даних» у дефініції поняття «обробка персональних даних» законодавець обґрунтовано, на нашу думку, закріпив одним із її елементів «використання», натомість «захисту» там немає.[15]

Тому неможливо не погодитися із позицією Бема М. В., Городиського І. М., Саттона Г. та іншими, що захист персональних даних необхідно відмежовувати від обробки, оскільки захист не передбачає вчинення окремих дій з персональними даними, а тому є (має) бути категорією, яку необхідно відмежовувати від поняття їх «обробки» та «використання».

---

[13] «L. H. v. Latvia», заява № 52019/07, рішення від 29/04/2014

[14] Конвенція про захист осіб у зв’язку з автоматизованою обробкою персональних даних від 28.01.1981. Конвенцію ратифіковано із заявами згідно із Законом N 2438-VI (2438-17) від 06.07.2010.). Офіційна інтернет-сторінка Верховної Ради України – Режим доступу: https://zakon.rada.gov.ua/laws/show/994_326#Text;

[15] Про захист персональних даних: Закон України від 01 червня 2010 року № 2297-VI// Відомості Верховної Ради України (ВВР) – 2010. - № 34. - ст. 481

Натомість, «використання» доцільно розглядати як один із видів «обробки» персональних даних[16].

Окрему увагу необхідно звернути на підстави обробки медичних даних про особу.

Статтею 32 Конституції України закріплено, що 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.[17]

Виходячи із зазначеного, можемо дійти висновку, що збирання, зберігання, використання поширення та/або будь-які інші дії щодо обробки персональних даних (у тому числі і медичні дані особи) можливі виключно на підставі згоди особи або у випадках, які визначені у законі та лише в інтересах національної безпеки, економічного добробуту та прав людини.

Пунктом 2.7 Типового порядку обробки персональних даних, що затверджений наказом Уповноваженого від 08.01.2014 № 1/02–14, передбачено, що обробка персональних даних здійснюється володільцем персональних даних лише за згодою суб'єкта персональних даних, за винятком тих випадків, коли така згода не вимагається Законом.[18]

Підкреслимо, що володільцем медичних даних у сфері охорони здоров'я є як заклад охорони здоров'я, фізична особа - підприємець, або юридична особа яка одержала ліцензію на провадження господарської діяльності з медичної практики.

Обробка медичних даних як вид «чутливих» даних, за загальним правилом, є забороненою (ч.1 ст.7 Закону). Проте, така заборона не застосовується у

[16] 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. – 56 с.

[17] Конституція України від 28.06.1996 № 254к/96-ВР// Відомості Верховної Ради України (ВВР) – 1996. - № 30. – ст. 141

[18] Типовий порядок обробки персональних даних: наказ Уповноваженого Верховної Ради України з прав людини 08.01.2014 № 1/02-14. Офіційна інтернет-сторінка Верховної Ради України – Режим доступу: https://zakon.rada.gov.ua/laws/show/v1_02715-14#Text

випадках, визначених в ч.2. ст.7 Закону України «Про захист персональних даних»[19]. 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.»

Із набранням чинності нової редакції ст. 7 Закону України «Про захист персональних даних» від 30.01.2018, скасування наказу МОЗ України форми «Інформована добровільна згода пацієнта на обробку персональних даних» (Наказ Міністерства охорони здоров’я України від 8 серпня 2014 р. № 549), вилученням пункту 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[20] (далі наказ

[19] Про захист персональних даних: Закон України від 01 червня 2010 року № 2297-VI// Відомості Верховної Ради України (ВВР) – 2010. - № 34. - ст. 481

[20] Про затвердження Порядку вибору лікаря, який надає первинну медичну допомогу, та форми декларації про вибір лікаря, який надає первинну медичну допомогу. Наказ Міністерства охорони здоров’я України від 19.03.2018 № 503. Офіційна інтернет-сторінка Верховної Ради України – Режим доступу: https://moz.gov.ua/article/ministry-mandates/nakaz-moz-ukraini-vid19032018--503-pro-zatverdzhennja-porjadku-viboru-likarja-jakij-nadae-pervinnu-medichnu-dopomogu-ta-formideklaracii-pro-vibir-likarja-jakij-nadae-pervinnu-medichnu-dopomogu?preview=1;

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 сьогодні, в пункті 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.

Вважаємо, що наразі редакція Декларації про вибір лікаря, який надає первинну медичну допомогу, цілком відповідає чинним вимогам Закону України «Про захист персональних даних»

Однак, оскільки законодавець не систематизовано вносить зміни до пов'язаних між собою нормативно-правових актів, вибудувалася колізія між положеннями Закону України «Про захист персональних даних» та Закону України «Про державні фінансові гарантії медичного обслуговування населення»[21]. Так наприклад, в ч.2 та ч.3 ст.11 Закону «Про державні фінансові гарантії медичного обслуговування населення» закріплена можливість доступу до даних про пацієнта, що містяться в електронній системі охорони здоров'я, можливий лише у разі отримання згоди такого пацієнта (його законного представника) у письмовій формі або у формі, що дає змогу зробити висновок про надання згоди та необхідність надання згоди на доступ до даних про нього, що містяться в електронній системі охорони здоров'я, такому лікарю.

Такі положення суперечать п.6 ч.2 ст. 7 Закону України «Про захист персональних даних», в якому закріплено можливість обробки персональних даних пацієнта (його законного представника) конкретними суб'єктами за вищенаведеної мети без отримання окремої згоди. Колізія положень

[21] Про державні фінансові гарантії медичного обслуговування населення. Закон України 19.10.2017 № 2168-VIII. Офіційна інтернет-сторінка Верховної Ради України – Режим доступу: https://zakon.rada.gov.ua/laws/show/2168-19#Text

нормативно-правових актів має вирішуватися на користь Закону України «Про захист персональних даних, оскільки він є спеціальним через пряму вказівку в ч.1 ст. 7 Закону України «Про державні фінансові гарантії медичного обслуговування населення».

Аналогічну думку, із якою ми погоджуємося, висловлює І. Сенюта[22].

Наступний нормативно-правовий акт, який, на наш погляд, не повністю відповідає положенням Закону України «Про захист персональних даних» є підпункт 5 пункту 8 Порядку функціонування електронної системи охорони здоров'я, затверджений постановою КМУ від 25.04.2018 № 411[23] (далі – Порядок № 411), де закріплені функціональні можливості 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, лікарям, третім особам.

Пункт 30 Порядку № 411 надає 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

Беручи до уваги, що Закон України «Про захист персональних даних» не вимагає надання згоди на обробку персональних даних у медичних цілях, суперечливими є положення про можливість відкликання такої згоди пунктом 30 Порядку № 411.

Отже, враховуючи існування колізій у вищенаведених нормативно-правових актів по відношенню до положень Закону України «Про захист персональних даних» у правовому регулюванні підстав для обробки персональних, є необхідність в узгоджені Закону України «Про державні

[22] Сенюта І. Чому надані Омбудсманом роз'яснення породжують правову невизначеність? – Режим доступу: https://advokatpost.com/advokat-seniuta-chomu-nadani-ombudsmanom-roz-iasnennia-porodzhuiut-pravovu-nevyznachenist/

[23] Порядок функціонування електронної системи охорони здоров'я. Постанова Кабінету Міністрів України від 25 квітня 2018 р. № 411 // Офіційна інтернет-сторінка Верховної Ради України – Режим доступу: https://zakon.rada.gov.ua/laws/show/411-2018-%D0%BF#Text

фінансові гарантії медичного обслуговування населення» та Порядку №411 відповідно до Закону України «Про захист персональних даних» аналізуючи ч.1 ст. 7 Закону України «Про державні фінансові гарантії медичного обслуговування населення», застосуванню підлягають саме положення Закону України «Про захист персональних даних» та методи подолання колізій у правовому полі.

1.3. Персональні дані та конфіденційна інформація.

Законом України «Про інформацію» передбачено (запроваджено) два поняття: «персональні дані» та «конфіденційна інформація».

Законом України «Про інформацію» визначено, що інформація про фізичну особу (персональні дані) - відомості чи сукупність відомостей про фізичну особу, яка ідентифікована або може бути конкретно ідентифікована (ч.1 ст. 11)[24]. Не допускаються 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 захисту прав людини. До конфіденційної інформації про фізичну особу належать, зокрема, дані про її національність, освіту, сімейний стан, релігійні переконання, стан здоров'я, а також адреса, дата і місце народження.

Конфіденційна інформація - є інформація про фізичну особу, а також інформація, доступ до якої обмежено фізичною або юридичною особою, крім суб'єктів владних повноважень. Конфіденційна інформація може поширюватися за бажанням (згодою) відповідної особи у визначеному нею порядку відповідно до передбачених нею умов, а також в інших випадках, визначених законом (ч. 1 ст. 23)[25].

Виходячи із аналізу поняття, «персональні дані» стосуються характеру інформації (інформація щодо фізичної особи), поняття «конфіденційна інформація» стосується характеру відкритості інформації а також режим доступу

[24] Про інформацію. Закон України від 02.10.1992 № 2657-XII // Офіційна інтернет-сторінка Верховної Ради України – Режим доступу: https://zakon.rada.gov.ua/laws/show/2657-12#Text

[25] Про інформацію. Закон України від 02.10.1992 № 2657-XII // Офіційна інтернет-сторінка Верховної Ради України – Режим доступу: https://zakon.rada.gov.ua/laws/show/2657-12#Text

до такої інформації (накладення певних обмежень щодо обробки такої інформації) . Отже за функціональною складовою та історичним обумовлення виникнення цих двох понять та/або категорій, відмінність чітко не прослідковується – а отже потребує додаткового вивчення, задля чіткого розмежування, та виявлення, на що розповсюджується режим «конфіденційності» установ та закладів охорони здоров'я, та як співвідносяться «персональні дані» і «конфіденційна інформація».

Беручи до уваги, що персональні дані стосуються лише інформації щодо фізичної особи, а конфіденційна інформація може бути інформацією і щодо юридичної особи (кількість співробітників, внутрішня політика певною юридичної особи). Разом із тим, інформація про особу, що може бути у відомості юридичної особи, підпадає як під «персональні дані», а отже під дію Закону України «Про захист персональних даних» так і під положення Закону України «Про інформацію» щодо режиму конфіденційності інформації, яка знаходиться у володінні юридичної особи, внаслідок здійснення певного виду діяльності.

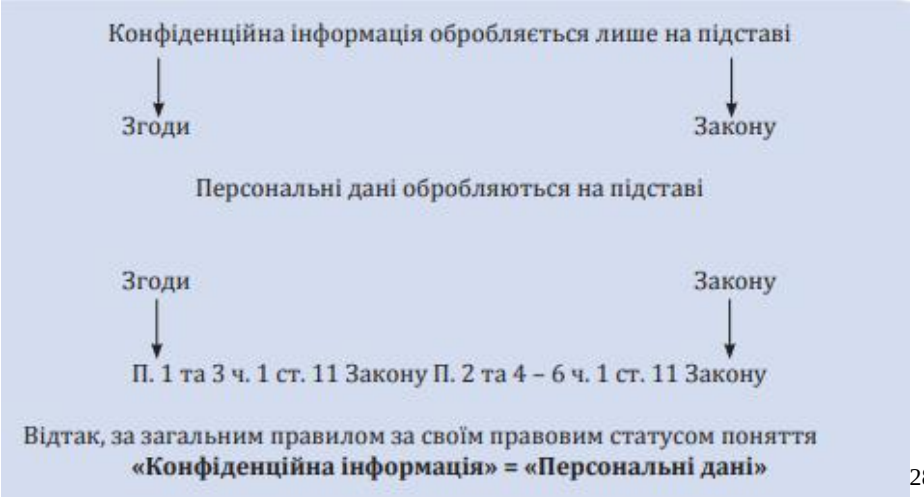
Виходячи з цього, якщо персональні дані (всі чи окремі категорії) не охоплюються поняттям конфіденційної інформації, вони повинні розглядатися як відкрита інформація, а відтак можуть оброблятися фактично без обмежень. Ті ж персональні дані, що належать до конфіденційної інформації, можуть оброблятися лише за згодою суб'єкта або на підставі закону. Однак, законодавчі положення щодо віднесення персональних даних до конфіденційної інформації є суперечливими[26].

Відповідно до ч. 2 ст. 5 Закону України «Про захист персональних даних» персональні дані можуть бути віднесені до конфіденційної інформації про особу законом або відповідною особою. Статтею 11 вищезазначеного закону передбачено обробка персональних даних на підставі згоди чин а підставі Закону[27].

[26] 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. – 55 с.

[27] Про захист персональних даних: Закон України від 01 червня 2010 року № 2297-VI// Відомості Верховної Ради України (ВВР) – 2010. - № 34. - ст. 481

Із врахуванням ст. 11, 21 Закону України «Про інформацію» та ст. 5,11 Закону України «Про захист персональних даних» встановлюється фактична презумпція відкритості персональних даних.



[28]

Тому, за формального тлумачення вищезазначених законодавчих нормативно-правових актів, як персональні дані, як і конфіденційна інформація, можуть оброблятися лише за наявності згоди особи або на підставі закону.

Таким чином, логічним видається ототожнення понять персональних даних та конфіденційної інформації.[29]

Окрім цього, конкретні підстави обробки персональних даних передбачені ст.7 і ст. 11 Закону України «Про захист персональних даних», які також ґрунтуються на тому, що обробка здійснюється на підставі згоди або Закону, що органічно поєднується із рештою законодавства України.

У зв'язку із цим, не прив'язуючись до понять конфіденційної інформації чи інформації з обмеженим доступом, при обробці персональних даних слід виходити саме з указаних положень Закону України «Про захист персональних даних», оскільки особливості обробки та спеціальний статус персональних даних визначається саме цим Законом.

Таким чином, підприємства, установи та організації у сфері охорони здоров'я, при обробці інформації про фізичну особу, надання доступу до такої

[28] 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. – 56 с.
[29] 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. – 56 с.

інформації її збирання, реєстрація, накопичення, зберігання, адаптування, зміна, поновлення, використання і поширення (розповсюдження, реалізація, передача), знеособлення, знищення мають керуватися нормами Закону України «Про захист персональних даних», неважливо коли це стосується інформації щодо пацієнта, або щодо працівника такої установи.

Висновки до розділу І

1. Персональні дані стосуються виключно фізичної особи. Будь-які дані про фізичну особу можна віднести до персональних даних, у разі якщо такі дані, при відповідних обставинах, дадуть можливість ідентифікувати фізичну особу.
2. У сфері охорони здоров'я здійснюється як автоматизована так і неавтоматизована обробка персональних даних.
3. Обробка персональних даних завжди обмежується метою такої обробки, тобто межі обробки персональних даних прямо пов'язані із метою обробки персональних даних. У разі, якщо обробка персональних даних виходить за межі мети обробки персональних даних – обробка є незаконною та має бути негайно припинена.
4. Є необхідність в узгоджені Закону України «Про державні фінансові гарантії медичного обслуговування населення» та Порядку №411 відповідно до Закону України «Про захист персональних даних» аналізуючи ч.1 ст. 7 Закону України «Про державні фінансові гарантії медичного обслуговування населення», застосуванню підлягають саме положення Закону України «Про захист персональних даних» та методи подолання колізій у правовому полі.
5. Виходячи із положень наявних нормативно-правових актів (Закон України «Про захист персональних даних» та Закон України «Про інформацію») конфіденційна інформація = персональним даним.
6. При обробці персональних даних фізичної особи, необхідно керуватися та дотримуватися положень Закону України «Про захист персональних даних», оскільки особливості обробки та спеціальний статус персональних даних визначається саме цим Законом та для запобігання колізій із Законом України «Про інформацію».

РОЗДІЛ 2. ОБРОБКА ПЕРСОНАЛЬНИХ ДАНИХ НА ПІДСТАВІ ЗГОДИ

2.1. **Згода на обробку 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. (абз. 3 ст. 2 Закону України «Про захист персональних даних»)[30].

Під згодою суб'єкта на обробку персональних даних слід розуміти добровільне, поінформоване, конкретне, однозначне волевиявлення суб'єкта персональних даних у письмовій формі або іншій формі, в тому числі у формі конклюдентних дій, що безсумнівно підтверджує його дозвіл на обробку персональних даних відповідно до сформульованої мети їх обробки.[31]

Піддаючи аналізу дане визначає, вбачається, що згода суб'єкта на обробку персональних даних передбачає три аспекти.

Добровільність згоди проявляється у відсутності прямого чи опосередкованого примусу при її наданні.

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»[32]. Зокрема, опосередкований примус може виникнути, зокрема, якщо отримання 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.

---

[30] Про захист персональних даних: Закон України від 01 червня 2010 року № 2297-VI// Відомості Верховної Ради України (ВВР) – 2010. - № 34. - ст. 481

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

[32] 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. Режим доступу: https://zakon.rada.gov.ua/laws/show/n0003715-14#Text

Так, наприклад у п. 43 Регламенту 2016/679 закріплюється: «Щоб забезпечити, щоб 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»[33]

Поінформованість: перед наданням згоди на обробку персональних даних суб'єкт повинен отримати вірогідну інформацію про те, хто, з якою метою буде обробляти його персональні дані, кому будуть передаватися ці дані, які саме дані (склад даних), а також про права, визначені Законом України «Про захист персональних даних». Така інформація повинна бути надана в доступному вигляді і володілець повинен за будь-яких умов мати можливість підтвердити факт надання такої інформації суб'єктові.[34]

Форма надання згоди може бути фактично будь-якою. Однозначність згоди не повинна викликати сумнівів і володілець повинен мати змогу підтвердити її наявність упродовж усього часу проведення обробки персональних даних.[35]

Внаслідок існування так званих чутливих персональних даних (у т.ч. щодо інформації про стан здоров'я особи), у національному законодавстві було закріплено додатковий критерій – однозначність.

---

[33] 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). Офіційна інтернет-сторінка Верховної Ради України – Режим доступу: https://zakon.rada.gov.ua/laws/show/984_008-16#Text;

[34] Захист персональних даних: Правове регулювання та практичні аспекти: науково-практичний посібник./ Бем М. В., Городиський І. М.– К.: К.І.С., 2021. – с. 61.

[35] Захист персональних даних: Правове регулювання та практичні аспекти: науково-практичний посібник./ Бем М. В., Городиський І. М.– К.: К.І.С., 2021. – с. 61.

За думкою Бєлова Ю., така згода «повинна бути явно вираженою, зрозумілою та безсумнівною».[36]

Зазначеній позиції Бєлова Ю. можна віднайти у п.11 ст.4 Регламенту 2016/679 (GDPR), де визначено: «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».[37]

Разом із тим, GDPR виводить нову вимогу – конкретність. Згідно з 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.[38]

Конкретність формулювання – основний крок для гарантування законності обробки. Будь-яка дія щодо персональних даних повинна відповідати визначеній меті їх обробки.

Відповідно, для кожної чітко визначеної цілі обробки є необхідною окрема згода суб'єкта даних. Конкретність тісно пов'язана з метою обробки, і в національному законодавстві опосередковано випливає з «конкретизації мети».

Тобто, з одного боку, надання згоди повинно бути добровільне, поінформоване, однозначне, конкретне та чітко виражене, проте з іншого боку надання безвідкличної, необмеженої згоди на обробку персональних даних(у тому числі, на їх збір, систематизацію, накопичення, зберігання, уточнення (оновлення та зміну), використання, розповсюдження, передачу, знеособлення, блокування та знищення будь-якої інформації, що стосується суб'єкта персональних даних суперечить одному із принципів обробки персональних

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

[37] 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). Офіційна інтернет-сторінка Верховної Ради України – Режим доступу: https://zakon.rada.gov.ua/laws/show/984_008-16#Text;

[38] 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). Офіційна інтернет-сторінка Верховної Ради України – Режим доступу: https://zakon.rada.gov.ua/laws/show/984_008-16#Text;

даних – а саме меті обробки таких персональних даних, так як мета має бути чітко сформульована.

Згідно із постановою Верховного Суду від 06.12.2019 у справі № 664/1261/16: «Згідно з частиною шостою статті 6 Закону України «Про захист персональних даних» не допускається обробка даних про фізичну особу без її згоди, крім випадків, визначених законом, і лише в інтересах національної безпеки, економічного добробуту та прав людини. Проаналізувавши зміст пункту 9.4 кредитного договору суди дійшли висновку, що згідно з цим пунктом відповідач може розповсюджувати, реалізовувати та передавати персональні дані позивача будь-яким третім особам, без будь-яких обмежень, а позивач позбавлений права відізвати свою згоду на обробку персональних даних, оскільки у цьому пункті кредитного договору встановлено її безвідкличність, що не відповідає закону. Верховний Суд зазначає, що суди дійшли обґрунтованого висновку про визнання недійсним пункту 9.4. кредитного договору, оскільки він не відповідає пунктам, 11 частини другої статті 8 Закону України "Про захист персональних даних».[39]

У своїй іншій постанові Верховний Суд зазначив: «Установивши, що умови про безвідкличну згоду на обробку персональних даних позичальника, які містяться у пункті 2.13.18. Правил банківського обслуговування фізичних осіб у ПАТ Дельта Банк", суперечать Закону України "Про захист персональних даних", а третейське застереження, яке міститься у пункті 18.1. вказаних Правил, суперечить Закону України "Про третейські суди" (у редакції чинній на час укладання кредитного договору), суд апеляційної інстанції дійшов обґрунтованого висновку про визнання оспорюваного кредитного договору в цій частині положень недійсним.»[40]

Отже, існування таких положень у згоді про обробку персональних даних як безвідкличність та необмеженість не має права на життя, не може бути

[39] Постанова Верховного Суду від 06.12.2019 у справі № 664/1261/16. Режим доступу: https://reyestr.court.gov.ua/Review/86205971;

[40] Постанова Верховного Суду від 16.10.2019 у справі № 752/10234/16. Режим доступу: https://reyestr.court.gov.ua/Review/85135423

зазначено у типових згодах про обробку персональних даних, а у разі їх зазначення не має створювати значущих юридичних наслідків для особи, яка дає згоду на обробку своїх персональних даних, а володілець/розпорядник не повинен керуватися/оперувати цими категоріями при взаємодії із суб'єктами персональних даних.

Усе це безпосередньо та прямо стосується й надання згоди у сфері охорони здоров'я, оскільки переважна більшість обробки персональних даних пацієнтів у сфері охорони здоров'я здійснюється саме на підставі Згоди (надання згоди про обробку персональних даних та/або укладення/виконання правочинів) а не на підставі Закону.

Разом із тим, порушення Закону України «Про захист персональних даних» у розрізі зазначення у згоді про обробку персональних даних надання безвідкличної згоди, є непоодинокі у сфері охорони здоров'я.

Так, наприклад типова згода про обробку персональних даних товариства з обмеженою відповідальністю «Клініка відновлення зору» (ТМ – «Візіум») (код ЄДРПОУ 37331584) викладена наступним чином: «Відповідно до Закону України «Про захист персональних даних» від 01.06.2011 р № 2297, надаю безвідкличну згоду щодо обробки моїх персональних даних з метою здійснення медичної та господарської діяльності Виконавця» (Додаток 1 – фото типової згоди про обробку персональних даних ТОВ «Клініка відновлення зору»).

Окремо слід наголосити на дотриманні наскрізної умови при отриманні згоди суб'єкта (пацієнта) на обробку його персональних даних. Такою обов'язковою умовою є зазначення мети обробки таких даних.

Тобто необхідність окреслення мети обробки персональних даних походить із самих складових надання згоди на обробку персональних даних. Мета обробки має бути зазначена у згоді про обробку персональних даних, а тому просте формулювання «з метою здійснення медичної діяльності», «надання медичних послуг» не є такою, що відповідає складовим надання згоди на обробку персональних даних, а саме порушує конкретність формулювання та чітке окреслення (рамки) обробки персональних даних, так як обробка

персональних даних пацієнта може виходити за межі фактично наданих йому медичних послуг, але формально буде підпадати під надану згоду пацієнтом на обробку персональних даних «з метою здійснення медичної діяльності». Наведемо простий приклад: пацієнт звернувся до стоматологічної клініки. Надав згоду на обробку персональних даних із метою «здійснення медичної діяльності стоматологічної клініки». Разом із тим, працівники стоматологічної клініки, оскільки планували розширення своєї медичної діяльності, вносили у себе до бази медичні дані пацієнта, що не пов'язані із наданням стоматологічних послуг, але в цілому пов'язані із медичної діяльністю (послуг) стоматологічної клініки.

Тому формулювання «з метою здійснення медичної діяльності» або ідейно подібні формулювання є обширними, такими, що надають змогу здійснювати обробку персональних даних у будь-якому випадку, коли суб'єкт здійснюватиме медичну діяльністю.

Згода на обробку персональних даних повинна закінчуватися там, де закінчується конкретна мета обробки персональних даних, і обробка володільцем/розпорядником персональних даних суб'єкта поза конкретною метою для якої було отримано згоду, автоматично тягне за собою необхідність отримання нової згоди (як підстави для обробки) та формулювання нової мети обробки персональних даних.

Таким чином замість зазначення абстрактної мети обробки персональних даних «з метою медичної діяльності» необхідно сформулювати чітку мету, задля визначення меж обробки та недопущення здійснення незаконної обробки персональних даних, згода на яку не давалася.

2.2. **Згода на обробку персональних даних та договір про надання медичних послуг (в контексті обробки персональних даних). Їх співвідношення.**

Підстави для обробки персональних даних, виходячи із ст. 11 Закону України «Про захист персональних даних», можна поділити на два великі блоки: одні базуються на підставі Згоди, інші на підставі Закону.

Аналогічної думки дотримуються автори Науково-практичного посібника «Захист персональних даних: правове регулювання та практичні аспекти»[41], які відносять пункти 1,3 ч.1 ст. 11 Закону України «Про захист персональних даних» до обробки на підставі отримання згоди, тобто добровільної обробки, за волевиявленням суб'єкта, а інші пункти ч.1 ст. 11 Закону України «Про захист персональних даних» відносять до підстав обробки внаслідок Закону.

Згідно із п.1,3 ч.1 ст. 11 Закону України «Про захист персональних даних» підставами для обробки персональних даних є: згода суб'єкта персональних даних на обробку його персональних даних; укладення та виконання правочину, стороною якого є суб'єкт персональних даних або який укладено на користь суб'єкта персональних даних чи для здійснення заходів, що передують укладенню правочину на вимогу суб'єкта персональних даних[42].

Перш за все необхідно звернути увагу на формулювання словосполучення «укладення та виконання правочину» та довести його розмежування із згодою на обробку персональних даних.

Так, відповідно до ч.ч.1,2 ст. 202 ЦК України[43], правочином є дія особи, спрямована на набуття, зміну або припинення цивільних прав та обов'язків. Правочини можуть бути односторонніми та дво- чи багатосторонніми (договори).

Договором є домовленість двох або більше сторін, спрямована на встановлення, зміну або припинення цивільних прав та обов'язків (ч.1 ст. 626 ЦК України).

Тобто, кожен договір є правочином, однак не кожен правочин є договором. Наприклад, постановою Верховного Суду від 19.08.2020 у справі № 201/16327/16-ц зазначено наступне: «До односторонніх правочинів, зокрема,

[41] Захист персональних даних: Правове регулювання та практичні аспекти: науково-практичний посібник./ Бем М. В., Городиський І. М.– К.: К.І.С., 2021. – с. 58.
[42] Про захист персональних даних: Закон України від 01 червня 2010 року № 2297-VI// Відомості Верховної Ради України (ВВР) – 2010. - № 34. - ст. 481
[43] Цивільний кодекс України від 16.01.2003 № 435-IV. Відомості Верховної Ради України (ВВР), 2003, NN 40-44, ст.356

відноситься: видача довіреності, відмова від права власності, складання заповіту, публічна обіцянка винагороди, прийняття спадщини».[44]

В іншій постанова Верховного Суду від 07.04.2020 у справі № 456/2628/17 висловлювалося: «За своєю сутністю прийняття спадщини - це односторонній правочин, який спрямований на набуття спадкового майна (спадщини). Для прийняття спадщини властивий універсальний характер, оскільки воно поширюється на всю спадщину, з чого б вона не складалася і де б вона не знаходилась, тобто на всі спадкові активи і пасиви»[45].

При системному тлумаченню ст.ст. 202,626 ЦК України, п.3 ч.1 ст. 11 Закону України «Про захист персональних даних» можна дійти висновку, що у формулюванні «укладення та виконання правочину, стороною якого є суб'єкт персональних даних або який укладено на користь суб'єкта персональних даних чи для здійснення заходів, що передують укладенню правочину на вимогу суб'єкта персональних даних» законодавець мав на увазі «укладення та виконання договорів», а тому вживання термінології «укладення та виконання правочинів» у Законі України «Про захист персональних даних» є недоречним, так як не відповідає засадам Цивільного кодексу України щодо визначення та розмежування між собою правочинів та договорів.

При вчиненні одностороннього правочину воля виражається (виходить) від однієї сторони. Між цим така сторона може бути представлена декількома особами, прикладом чого може виступати видання довіреності двома та більше особами, спільний заповіт подружжя та ін. Аналіз розуміння як правочину, так і одностороннього правочину свідчить, що односторонні правочини: є вольовими діями суб`єкта; вчиняються суб`єктами для здійснення своїх цивільних прав і виконання обов`язків; спрямовані на настання правових наслідків (набуття, зміну або припинення цивільних прав та обов`язків)[46]

---

[44] Постанова Верховного Суду від 19.08.2020 у справі № 201/16327/16-ц. Режим доступу - https://reyestr.court.gov.ua/Review/91104471

[45] Постанова Верховного Суду від 07.04.2020 у справі № 456/2628/17. Режим доступу - https://reyestr.court.gov.ua/Review/88692181

[46] Постанова Верховного Суду від 19.08.2020 у справі № 201/16327/16-ц. Режим доступу - https://reyestr.court.gov.ua/Review/91104471

Згода суб'єктна на обробку персональних даних є одностороннім правочином, оскільки не вимагає наявності волевиявлення іншої сторони при надані згоди на обробку персональних даних, є вольовою дією особи, що спрямована для здійснення своїх цивільних прав і виконання обов'язків та настання конкретних наслідків.

Отже, укладення договору є самостійною підставою для обробки персональних даних Володільцем та/або розпорядником персональних даних та не потребується від суб'єкта надання окремої згоди.

Останній тезис має істотне значення саме для сфери охорони здоров'я, оскільки сфера охорони здоров'я є сферою надання особливих послуг, направлених на покращення фізичного (психологічного) стану особи (пацієнта), де обробляються чутливі персональні дані про особу.

Найбільш загальним договором у медичній сфері є договір про надання медичних послуг.

Аналогічну думку висловлює Кізлова О.С.: «Договір про надання медичних послуг є найпоширенішою підставою виникнення цивільних відносин з оплатного надання медичних послуг».[47]

Предметом договору про надання медичних послуг є надання медичної послуги, яка споживається в процесі вчинення дій або провадження медичної діяльності. Сторонами договору виступають Виконавець та Замовник.[48]

У предметі договору чітко та конкретно вказується, які саме медичні послуги надаються особі за даних фактичних обставин.

Сам по собі, інститут захисту персональних даних являє собою сукупність правових норм, що регулюють суспільні відносини, які виникають при зборі, використанні, зберіганні, обробці, видаленні, передачі і розкритті персональних даних, а саме будь-якої інформації, пов'язаної з ідентифікованою особою[49].

---

[47] Кізлова О. С. Договір про надання медичних послуг як цивільно-правовий договір / О. С. Кізлова // Право і суспільство. - 2014. - № 2. - С. 39-44.

[48] Кізлова О.С. Цивільно-правовий договір про надання медичних послуг /О.С. Кізлова // Правові та інституційні механізми забезпечення розвитку держави та права в умовах євроінтеграції : матеріали Міжнародної науково-практичної конференції (20 травня 2016 р., м. Одеса) : у 2 т. Т. 2 / відп. ред. М. В. Афанасьєва. - Одеса : Юридична література, 2016. - С. 416-420.

[49] Костенко, З.В. Механізм захисту персональних даних в європейському союзі та його вдосконалення в Україні [Текст] / З.В. Костенко, М.О. Думчиков // Реформування правової системи в контексті євроінтеграційних процесів: матеріали IV

Отже, з боку договірного права, предмет договору виступає як істотна умова договору, однак з боку інституту персональних даних, предмет договору про надання медичних послуг є тією конкретною метою обробки персональних даних, за якої особа (Замовник) укладає договір (правочин) із Виконавцем та погоджується, що його персональні дані будуть використовуватися Виконавцем (Володільцем) для виконання обов'язків (предмету договору), які закріплені у договорі про надання медичних послуг.

Таким чином, при укладенні договору про надання медичних послуг або іншого договору у сфері охорони здоров'я не є необхідним отримувати від особи (Замовника, суб'єкта персональних даних) окрему згоду на обробку персональних даних, так як укладення та виконання правочинів (договір) є окремою підставою для обробки персональних даних. Межі здійснення обробки персональних даних на підставі виконання сторонами договору, обмежується предметом договору, тобто тими послугами, які надаються Виконавцем і якими обумовлюється необхідність у обробці певної частини персональних даних Замовника для надання відповідних медичних послуг.

Укладаючи договір, особа повинна індивідуалізувати себе як учасника правовідносин за допомогою інформації, яка становить персональні дані. Індивідуалізація фізичної особи є об'єктивною потребою встановлення правових відносин. Без належної індивідуалізації особа не може бути ідентифікована як їх учасник і, відповідно, правочин не може бути укладений.

Отже, суб'єкт персональних даних, виражаючи своє волевиявлення як учасник правочину, тобто надаючи явну «згоду», усвідомлює свої правові дії, є поінформованим про їх зміст і наслідки. Внаслідок цього при укладенні та виконанні договору уникнути обробки персональних даних неможливо. Відповідно, надання окремої «згоди на обробку персональних даних» для укладення договору не є доцільним. Законодавець, виділивши укладення та виконання правочину в окрему підставу для здійснення обробки персональних

Міжнародної науково-практичної конференції: у 2-х ч. (м. Суми, 21–22 травня 2020 року) / редкол.: А.М. Куліш, О.М. Рєзнік. – Суми: Сумський державний університет, 2020. – Ч.2 – С. 69-73.

даних (п. 3 ст. 11 Закону), зумовив необхідний правовий захист учасників правовідносин і неможливість відкликати таку згоду до моменту повного виконання зобов'язань між сторонами.

Тому, немає жодної необхідності у самому тексті договору про надання медичних послуг передбачати конструкцію надання згоди на обробку персональних даних, з огляду на аргументи, перелічені вище. Більш того, передбачення конструкції отримання згоди на обробку персональних даних у самому тексті договору суперечить і положення Закону України «Про захист персональних даних», так як надання згоди на обробку персональних даних та укладення правочинів є різними окремими підставами для обробки.

Разом із тим, якщо обробка персональних даних, за певних обставин, не охоплюється договором (не відповідає предмету договору, з метою якого і укладався договір), тоді є цілком об’єктивна необхідність в отриманні від особи окремої згоди на обробку персональних даних, із зазначенням нової, що різниться від договору, мети такої обробки. Наприклад, особа уклала договір про надання медичних послуг – а саме протезування зубів, то персональні дані про стан здоров’я особи та інші персональні дані, які необхідні для надання якісних медичних послуг, будуть оброблятися на підставі укладеного договору.

Проте, якщо Виконавець за договором забажає викласти новину про результат надання послуги у себе на веб сайті із викладенням фото особи, яка отримувала медичні послуги або із викладенням будь-якої іншої інформації (персональних даних) про особу, що наддасть змогу її ідентифікувати, то для публікації такої новини із використанням персональних даних особи, Виконавцю за договором необхідно буде отримати окрему згоду від особи на обробку її персональних даних із метою викладення результату надання медичних послуг у себе на веб сайті, оскільки така обробка персональних даних виходитиме за межі предмету договору, за для якого сторони й укладали договір про надання медичних послуг.

Отже підсумовуючи вищесказане, укладення договору та отримання згоди на обробку персональних даних щодо однієї і тієї ж мети обробки персональних

даних є недоречним. Зазначення конструкції надання згоди про обробку персональних даних у самому тексті договору є нікчемним. Одночасне існування договору та згоди про обробку персональних даних можливе за умови, якщо мета обробки різниться.

Досить цікавим видається момент припинення обробки персональних даних, обробка яких відбувається на підставі надання згоди на обробку персональних даних та укладення та виконання правочинів (договорів).

Так, наприклад, суб'єкт персональних даних має право відкликати згоду на обробку персональних даних (п.11 ч.2 ст. 8 Закону України «Про захист персональних даних).[50]

Оскільки, згода на обробку персональних даних є одностороннім правочином, то є цілком логічним передбачення даного права особи про можливість відкликати згоди на обробку персональних даних, так як згідно із ч.1,3 ст. 214 ЦК України особа, яка вчинила односторонній правочин, має право відмовитися від нього, якщо інше не встановлено законом. Якщо такою відмовою від правочину порушено права іншої особи, ці права підлягають захисту. Відмова від правочину вчиняється у такій самій формі, в якій було вчинено правочин.[51]

Тобто, право особи на вчинення одностороннього правочину у формі відкликання згоди на обробку персональних цілком та повністю корелює із загальними засадами Цивільного кодексу України щодо вчинення правочину, тому що, вчинення та відмова від раніше вчиненого одностороннього правочину є лише правом особи, яка його вчинила. Такий односторонній правочин виражає лише дії особи, що його вчиняє та не впливає на законні права, обов'язки та інтереси інших суб'єктів у певних правовідносинах.

Право відкликати згоду на обробку персональних даних стосується, як можна дійти із системного тлумачення положень Закону України «Про захист

[50] Про захист персональних даних: Закон України від 01 червня 2010 року № 2297-VI// Відомості Верховної Ради України (ВВР) – 2010. - № 34. - ст. 481

[51] Цивільний кодекс України від 16.01.2003 № 435-IV. Відомості Верховної Ради України (ВВР), 2003, NN 40-44, ст.356

персональних даних» (ст.8,11) та Цивільного кодексу України (ст.ст. 203, 214) лише однієї підстави для обробки персональних даних – а саме надання згоди на обробку персональних даних – а тому, у разі укладення та виконання договору (правочинів) особа невзмозі буде скористатися правом відкликати згодну на обробку своїх персональних даних, оскільки правова підстава виникнення підстави для обробки персональних даних та правова конструкція укладення договору істотно відрізняються від надання згоди на обробку персональних даних.

Як було зазначено вище, укладення та виконання правочинів є ніщо інше, як договором, тому підставою припинення обробки персональних даних, яка виникла на підставі укладення договору будуть використовуватися положення Цивільного кодексу України – глава 50 «Припинення зобов'язання» та ст. 651 Цивільного кодексу України – підстави для зміни або розірвання договору.

Відповідно до ст. 509 ЦК України, зобов'язанням є правовідношення, в якому одна сторона (боржник) зобов'язана вчинити на користь другої сторони (кредитора) певну дію (передати майно, виконати роботу, надати послугу, сплатити гроші тощо) або утриматися від вчинення певної дії (негативне зобов'язання), а кредитор має право вимагати від боржника виконання його обов'язку.[52]

Отже, у разі виявлення підстав для припинення договору про надання медичних послуг, такі підстави одночасно є підставами для припинення обробки персональних даних, так як договір є виконаним або припиненим, і як наслідок відпадає підстава для подальшої обробки персональних даних. Сама мета обробки персональних даних зникає також.

Таким чином, Законом України «Про захист персональних даних» чітко закріплено право особи про відкликання (припинення) згоди на обробку персональних даних, яка виникла на підставі згоди на обробку персональних даних, проте Законом України «Про захист персональних даних» жодним чином

[52] Цивільний кодекс України від 16.01.2003 № 435-IV. Відомості Верховної Ради України (ВВР), 2003, NN 40-44, ст.356

не уточнено (роз'яснено) момент припинення обробки персональних даних, який виник на підставі укладення та виконання правочину, стороною якого є суб'єкт персональних даних або який укладено на користь суб'єкта персональних даних чи для здійснення заходів, що передують укладенню правочину на вимогу суб'єкта персональних даних, а єдиним правом суб'єкта персональних даних у результаті виконання договору, для захисту своїх персональних даних є право пред'являти вмотивовану вимогу володільцю персональних даних із запереченням проти обробки своїх персональних даних із зазначенням, що правовідносини за договором (правочином) між сторонами припинилися, а тому не є необхідним подальша обробка персональних даних щодо суб'єкта.

Висновки до розділу II

1. Згода на обробку персональних даних складається з наступних елементів: добровільність, поінформованість, конкретність, однозначність волевиявлення суб'єкта персональних даних.
2. Включення у згоду на оброку персональних даних такої вимоги як «безвідкличність» не є можливою та прямо суперечить положенням Закону України «Про захист персональних даних».
3. У згоді на обробку персональних даних має бути чітко зазначена мета оброки, аби, з однієї сторони, не допустити необмеженої обробки персональних даних пацієнта (суб'єкта) з боку Володільця/Розпорядника, а з другої задля забезпечення дотримання прав пацієнта (суб'єкта персональних даних) відповідно до вимог Закону України «Про захист персональних даних».
4. Згода на оброку персональних даних є одностороннім правочином. «Укладення та виконання правочинів» слід розуміти та розглядати як договір та виконання його умов.
5. Згода на обробку персональних даних та «укладення і виконання правочинів» мають різних порядок припинення обробки персональних даних.
6. Отримання окремої згоди на обробку персональних даних під час виконання умов договору не потребується, окрім випадку, якщо використання та отримання персональних даних не охоплюється предметом договору.

7. Предмет договору є тією метою з якою надаються персональні дані для їх обробки. Разом із тим, предмет договору окреслює межі обробки персональних даних.

РОЗДІЛ 3. E-HEALTH В УКРАЇНІ: ВИЗНАЧЕННЯ ПОНЯТТЯ, ПЕРЕВАГИ ТА НЕДОЛІКИ

3.1. Визначення поняття E-Health.

Постановою від 25.04.2018 р. № 411 Кабінет Міністрів України затвердив Порядок функціонування електронної системи охорони здоров'я[53], 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 відповідно до Закону України «Про державні фінансові гарантії медичного обслуговування населення».

З цього періоду розпочалося впровадження електронної системи охорони здоров'я в Україні - E-Health. Основні переваги та недоліки цієї системи розглянемо у цьому пункті.

Перш за все, вважаємо за необхідне визначитися, що таке система «E-Health». У п.2 ч.1 ст. 2 Закону України «Про державні фінансові гарантії медичного обслуговування населення» зазначено, що «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)»[54].

Наукове середовище пропонує своє визначення «E-Health». Так, наприклад, Н. Азіз та Ч. Вивера стверджують що «E-Health» є використанням

[53] Порядок функціонування електронної системи охорони здоров'я. Постанова Кабінету Міністрів України від 25 квітня 2018 року № 411 // Офіційна інтернет-сторінка Верховної Ради України: https://zakon.rada.gov.ua/laws/show/411-2018-%D0%BF#Text.

[54] Про державні фінансові гарантії медичного обслуговування населення. Закон України 19.10.2017 № 2168-VIII. Офіційна інтернет-сторінка Верховної Ради України – Режим доступу: https://zakon.rada.gov.ua/laws/show/2168-19#Text

інфраструктури інформаційних технологій та методів електронної комерції для обробки, обміну та управління медичною інформацією.[55]

З іншого боку, Самофалов Д.О. визначає E-Health як центральний компонент комунікативної діяльності публічного управління охороною здоров'я.[56]

Ґ. Ейзенбах запропонував 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 широкому розумінні, на думку Ґ. Ейзенбах, це поняття висвітлює 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.[57]

С. Юнкап Кванкам виходить із того, що E-Health – це всеосяжний термін для комбінованого використання в галузі охорони здоров'я електронних інформаційно-комунікаційних технологій (ІКТ) для клінічних, освітніх, наукових досліджень та адміністративних цілей, як на місцевому місці, так і на відстань.[58]

Таким чином, E-Health – інформаційно-телекомунікаційна система у сфері охорони здоров'я, яка забезпечує можливість обробки, обміну та управління медичною інформацією і використовується у клінічних, освітніх, наукових досліджень у взаємозв'язку із публічним адмініструванням.

[55] 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. Режим доступу: https://cg.harran.edu.tr/admin/Upload/files/Security_and_privacy_issues_in_e-health.pdf.

[56] Самофалов Д.О. Публічне управління у сфері охорони здоров'я /Самофалов Д.О.// Державне управління та місцеве самоврядування – 2020 рік - вип. № 1(44) – с. 92 – 99.

[57] Eysenbach, G. What is e-health? / Eysenbach, G// Journal of medical Internet research - 2001 - № 3(2) - p.20.

[58] S. Yunkap Kwankam. What e-Health can offer / S. Yunkap Kwankam// Bulletin of the World Health Organization – 2004 - № 82 (10) – c. 800 -802.

3.2. Переваги та недоліки системи E-Health в Україні.

Електронна система охорони здоров'я в Україні – не є єдиною базою. 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)[59]. У національній системі E-Health використовується новітні міжнародні стандарти обміну інформацією HL7 FHIR (Fast Health Care Interoperability Resources), які дозволяють збереження та миттєву, точну передачу медичних даних на основі міжнародних кодів.

Власником центральної бази 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). Володільцем відомостей Реєстру медичних спеціалістів, Реєстру суб'єктів господарювання у сфері охорони здоров'я, Реєстру медичних висновків та Національного реєстру донорів крові та компонентів крові, а також осіб, яким заборонено виконувати донорську функцію, в електронній системі охорони здоров'я є МОЗ. Розпорядником Реєстру медичних спеціалістів, Реєстру суб'єктів господарювання у сфері охорони здоров'я, Реєстру медичних висновків та Національного реєстру донорів крові та компонентів крові, а також осіб, яким заборонено виконувати донорську функцію, є НСЗУ[60].

Розпорядником інших реєстрів та володільцем їх відомостей та іншої інформації у центральній базі даних є НСЗУ, якщо інше не визначено законодавством. Адміністратором центральної бази даних є державне підприємство "Електронне здоров'я" (далі - адміністратор), крім Інформаційної

[59] Порядок функціонування електронної системи охорони здоров'я. Постанова Кабінету Міністрів України від 25 квітня 2018 року № 411 // Офіційна інтернет-сторінка Верховної Ради України: https://zakon.rada.gov.ua/laws/show/411-2018-%D0%BF#Text

[60] Порядок функціонування електронної системи охорони здоров'я. Постанова Кабінету Міністрів України від 25 квітня 2018 року № 411 // Офіційна інтернет-сторінка Верховної Ради України: https://zakon.rada.gov.ua/laws/show/411-2018-%D0%BF#Text

системи НСЗУ, адміністрування якої забезпечує НСЗУ. Адміністратор не здійснює обробку персональних даних пацієнтів.

Тобто Адміністратор забезпечує лише технічні, організаційні та інші заходи, необхідні, щоб забезпечити функціонування центральної бази даних електронної системи охорони здоров'я

На думку науковців, домени різних рівнів, що використовуються під час опрацювання (обміну) медичною інформацією, ускладнюють застосування інформаційних систем, а тому є необхідність у використанні хмарних сховищів (cloud-based environment), які б забезпечили можливість у легкості обміну даними між різними адміністративними доменами[61].

Перевагами хмарних сховищ є безперешкодна і постійна передача даних, що призводить до надання можливості обміну медичними даними (у т.ч. персональною інформацією) у сьогоднішньому часі та забезпечує правдивість медичних даних.

Разом із тим, у науковому колі виділяють позитивно економічну складову використання електронних систем і підвищення гнучкості обміну даних при використанні хмарних технологій[62].

Ще одним плюсом застосування хмарних сховищ є можливість створення резервної копії інформації на серверах, що знижує ризик її втрат. Більш того, e-health дозволяє вирішити низку проблем, серед яких низька ємність, високі витрати на експлуатацію та технічне обслуговування та інтеграцію системи[63].

Та наостанок E-Health є гарантом забезпечення прозорості та відкритості при управлінні охороною здоров'я та розподілом і використання бюджетних коштів.

[61] 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 - 2010 - pp. 268–275. Режим доступу: https://faculty.cc.gatech.edu/~lingliu/papers/2010/RuiZhang-cloud2010.pdf

[62] 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

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

З іншого боку, використання системи E-Health тягне за собою і негативні аспекти: залишаються відкритими питання про безпеку та конфіденційність персональних даних, в тому числі медичних даних[64]. У звіті про стратегію електронного здоров'я, опублікованому в січні Європейською Комісійною зазначається: «У всіх країнах довіра до систем електронної охорони здоров'я як громадян, так і фахівців була визначена як одна з, якщо не головна проблема. Конфіденційність визнається найбільш чутливим аспектом систем електронних медичних карт»[65].

Одним із головних проблем конфіденційності визначаються: незаконне або недобровільне обробка персональних даних суб'єкта, порушення права суб'єкта (пацієнта) бути ознайомленим хто, як та коли отримав доступ до медичних даних пацієнта, сприйняття до атак.

Більш того, є загроза при проведенні веб-аналітики, здійсненої третіми особами, які використовують персональні дані користувачів для цільової реклами[66].

Щоб захисти інформацію, яка зберігається та оброблюється через електронну систему, використовуються організаційні, технічні методи задля ефективної протидії різноманітним загрозам, таким як несанкціонований доступ, відмова в доступі, втрата даних, підробка особистих даних тощо.

Визначення міжнародних стандартів щодо механізмів захисту персональних даних в електронній системі даних немає. Разом із тим, серед наукового середовища висувають наступні засоби запобігання незаконної обробки медичних даних.

Перше за все, це можливість пацієнтів (суб'єкти медичних даних), цілковитого контролю над обробкою своїх персональних даних (пацієнто-орієнтований підхід). Іншими словами, замість того, щоб власник хмарного сховища шифрував дані пацієнтів, пацієнти можуть генерувати власні ключі

[64] Zissis D, Lekkas D. Addressing cloud computing security issues. Future Generation Computer Systems. Volume 28, Issue 3, March 2012, p.p. 583-592. Режим доступу: https://www.sciencedirect.com/science/article/pii/S0167739X10002554#!
[65] Mahony, M. Trust remains key barrier to eHealth. [Електронний ресурс]. Режим доступ: http://euobserver.com/ 893/31958
[66] Eman Abukhousa, Nader Mohamed, Jameela Al-Jaroodi. e-Health Cloud: Opportunities and Challenges July 2012 Future Internet 4(4), p.p. 621-645

шифрування, використовуючи атрибутивне шифрування, а потім розповсюджувати їх конкретним авторизованим користувачам.[67]

У цьому випадку, пацієнтам надається можливість скласти перелік осіб, яким надається право на обробку їх медичних даних, обсяг та строк оброки персональних даних.

Наступний 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[68].

Також існує виникнення реєстраторів даних, різні механізми автентифікації, авторизації та контролю доступу, періодична сертифікація стороннім аудитом (TPA), довірені домени конфіденційності.[69]

Окрім цього, використання технологій в E-Health мають прямий вплив на право на приватність. Так, деякі науковці підкреслюють, що обробка персональних, і як наслідок медичних даних, здійснюється як медичними працівниками, так і різними пристроями із щоденного життя: датчики та інтелектуальні пристрої в особистому просторі, наприклад, автомобіль, який відчуває стрес або втому водія, так звані фітнес трекери, які перманентно збирають персональні дані про різні аспекти людини: частота пульсу, тривалість сну, активності, місцезнаходження, рівень цукру в крові.[70]

Для захисту персональних даних, які оброблюються в електронній системі E-Health, використовуються різноманітні організаційні та технічні заходи захисту.

[67] 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

[68] 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.

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

[70] 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. Режим доступу: https://doi.org/10.3390/info11070356.

Пропонуємо до вивчення, організаційні та технічні заходи захисту обробки персональних даних, які реалізуються та використовуються в національній моделі E-Health.

Так, для забезпечення функціонування системи e-Health в Україні реалізується приватно хмарна модель. 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[71].

Технічне завдання, передбачало вимоги до технічних та якісних характеристик предмета договору. Предметом договору є послуги зі зберігання та обробки даних системи E-Health 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

[71] 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.

задану ступінь доступності (готовності) розміщеного обладнання в заданому режимі функціонування.[72]

Приватне хмарне сховище є найзахищенішим, так як дані повністю обмежені від загального доступу в Інтернеті.[73]

До електронних медичних записів у приватному хмарному сховищі має доступ лише визначений персонал закладів охорони здоров'я або фізичні особи-підприємці, які отримали ліцензію на провадження господарської діяльності з медичної практики, У разі проходження авторизації та ідентифікації за допомогою цифрових підписів.

Бажаємо наголосити, що згідно із п.11. Порядку № 411, технічні засоби центральної бази даних повинні перебувати у межах території України.

Щоб виконати вимоги Порядку № 411, у 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.[74]

Окремо вважаємо звернути увагу на технічні вимоги до національної системи E-Health та відзначити деякі із них. Щоб забезпечити цілісність усіх даних, фізичні ресурси зберігання даних для віртуальних дисків та хмарного сховища мають бути рівня 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

[72] 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.

[73] 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.

[74] 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

ліцензійного програмного забезпечення тощо[75]. 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.

Хочемо звернути увагу, що, на нашу думку, організаційні заходи та методи захисту інформації в електронній системі E-Health повністю відповідають положенням Типовому порядку обробки персональних даних. Також звертаємо увагу на такий організаційний захід забезпечення безпеки в хмарній системі E-Health, як реєстрацію будь-яких дій користувачів, що відбувається безперервно за допомогою програмних засобів захисту та збереження персональних даних строком до трьох місяців.

Наступним заходом захисту є кваліфікований електронний підпис (далі-КЕП) працівника закладу охорони здоров'я чи фізичної особи-підприємця, наявність якого надає власнику КЕП права доступу до електронної системи. Відповідно до пункту 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»[76].

Відповідно до пункту 23 ч. 1 ст. 1 Закону України «Про електронні довірчі послуги», кваліфікований електронний підпис - удосконалений електронний підпис, який створюється з використанням засобу кваліфікованого електронного

[75] 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

[76] Регламент функціонування компонентів електронної системи обміну медичною інформацією, що необхідні для запуску нової моделі фінансування на первинному рівні надання медичної допомоги. Наказ Державного підприємства "Електронне здоров'я" від 29 березня 2018 року №5-ГД. Режим доступу: https://ehealth.gov.ua/wpcontent/uploads/2018/10/Rehlament_funktsionuvannia_komponentiv_elektronnoi_systemy.pdf

підпису і базується на кваліфікованому сертифікаті відкритого ключ. Таким чином, КЕП прирівняний, законодавчо, до власноручного підпису[77].

Однак варто розуміти різницю між особистим КЕП та КЕП працівника закладу охорони здоров'я, оскільки перший використовується для власних, особистих цілях та не може використовуватися працівником закладу охорони здоров'я при здійсненні ним обов'язків як медичного працівника та входження до електронної системи 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.

З іншої сторони, хочемо підкреслити певні недоліки (мінуси) національної електронної системи E-Health.

Перш за все, у пацієнтів як суб'єктів персональних даних відсутня можливість здійснювати контроль щодо факту, хто, як і коли мав доступ до їхніх персональних даних. Наприклад, пацієнти не можуть ознайомитись із інформацією щодо обробки їхніх персональних даних на рівні НСЗУ як власника центральної бази даних.

По-друге, необґрунтоване збереження усього об'єму інформації в центральній базі даних (у тому числі із різноманітних медичних інформаційних систем, підключених до системи E-Health). Вважаємо, такий великий обсяг інформації, яка зберігається в одному місці, є недоцільним та становить загрозу її безпеці, не зважаючи на належний рівень захисту. Як наслідок, усе це може спричинити в майбутньому перевантаженість системи і, призвести до порушення нормального функціонування системи. Тож, на нашу думку, необхідним є здійснити розподіл інформації, яка буде зберігатися на різних захищених серверах, що разом становитимуть систему E-Health.

[77] Про електронні довірчі послуги. Закон України від 17.05.2017 № 2155-VIII. Офіційна інтернет-сторінка Верховної Ради України: https://zakon.rada.gov.ua/laws/show/2155-19#Text

3.3. **Особливості відповідальності за порушення обробки персональних даних.**

Відповідальність за порушення обробки персональних даних у сфері охорони здоров'я можна розподілити на: дисциплінарну, цивільно-правову, адміністративну та кримінальну. Особливе місце слід приділити відповідальності у зв'язку з винесенням Уповноваженим Верховної Ради з прав людини приписів про запобігання або усунення порушень законодавства про захист персональних даних, оскільки невиконання законних приписів Уповноваженого Верховної Ради з прав людини або представників є складом адміністративного правопорушення, що передбачено частиною 2 статті 188-39 КУпАП.

Щодо дисциплінарної відповідальності, то слід зазначити наступне: дисциплінарна відповідальність проявляється або у формі догани або у формі звільнення та виникає у разі вчинення медичним працівником, дисциплінарного проступку (невиконання чи неналежного виконання працівником своїх трудових обов`язків відповідно до посадової інструкції відповідного медичного закладу), наприклад, в разі порушення лікарської таємниці, вимог професійної етики та деонтології. Окрім цього, згідно із ст. 148 КЗпП України[78], дисциплінарне стягнення застосовується власником або уповноваженим ним органом безпосередньо за виявленням проступку, але не пізніше одного місяця з дня його виявлення. Дисциплінарне стягнення не може бути накладене пізніше шести місяців з дня вчинення проступку.

Звернемо увагу, що обов'язок доказування правомірності застосування дисциплінарного стягнення покладається на роботодавця, виходячи із положень Цивільного процесуального кодексу України. Щоб притягнути особу до дисциплінарної відповідальності обов'язковим є доведення конкретних фактичних обставин допущеного порушення посадової інструкції та правил внутрішнього трудового розпорядку. Із вищевказаного можна дійти висновку,

[78] Кодекс законів про працю України від 10.12.1971 №322-VIII. Офіційна інтернет-сторінка Верховної Ради України: https://zakon.rada.gov.ua/laws/show/322-08#Text

що притягнути особу до відповідальності за порушення положень, які не закріплені в будь-якому трудовому документі є неможливим, що корелюється із ст. 19 Конституції України.

Відповідно до статті 55 Конституції України[79], кожен має право будь-якими не забороненими законом засобами захищати свої права і свободи від порушень і протиправних посягань.

За цивільно-правової відповідальності, особа сама може обирати спосіб захисту свого порушеного права, у т.ч. у сфері охорони здоров'я. Доцільним у разі розголошення персональних даних є формулювання позивних вимог про визнання протиправними дій відповідача та відшкодування матеріальної та/або моральної шкоди.

У спорах про стягнення моральної шкоди, діє презумпцією нанесення моральної шкоди особі відповідачем. У постанові ВСУ від 27.09.2017 по 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 судами першої та апеляційної інстанції 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».[80]

Проте, Верховний Суд України обґрунтовано підкреслив, що у деліктних зобов'язаннях саме на відповідача покладено обов'язок спростування презумпції вини у заподіянні шкоди.

Адміністративна відповідальність, покладається на володільців та розпорядників персональних даних за незаконну обробку персональних даних суб'єктів або порушення інших прав суб'єктів, у тому числі у сфері охорони

[79] Конституція України від 28.06.1996 № 254к/96-ВР// Відомості Верховної Ради України (ВВР) – 1996. - № 30. – ст. 141

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

здоров'я. За такі дії передбачена адміністративна відповідальність за статями: 188-39, 188-40 КУпАП.[81]

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).

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).

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)

Хочемо звернути увагу на адміністративний склад правопорушення, визначений ч.4 ст.188-39 КУпАП.

Національним законодавством не закріплено визначення поняття, що таке: порядок захисту персональних даних. Як зазначають Бем М. В., Городиським І. М., Саттоном Г. та інші[82], розтлумачити таке поняття можливо за допомогою двох складових.

Перша – це зобов'язання володільця, розпорядника, третіх особі вживати організаційних та технічних заходів з метою забезпечити їх захист від випадкової втрати або знищення, незаконної обробки, у тому числі незаконного знищення

[81] Кодекс України про адміністративні правопорушення. Відомості Верховної Ради Української РСР (ВВР) 1984, додаток до № 51, ст.1122

[82] Захист персональних даних: Правове регулювання та практичні аспекти: науково-практичний посібник./ Бем М. В., Городиський І. М.– К.: К.І.С., 2021

чи доступу до персональних даних (ч.1 ст. 24 Закону України «Про захист персональних даних»)[83]

Друга складова, пов’язана із тим, що використання персональних даних працівниками суб'єктів відносин, пов'язаних з персональними даними, повинно здійснюватися лише відповідно до їхніх професійних чи службових або трудових обов'язків.[84]

Одночасно із тим, варто звернути увагу на певну недосконаліть формулювання ч.4 ст.188-39 КУпАП – а саме матеріальний склад правопорушення, де відповідальність настає не лише за недодержання встановленого національним законодавством порядку захисту персональних даних, але що порушення такого порядку призвело до незаконної обробки персональних даних або інших порушень прав суб’єкта персональних даних.

З боку практичного застосування вищезгаданої норми, виявляться складним довести причинно-наслідковий зв'язок між діянням та протиправними наслідками. За таким формулюванням, відповідальність настає не у момент коли був порушений порядок захисту персональних даних, а за фактичної обробки персональних даних, в тому числі, медичних даних.

З огляду на вказане, вважаємо, що такі конструкції (склад адміністративного правопорушення) не мають реальний вплив на володільців та розпорядників щодо дотримання ними положень Закону України «Про захист персональних даних».

Разом із тим, висловлюємо свою згоду щодо позиції Бема М. В., Городиського І. М., Саттона Г. та інших[85], що в статті КУпАП ведеться мова не про доступ «третіх осіб», оскільки у статті 16 Закону України «Про захист персональних даних» йдеться про порядок доступу третіх осіб до персональних даних, а саме про незаконне розголошення, поширення відповідних відомостей.

---

[83] Про захист персональних даних: Закон України від 01 червня 2010 року № 2297-VI// Відомості Верховної Ради України (ВВР) – 2010. - № 34. - ст. 481

[84] Про захист персональних даних: Закон України від 01 червня 2010 року № 2297-VI// Відомості Верховної Ради України (ВВР) – 2010. - № 34. - ст. 481

[85] 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 – с. 220

Наступним недолік притягнення до адміністративної відповідальності є відсутність механізму притягнення саме юридичних осіб до адміністративної відповідальності за незаконну обробку персональних даних.

Коли здійснюється обробка персональних даних, у тому числі, медичних даних, а володільцем є юридична особа (заклад охорони здоров'я), є ситуації, коли визначити працівника володільця, який винний в розголошенні медичних даних пацієнта є неможливо (наприклад, коли медичний заклад порушив вимоги щодо обліку осіб, що мають доступ до персональних даних). Тому, притягнути до адміністративної відповідальності заклад охорони здоров'я як володільця даних є неможливим, оскільки заклад охорони здоров'я є юридичною особою.

Вважаємо, що недоліком в КУпАП є передбачення відповідальності за неповідомлення суб'єкта про обробку 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).

Строки притягнення до відповідальності за адміністративні правопорушення щодо захисту персональних даних також заважають ефективно реалізувати надані способи притягнення до відповідальності, оскільки законодавством встановлено обмеження щодо 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).

Відповідно до даних Єдиного державного реєстру судових рішень винесено десять постанов про притягнення до адміністративної відповідальності за ч.4 ст. 188-39 КУпАП, п'ятдесят одну постанову про притягнення до адміністративної відповідальності за ч.1 ст. 1-40 КУпАП (невиконання приписів Уповноваженого) та немає ні одної постанови щодо притягнення до адміністративної відповідальності за ч.1-ч.3 ст. 188-39 КУпАП.

Кримінальна відповідальність є найсуворішою відповідальністю, яка передбачена статтями 132, 145 та 182 Кримінального кодексу України (далі – КК

України). Частина 1 ст. 182 КК України закріплено 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» - Кримінальний кодекс України

Злочин, передбачений ч.1 ст. 182 КК України[86] за своїм складом є формальним, - тому вважається закінченим з моменту вчинення одного із діянь, передбачених у диспозиції статті. Істотною вважається шкода, що в сто і більше разів перевищує неоподатковуваний мінімум доходів громадян.

Дана стаття є основною щодо інших складів злочину про незаконне поширення конфіденційної (персональної) інформації. Так, розповсюдження медичної інформації, що є складовою лікарської таємниці суб'єктом, який не підпадає під сферу дію ст. 145 КК України («незаконне розголошення лікарської таємниці»), така особа нестиме кримінальну відповідальність за ст. 182 КК України.

Статтею 145 КК України закріплено відповідальність за «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»[87]. Головними для цієї статті є вимоги щодо умислу (прямого/непрямого), спеціального суб'єкта (особа, якій інформація стала відомою саме через виконання її професійних чи службових, трудових обов'язків).

Звертаємо увагу на, що за ст. 145 КК України склад злочину є матеріальним а отже відповідальність настає у разі спричинення ним тяжких наслідків. Кримінальним кодексом України не надається визначення поняття «тяжкі наслідки», що в правозастосовній практиці. Також проблематичним на практиці є доведення причинно-наслідкового зв'язку.

[86] Кримінальний кодекс України від 05.04.2001 № 2341-III. Відомості Верховної Ради України (ВВР), 2001, № 25-26, ст.131
[87] Кримінальний кодекс України від 05.04.2001 № 2341-III. Відомості Верховної Ради України (ВВР), 2001, № 25-26, ст.131

За думкою Антонова С. В., розголошення медичної таємниці є 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.[88]

Таким чином, для цього злочину не важливо за яких умов було незаконно передано інформацію, що є медичною таємницею, достатнім є факт розголошення такої за відсутності підстав, передбачених Конституцією України.

Стаття 132 КК України, передбачає кримінальну відповідальність за «розголошення службовою 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».[89]

Відповідно до 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.[90]

Із аналізу вищезазначеної статті Кримінального кодексу України можна дійти висновку, що склад злочину є формальним. Суб'єкт спеціальний - службова особа лікувального закладу, допоміжний працівник, який самочинно здобув інформацію, або медичний працівник.

Якщо особа що вчинила злочин, передбачений за ст. 132 КК України, немає ознак спеціального суб'єкту то такі дії повинні кваліфікуватись за ст. 182 КК України.

---

[88] 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.

[89] Кримінальний кодекс України від 05.04.2001 № 2341-III. Відомості Верховної Ради України (ВВР), 2001, № 25-26, ст.131

[90] Про запобігання захворюванню на синдром набутого імунодефіциту (СНІД) та соціальний захист населення. Закону України від 15.01.2011 №2861-VI.

За 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 не засуджено за наведеними статтями КК України.[91]

Висновки до розділу ІІІ

1. Система E-Health розглядається як сукупність технологічних рішень (інформаційно-телекомунікаційна система) в сфері охорони здоров'я та як платформа для обробки та консолідації медичних даних пацієнтів .
2. Запровадження електронної системи E-Health є кроком уперед щодо систематизації, обміну, зберігання та обробки медичних даних пацієнта, а з іншої сторони є викликом для підвищення рівня захисту чутливих персональних даних.
3. Система E-Health забезпечує прозорість та відкритість інформації при управлінні охороною здоров'я та розподілом і використання бюджетних коштів.
4. Разом із тим, система E-Health має свої недоліки, більшість яких пов'язано із забезпечення захисту персональних даних, що зберігаються на серверах. Є різні думки щодо того, як підвищити рівень захисту, але наукова спільнота схильна до ідеї про використання віддаленого хмарного сховища, на той випадок, якщо відбудеться масовий збій системи.
5. Наступним недоліком є відсутня можливість пацієнтів здійснювати контроль щодо факту, хто, як і коли мав доступ до їхніх персональних даних. Загалом, рівень захист, що використовується у національній системі E-Health відповідає європейським стандартам.

[91] 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.pd

6. Види відповідальності за порушення обробки персональних даних можливо поділити на 4 види: цивільно-правова, адміністративна, кримінальна та дисциплінарна. Вид відповідальності залежить від специфіки відносин між суб'єктами та їх статус у цих відносинах.
7. Види відповідальності можливо умовно розділити від найбільш легкого за наслідками та впливу: цивільно-правова, дисциплінарна (лише щодо працівника), адміністративна та кримінально-правова.
8. Притягнення винної особи як до адміністративної відповідальності так і до кримінальної у сфері персональних даних є важко здійсненним в силу специфіки об'єкта правопорушення, доведення нанесення шкоди, строків притягнення (стосується адміністративного складу правопорушення) та доведення причино-наслідкового зв'язку.
9. Саме по собі існування різних видів відповідальності за порушення прав у сфері персональних даних, без можливості реалізації, не має ніякого впливу та ефекту. Захист прав у сфері персональних даних та ефективні механізми і способи притягнення винних до відповідальності в Україні лише набувають своїх обертів та це є сфера законодавчої діяльності, на яку має звернути увагу Верховна Рада України.

ВИСНОВКИ

У процесі написання магістерської роботи автором ґрунтовно проаналізовано нормативно-правові акти, що регулюють чи є дотичними, прямо або опосередковано, питання персональних даних, спеціалізовану літературу (монографії, наукові статті), що стосувалася обробки та захисту персональних даних, системи E-health, її переваги та недоліки.

У своїй роботі, автором, під керівництвом наукового керівника, було виявлено колізії у регулюванні відносин, що виникають у сфері персональних даних та запропоновано шляхи їх вирішення при використанні правил подолання колізій у законодавстві.

На нашу думку, усі нормативно-правові акти, що суперечать Закону України «Про захист персональних даних» слід привести до відповідності, як от Порядок функціонування електронної системи охорони здоров'я. Постанова Кабінету Міністрів України від 25 квітня 2018 р. № 411, Закон України «Про державні фінансові гарантії медичного обслуговування населення».

Більш того, для того, щоб законодавство України у сфері персональних даних більш відповідало європейським стандартам, пропонуємо внести зміни у профільний Закону України «Про захист персональних даних», а саме викласти основоположне визначення «персональні дані» у відповідності до Загального регламенту (ЄС) 2016/679 захисту фізичних осіб в зв'язку з обробкою персональних даних та вільних рух таких даних (Regulation (EU) 2016/679.

Проте, вважаємо за найкраще, прийняття Верховною Радою України за основу законопроект 5628 (Проект Закону України «Про захист персональних даних»). Даний проект закону повністю відповідає європейським стандартам у сфері персональних даних, відображаючи національні інтереси та особливості регулювання в Україні.

Одностайно визначено, що медичні дані відносяться до категорії чутливих персональними даними, а тому їх обробка має відбуватися за особливої процедури, що має мінімізувати незаконну обробку третіми особами, які не мають права на здійснення такої обробки.

Автором зауважено, що при кожній обробці персональних даних має бути дотримано межі такої обробки. Межі обробки визначаються метою та ціллю, з якою персональні дані особи підлягають обробці. При доходженні до таких висновків, було проаналізовано судові рішення, що стосуються медичних даних.

У даній роботі, автор спробував надати єдине все об'ємне визначення системі E-Health, оскільки єдиного нормативного визначення цьому поняття не існує. Аналіз національної системи E-Health доводить, що рівень захисту відповідає європейським стандартам, але все одно є шляхи до вдосконалення, які наводяться у роботі.

Для того, щоб підвищити безпечність функціонування системи E-Health, пропонуємо диференційований метод зберігання персональних даних на різних серверах, що забезпечить мінімізацію витоку/знищення великої кількості персональних даних. Разом із тим, для повної реалізації прав суб'єктів персональних даних у системі E-Health необхідно створити таким суб'єктам можливість відслідковувати у режимі реального часу факт того, хто мав доступ до їх персональних даних та з якою метою (запитом) здійснювалася обробка.

Питанню відповідальності приділено окремий пункт, з якого випливає, що ефективних механізмів притягнення до відповідальності національним законодавством не передбачено, внаслідок обрання законодавцем невідповідного формулювання складу правопорушення (як адміністративного, так і кримінального). Статі та норми права, що стосуються персональних даних є мало використовуваними, що призводить до недостатності відповідної практики, у тому числі судової.

Тому цілком виникає необхідність у зміні конструкцій відповідних статей (складу правопорушення), або забезпечити ефективний захист та притягнення до відповідальності винних осіб за порушення законодавства у сфері персональних даних.

Узагальнюючи практику притягнення до адміністративної та кримінальної відповідальності у сфері персональних даних, вважаємо за необхідне запропонувати зміну складу правопорушень з матеріального, який вимагає

наявність шкоди та причинно-наслідкового зв’язку на формальний, де порушення буде вважати завершеним з моменту його вчинення, а не з моменту настання несприятливих наслідків.

У силу того, що сфера персональних даних та ті відносини, які нею регулюються має свою особливу специфіку – то не завжди порушення законодавства у сфері персональних даних нестиме ті матеріальні наслідки, які наразі вимагає законодавство. Зміна підходу до складу правопорушення забезпечить ефективну можливість притягнення до відповідальності та підвищити рівень захисту цих правовідносин. Притягнення особи (фізичної та/або юридичної) до адміністративної або кримінальної відповідальності значно покращить можливість подання позову у рамках цивільного судочинства про відшкодування моральної шкоди внаслідок незаконної обробки персональних даних.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Про захист персональних даних: Закон України від 01 червня 2010 року № 2297-VI// Відомості Верховної Ради України (ВВР) – 2010. - № 34. - ст. 481;

2. 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). Офіційна інтернет-сторінка Верховної Ради України – Режим доступу: https://zakon.rada.gov.ua/laws/show/984_008-16#Text;

3. Конвенція про захист осіб у зв’язку з автоматизованою обробкою персональних даних від 28.01.1981. Конвенцію ратифіковано із заявами згідно із Законом N 2438-VI (2438-17) від 06.07.2010.). Офіційна інтернет-сторінка Верховної Ради України – Режим доступу: https://zakon.rada.gov.ua/laws/show/994_326#Text

4. Про захист персональних даних. Законопроект № 5628 від 07.06.2021. Офіційна інтернет-сторінка Верховної Ради України - http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=72160;

5. Конвенція про захист осіб у зв’язку з автоматизованою обробкою персональних даних від 28.01.1981. Конвенцію ратифіковано із заявами згідно із Законом N 2438-VI (2438-17) від 06.07.2010.). Офіційна інтернет-сторінка Верховної Ради України – Режим доступу: https://zakon.rada.gov.ua/laws/show/994_326#Text;

6. Конституція України від 28.06.1996 № 254к/96-ВР// Відомості Верховної Ради України (ВВР) – 1996. - № 30. – ст. 141

7. Типовий порядок обробки персональних даних: наказ Уповноваженого Верховної Ради України з прав людини 08.01.2014 № 1/02-14. Офіційна інтернет-сторінка Верховної Ради України – Режим доступу: https://zakon.rada.gov.ua/laws/show/v1_02715-14#Text;

8. Про затвердження Порядку вибору лікаря, який надає первинну медичну допомогу, та форми декларації про вибір лікаря, який надає первинну медичну

допомогу. Наказ Міністерства охорони здоров'я України від 19.03.2018 № 503. Офіційна інтернет-сторінка Верховної Ради України – Режим доступу: https://moz.gov.ua/article/ministry-mandates/nakaz-moz-ukraini-vid19032018--503-pro-zatverdzhennja-porjadku-viboru-likarja-jakij-nadae-pervinnu-medichnu-dopomogu-ta-formideklaracii-pro-vibir-likarja-jakij-nadae-pervinnu-medichnu-dopomogu?preview=1;

9. Про державні фінансові гарантії медичного обслуговування населення. Закон України 19.10.2017 № 2168-VIII. Офіційна інтернет-сторінка Верховної Ради України – Режим доступу: https://zakon.rada.gov.ua/laws/show/2168-19#Text

10.Порядок функціонування електронної системи охорони здоров'я. Постанова Кабінету Міністрів України від 25 квітня 2018 р. № 411 // Офіційна інтернет-сторінка Верховної Ради України – Режим доступу: https://zakon.rada.gov.ua/laws/show/411-2018-%D0%BF#Text

11.Про інформацію. Закон України від 02.10.1992 № 2657-XII // Офіційна інтернет-сторінка Верховної Ради України – Режим доступу: https://zakon.rada.gov.ua/laws/show/2657-12#Text;

12.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. Режим доступу: https://zakon.rada.gov.ua/laws/show/n0003715-14#Text

13.Цивільний кодекс України від 16.01.2003 № 435-IV. Відомості Верховної Ради України (ВВР), 2003, NN 40-44, ст.356

14.[1] Регламент функціонування компонентів електронної системи обміну медичною інформацією, що необхідні для запуску нової моделі фінансування на первинному рівні надання медичної допомоги. Наказ Державного підприємства "Електронне здоров'я" від 29 березня 2018 року №5-ГД. Режим доступу: https://ehealth.gov.ua/wpcontent/uploads/2018/10/Rehlament_funktsionuvannia_komponentiv_elektronnoi_systemy.pdf;

15.Про електронні довірчі послуги. Закон України від 17.05.2017 № 2155-VIII. Офіційна інтернет-сторінка Верховної Ради України: https://zakon.rada.gov.ua/laws/show/2155-19#Text

16.Кодекс законів про працю України від 10.12.1971 №322-VIII. Офіційна інтернет-сторінка Верховної Ради України: https://zakon.rada.gov.ua/laws/show/322-08#Text

17.Кодекс України про адміністративні правопорушення. Відомості Верховної Ради Української РСР (ВВР) 1984, додаток до № 51, ст.1122

18.Кримінальний кодекс України від 05.04.2001 № 2341-III. Відомості Верховної Ради України (ВВР), 2001, № 25-26, ст.131

19.Про запобігання захворюванню на синдром набутого імунодефіциту (СНІД) та соціальний захист населення. Закону України від 15.01.2011 №2861-VI.

20.Рішення Суду ЄС, C-212/13, «Франтішек Ринеш проти Офісу захисту персональних даних». (František Ryneš v. Úřad pro ochranu osobních údajů), від 11 грудня 2014 р., п. 25. – Режим доступу: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:62013CJ0212;

21.Суд ЄС, C-101/01, Кримінальне провадження проти Bodil Lindqvist (Criminal proceedings against Bodil Lindqvist), від 6 листопада 2003 р., п. 27. – Режим доступу: https://eur-lex.europa.eu/legal content/EN/TXT/?qid=1512480526556&uri=CELEX:62001CJ0101;

22.«L. H. v. Latvia», заява № 52019/07, рішення від 29/04/2014

23.Постанова Верховного Суду від 06.12.2019 у справі № 664/1261/16. Режим доступу: https://reyestr.court.gov.ua/Review/86205971;

24.Постанова Верховного Суду від 16.10.2019 у справі № 752/10234/16. Режим доступу: https://reyestr.court.gov.ua/Review/85135423;

25.Постанова Верховного Суду від 19.08.2020 у справі № 201/16327/16-ц. Режим доступу - https://reyestr.court.gov.ua/Review/91104471;

26.Постанова Верховного Суду від 07.04.2020 у справі № 456/2628/17. Режим доступу - https://reyestr.court.gov.ua/Review/88692181;

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

28.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.pd;

29.Захист персональних даних: Правове регулювання та практичні аспекти: науково-практичний посібник./ Бем М. В., Городиський І. М.– К.: К.І.С., 2021 – с. 220;

30.Посібник з європейського права у сфері захисту персональних даних./ Переклад В. Костеллі — К.: К.І.С., - с. 352;

31.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 – с. 254;

32.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.

33.Сенюта І. Чому надані Омбудсманом роз'яснення породжують правову невизначеність? – Режим доступу: https://advokatpost.com/advokat-seniuta-chomu-nadani-ombudsmanom-roz-iasnennia-porodzhuiut-pravovu-nevyznachenist/;

34.Ю. Бєлова. Умови дійсності згоди на обробку персональних даних/ Ю. Бєлова// Підприємництво, господарство і право. – 2017 - № 11 – С. 14-18.;

35.Кізлова О. С. Договір про надання медичних послуг як цивільно-правовий договір / О. С. Кізлова // Право і суспільство. - 2014. - № 2. - С. 39-44.;

36.Кізлова О.С. Цивільно-правовий договір про надання медичних послуг /О.С. Кізлова // Правові та інституційні механізми забезпечення розвитку держави та права в умовах євроінтеграції : матеріали Міжнародної науково-практичної конференції (20 травня 2016 р., м. Одеса) : у 2 т. Т. 2 / відп. ред. М. В. Афанасьєва. - Одеса : Юридична література, 2016. - С. 416-420.;

37.Костенко, З.В. Механізм захисту персональних даних в європейському союзі та його вдосконалення в Україні [Текст] / З.В. Костенко, М.О. Думчиков // Реформування правової системи в контексті євроінтеграційних процесів: матеріали IV Міжнародної науково-практичної конференції: у 2-х ч. (м. Суми, 21–22 травня 2020 року) / редкол.: А.М. Куліш, О.М. Рєзнік. – Суми: Сумський державний університет, 2020. – Ч.2 – С. 69-73.;

38.Самофалов Д.О. Публічне управління у сфері охорони здоров'я /Самофалов Д.О.// Державне управління та місцеве самоврядування – 2020 рік - вип. № 1(44) – с. 92 – 99.;

39.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. Режим доступу: https://cg.harran.edu.tr/admin/Upload/files/Security_and_privacy_issues_in_e-health.pdf.

40.Eysenbach, G. What is e-health? / Eysenbach, G// Journal of medical Internet research - 2001 - № 3(2) - p.20.

41.S. Yunkap Kwankam. What e-Health can offer / S. Yunkap Kwankam// Bulletin of the World Health Organization – 2004 - № 82 (10) – c. 800 -802.;

42.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 - 2010 - pp. 268–275. Режим доступу: https://faculty.cc.gatech.edu/~lingliu/papers/2010/RuiZhang-cloud2010.pdf

43.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

44.Rahimli A. A Review of Cloud Computing Technology Solution for Healthcare System. Research Journal of Applied Sciences, Engineering and Technology 2014 8(20), p.p.2150-2153;

45.Zissis D, Lekkas D. Addressing cloud computing security issues. Future Generation Computer Systems. Volume 28, Issue 3, March 2012, p.p. 583-592. Режим доступу: https://www.sciencedirect.com/science/article/pii/S0167739X10002554#;

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

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

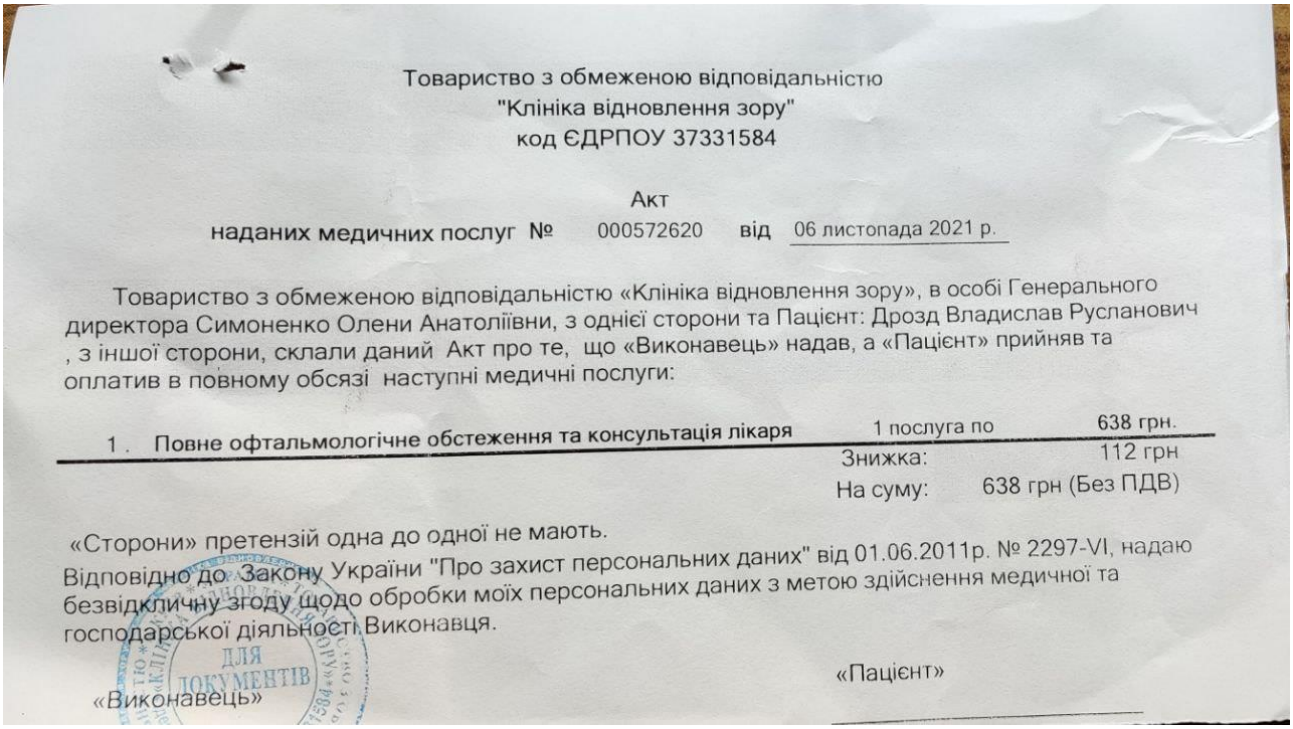
48.Li, M.; Yu, S.; Ren, K.; Lou, W. Securing Personal Health Records in Cloud Computing: Patient-centric and Fine-grained Data Access Control in Multi-owner Settings. In Proceedings of the 6th International ICST Conference on Security and Privacy in Communication Networks (SecureComm 2010), Singapore,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

49.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.;

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

51.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. Режим доступу: https://doi.org/10.3390/info11070356.

Додаток 1



Товариство з обмеженою відповідальністю
"Клініка відновлення зору"
код ЄДРПОУ 37331584

Акт
наданих медичних послуг № 000572620 від 06 листопада 2021 р.

Товариство з обмеженою відповідальністю «Клініка відновлення зору», в особі Генерального директора Симоненко Олени Анатоліївни, з однієї сторони та Пацієнт: Дрозд Владислав Русланович , з іншої сторони, склали даний Акт про те, що «Виконавець» надав, а «Пацієнт» прийняв та оплатив в повному обсязі наступні медичні послуги:

1.	Повне офтальмологічне обстеження та консультація лікаря	1 послуга по	638 грн.
		Знижка:	112 грн
		На суму:	638 грн (Без ПДВ)

«Сторони» претензій одна до одної не мають.
Відповідно до Закону України "Про захист персональних даних" від 01.06.2011р. № 2297-VI, надаю безвідкличну згоду щодо обробки моїх персональних даних з метою здійснення медичної та господарської діяльності Виконавця.

«Виконавець»

«Пацієнт»