МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

КИЇВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ ТЕХНОЛОГІЙ ТА ДИЗАЙНУ

Кваліфікаційна наукова
праця на правах рукопису

САНЖАРОВСЬКА ЛІДІЯ ІГОРІВНА

УДК 342.9:004.056.5:614

ДИСЕРТАЦІЯ

ПРАВОВЕ РЕГУЛЮВАННЯ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ У СФЕРІ ОХОРОНИ ЗДОРОВ'Я

081 – «Право»

Подається на здобуття ступеня доктора філософії

Дисертація містить результати власних досліджень. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело
_____ Л.І. Санжаровська

Науковий керівник **Оніщик Юрій Віталійович,** доктор юридичних наук, професор

Київ-2024

АНОТАЦІЯ

Санжаровська Л.І. Правове регулювання захисту персональних даних у сфері охорони здоров'я. – Кваліфікаційна наукова праця на правах рукопису.

Дисертація на здобуття ступеня доктора філософії за спеціальністю 081 «Право». – Київський національний університет технологій та дизайну, Міністерство освіти і науки України, Київ, 2024.

У дисертації здійснено теоретичне узагальнення й вирішення наукового завдання, що полягає у визначенні сутності та особливостей правового регулювання захисту персональних даних у сфері охорони здоров'я.

Встановлено, що інформатизація та цифровізація сфери охорони здоров'я зумовила виникнення проблеми безпеки персональної інформації пацієнтів. В умовах цифрової трансформації сфери охорони здоров'я випадки несанкціонованого втручання в особисте життя осіб та неправомірного поширення і використання їх медичних даних набувають загрозливого та масштабного характеру. Важливість проблеми захисту персональних даних зумовили її дослідження представниками різних юридичних наук, однак питанням правового регулювання захисту персональних даних у сфері охорони здоров'я увага на рівні фундаментальних правових досліджень не приділялася.

З'ясовано, що поняття «персональні дані» та сфера охорони здоров'я підпадають під правовий вплив різних галузей права. Персональні дані у сфері охорони здоров'я визначено як конфіденційну інформація про медичне обслуговування особи, яка дозволяє її ідентифікувати та дізнатися відомості щодо її стану здоров'я. До істотних ознак персональних даних у сфері охорони здоров'я віднесено такі: 1) конфіденційна інформація; 2) стосується фізичної особи; 3) містить інформацію про медичне обслуговування особи та відомості про її стан здоров'я; 4) фізична особа є ідентифікованою.

До конфіденційної інформації про медичне обслуговування особи відносено: інформацію про фізичну особу, зібрану під час реєстрації на надання медичних послуг або надання медичних послуг; номер, символьний знак або опис, що

приписують фізичній особі для того, щоб ідентифікувати фізичну особу для цілей охорони здоров'я; інформацію, отриману внаслідок дослідження або огляду частини тіла чи речовини, що міститься в тілі, у тому числі з генетичних даних або біологічних проб; будь-яку медичну інформацію (про медичні обстеження, про захворювання, про лікувальні заходи, про прогноз розвитку захворювання, про недієздатність, про ризик захворювання, про історію хвороби, про фізіологічний чи біомедичний стан здоров'я особи, про діагнози та будь-які документи, що стосуються здоров'я та обмеження повсякденного функціонування/життєдіяльності людини). Зазначено, що така інформація викладається у формалізованому вигляді, що забезпечує можливість обробки персональних даних у сфері охорони здоров'я в інформаційних системах.

Обґрунтовано, що інститут захисту персональних даних у сфері охорони здоров'я доцільно розглядати як: право на невтручання в особисте життя, а саме право на конфіденційну інформацію про медичне обслуговування особи та відомості щодо її стану здоров'я; комплексний правовий інститут – сукупність правових норм різної галузевої належності, які регулюють суспільні відносини, пов'язані із захистом і обробкою персональних даних у сфері охорони здоров'я; напрям діяльності – комплекс заходів, спрямованих на забезпечення конфіденційності персональних даних у сфері охорони здоров'я. Запропоновано під захистом персональних даних у сфері охорони здоров'я розуміти сукупність заходів, спрямованих на гарантування безпеки конфіденційної інформації про медичне обслуговування особи та відомостей щодо її стану здоров'я.

Періодизацію становлення інституту захисту персональних даних у сфері охорони здоров'я виокремлено за такими етапами розвитку: 1) 1991-2009 рр. – відсутність належного правового регулювання захисту персональних даних у сфері охорони здоров'я; 2) 2010-2014 рр. – запровадження інституту захисту персональних даних у сфері охорони здоров'я; 3) 2015 – дотепер – удосконалення інституту захисту персональних даних у сфері охорони здоров'я.

Аргументовано, що наявність значної кількості різних нормативно-правових актів щодо захисту персональних даних у сфері охорони здоров'я дає підстави для

класифікації їх за предметом правового регулювання на загальні та спеціальні акти. До загальних нормативних актів щодо захисту персональних даних у сфері охорони здоров'я відносено нормативні акти, які регулюють як питання захисту персональних даних, так і інші суспільні відносини. До спеціальних нормативних актів щодо захисту персональних даних у сфері охорони здоров'я відносено нормативні акти, які регулюють захист персональних даних у сфері охорони здоров'я.

Зроблено висновок, що обробка персональних даних у сфері охорони здоров'я здійснюється за умови надання пацієнтом однозначної згоди на обробку таких даних або на підставі закону. Обробка персональних даних у сфері охорони здоров'я без згоди пацієнта здійснюється: 1) коли медичні відомості необхідні в цілях охорони здоров'я (встановлення медичного діагнозу, забезпечення піклування чи лікування або надання медичних послуг, моніторинг відповідності встановленим умовам надання таких послуг функціонування електронної системи охорони здоров'я; контроль якості надання медичних послуг; обмін інформацією про фінансування медичних послуг та послуг у сфері охорони здоров'я); 2) для захисту життєво важливих інтересів суб'єкта персональних даних. Обробляти персональні дані без згоди пацієнта можна до часу, коли отримання згоди стане можливим. Обмеження щодо обробки персональних даних у сфері охорони здоров'я може здійснюватися у випадках, передбачених законом, наскільки це необхідно у демократичному суспільстві в інтересах національної безпеки, економічного добробуту або захисту прав і свобод суб'єктів персональних даних чи інших осіб.

Під суб'єктами забезпечення захисту персональних даних у сфері охорони здоров'я запропоновано розуміти фізичних та юридичних осіб, які зобов'язані забезпечити захист персональних даних у сфері охорони здоров'я від неправомірного збирання, зберігання, використання, знищення, поширення та доступу до медичних даних. До суб'єктів забезпечення захисту персональних даних у сфері охорони здоров'я віднесено: 1) володільців персональних даних у сфері охорони здоров'я – органи публічної влади (Міністерство охорони здоров'я

України та Національна служби здоров'я України) та суб'єкти господарювання приватної форми власності, діяльність яких пов'язана з медичним обслуговуванням; 2) розпорядників персональних даних у сфері охорони здоров'я – органи публічної влади та їх посадові особи, співробітники закладів охорони здоров'я публічної форми власності, суб'єкти господарювання приватної форми власності, діяльність яких пов'язана з медичним обслуговуванням, а також медичні працівники, співробітники медичного закладу, працівники, відповідальні за захист персональних даних у лікаря-підприємця; 3) третіх осіб персональних даних у сфері охорони здоров'я – органи публічної влади та суб'єкти господарювання будь-якої форми власності, діяльність яких пов'язана з медичним обслуговуванням; 4) Уповноваженого Верховної Ради України з прав людини.

Правові засоби захисту персональних даних у сфері охорони здоров'я визначено як заходи компетентних суб'єктів, які спрямовані на запобігання, припинення правопорушення у сфері захисту медичних даних, відновлення порушеного права чи компенсацію заподіяної правопорушенням шкоди. Серед таких заходів виокремлено превентивні, припиняючі та відновлючі, а також охарактеризовано особливості їх застосування. Наголошено, що превентивні заходи спрямовані на запобігання порушенням законодавства про захист персональних даних у сфері охорони здоров'я, припиняючі – на усунення та припинення порушення законодавства про захист персональних даних, відновлювальні – на відновлення порушеного права, усунення перешкод в його реалізації та загрози порушення суб'єктивних прав протиправними діями. Зроблено висновок, що превентивні та припиняючі заходи уповноважені застосовувати володільці, розпорядники, треті особи та Уповноважений Верховної Ради України з прав людини, а відновлючі заходи, крім цих суб'єктів, має право застосовувати також суд.

Встановлено, що у міжнародному та європейському правопорядку право на захист персональних даних є основоположним правом на рівні з правом на приватне життя. Запропоновано міжнародні стандарти правового регулювання захисту персональних даних у сфері охорони здоров'я класифікувати на

міжнародні акти загального характеру, які регулюють захист персональних даних у сфері охорони здоров'я опосередковано, та міжнародні документи, які безпосередньо стосуються захисту персональних даних у сфері охорони здоров'я. Зазначено, що міжнародні стандарти сприяють формуванню ефективного національного законодавства про захист персональних даних та охорону здоров'я. Європейські стандарти правового регулювання захисту персональних даних у сфері охорони здоров'я характеризуються значним масивом нормативних актів Ради Європи та Європейського Союзу, а також судовою практикою Європейського суду з прав людини. Європейські стандарти правового регулювання захисту персональних даних у сфері охорони здоров'я мають фундаментальне значення для України щодо виконання зобов'язання про приведення національного законодавства у відповідність до європейського законодавства. Наголошено, що забезпечення належного рівня захисту персональних даних у сфері охорони здоров'я відповідно до міжнародних та європейських стандартів є одним пріоритетних завдань України.

Констатовано, що сучасний стан законодавства характеризуються неузгодженістю та протиріччям і не в повній мірі забезпечує захист персональних даних у сфері охорони здоров'я в Україні. До напрямів вдосконалення правового регулювання захисту персональних даних у сфері охорони здоров'я в Україні, віднесено такі: 1) прийняття нового Закону України «Про захист персональних даних», який буде спрямований на регулювання суспільних відносин, пов'язаних із захистом персональних даних загалом, так і захисту персональних даних в конкретних сферах суспільних відносин, у тому числі у сфері охорони здоров'я; 2) упорядкування законодавства про охорону здоров'я із законодавством про захист персональних даних; 3) створення нового спеціального незалежного від інших органів публічної влади контролюючого органу за додержанням законодавства про захист персональних даних; 4) реформування інституту юридичної відповідальності за порушення законодавства про захист персональних даних; 5) належна регламентація відносин, пов'язаних із безпекою та конфіденційністю персональних даних у сфері охорони здоров'я;

6) приведення законодавства про захист персональних даних та охорону здоров'я у відповідність до міжнародних та європейських стандартів.

Обґрунтовано, що новий Закон України «Про захист персональних даних» повинен містити окремий розділ «Захист персональних даних у сфері охорони здоров'я», у якому необхідно передбачити чітке розуміння поняття «медичні дані», співвідношення законодавства про захист персональних даних та охорону здоров'я, цілі обробки медичних даних, підстави та вимоги до обробки медичних даних, порядок та умови надання згоди пацієнта на обробку його медичних даних, особливості функціонування електронної системи охорони здоров'я, права пацієнта як суб'єкта медичних даних, обов'язки суб'єктів господарювання у сфері медичного обслуговування як володільців (контролерів) та розпорядників (операторів) медичних даних, вимоги до порядку обробки медичних даних як внутрішнього документа суб'єктів господарювання у сфері медичного обслуговування, вимоги до суб'єктів інформаційного забезпечення системи охорони здоров'я, порядок та умови доступу до медичних даних третіх осіб, особливості передачі медичних даних на територію іноземної держави або міжнародній організації, правила конфіденційності щодо медичних даних, особливості контролю за дотриманням законності при обробці медичної інформації, особливості зберігання медичних даних, гарантії безпеки медичних даних.

Ключові слова: персональні дані, захист, охорона здоров'я, медичні дані, правове регулювання, медична інформація, медичне обслуговування, стан здоров'я.

SUMMARY

Sanzharovska L.I. Legal regulation of personal data protection in the field of health care. – Qualification scientific work on the rights of manuscript.

Dissertation for obtaining the scientific degree of the Doctor of Philosophy on a specialty 081 Law. – Kyiv National University of Technologies and Design, Ministry of

Education and Science of Ukraine, Kyiv, 2024.

In the dissertation, a theoretical generalization and solution of the scientific task is carried out, which consists in determining the essence and features of the legal regulation of personal data protection in the field of health care.

It was established that the informatization and digitization of the health care sector caused the problem of the security of personal information of patients. In the conditions of the digital transformation of the health care sector, cases of unauthorized interference in the private life of individuals and the illegal distribution and use of their medical data are becoming threatening and large-scale. The importance of the problem of personal data protection was determined by its research by representatives of various legal sciences, but the legal regulation of personal data protection in the field of health care was not given attention at the level of fundamental legal research.

It was found that the concept of «personal data» and the field of health care are under the legal influence of various branches of law. Personal data in the field of health care is defined as confidential information about the medical care of a person that allows him to be identified and to learn information about his health. The essential features of personal data in the field of health care include the following: 1) confidential information; 2) concerns a natural person; 3) contains information about a person's medical care and information about his state of health; 4) the natural person is identified.

Confidential information about a person's medical care includes: information about a natural person collected during registration for the provision of medical services or the provision of medical services; a number, symbol or description attributed to an individual in order to identify the individual for health care purposes; information obtained as a result of research or examination of a part of the body or a substance contained in the body, including from genetic data or biological samples; any medical information (about medical examinations, about diseases, about medical measures, about the prognosis of the development of the disease, about incapacity, about the risk of disease, about the medical history, about the physiological or biomedical state of health of the person, about diagnoses and any documents, related to health and

limitation of daily functioning/life activities of a person). It is noted that such information is presented in a formalized form, which provides the possibility of processing personal data in the field of health care in information systems.

It is justified that the institution of personal data protection in the field of health care should be considered as: the right to non-interference in personal life, namely the right to confidential information about a person's medical care and information about his state of health; complex legal institution – a set of legal norms of different branches that regulate social relations related to the protection and processing of personal data in the field of health care; the field of activity is a set of measures aimed at ensuring the confidentiality of personal data in the field of health care. It is suggested that the protection of personal data in the field of health care should be understood as a set of measures aimed at guaranteeing the safety of confidential information about a person's medical care and information about his state of health.

The periodization of the establishment of the institute for the protection of personal data in the field of health care is distinguished according to the following stages of development: 1) 1991-2009 – lack of proper legal regulation of personal data protection in the field of health care; 2) 2010-2014 – introduction of the institute for the protection of personal data in the field of health care; 3) 2015 – until now – improvement of the institute for the protection of personal data in the field of health care.

It is argued that the presence of a significant number of different normative legal acts on the protection of personal data in the field of health care provides grounds for classifying them according to the subject of legal regulation into general and special acts. The general regulations on the protection of personal data in the field of health care include regulations that regulate both the issue of personal data protection and other public relations. Special normative acts on the protection of personal data in the field of health care include normative acts that regulate the protection of personal data in the field of health care.

It was concluded that the processing of personal data in the field of health care is carried out on the condition that the patient gives unambiguous consent to the processing of such data or based on the law. Processing of personal data in the field of

health care without the patient's consent is carried out: 1) when medical information is necessary for the purposes of health care (establishing a medical diagnosis, providing care or treatment or providing medical services, monitoring compliance with the established conditions for the provision of such services, the functioning of the electronic system health care; quality control of the provision of medical services; exchange of information on the financing of medical services and services in the field of health care); 2) to protect the vital interests of the subject of personal data. It is possible to process personal data without the patient's consent until such time as consent becomes possible. Restrictions on the processing of personal data in the field of health care may be implemented in cases provided for by law, as far as it is necessary in a democratic society in the interests of national security, economic well-being or protection of the rights and freedoms of the subjects of personal data or other persons.

Subjects of protection of personal data in the field of health care are proposed to be understood as natural and legal entities that are obliged to ensure the protection of personal data in the field of health care from unlawful collection, storage, use, destruction, dissemination and access to medical data Subjects of personal data protection in the field of health care include: 1) owners of personal data in the field of health care – public authorities (the Ministry of Health of Ukraine and the National Health Service of Ukraine) and subjects management of a private form of ownership, the activities of which are related to medical care; 2) administrators of personal data in the field of health care – public authorities and their officials, employees of publicly owned health care institutions, private business entities whose activities are related to medical care, as well as medical employees, employees of a medical institution, employees responsible for the protection of personal data of a doctor-entrepreneur; 3) personal data of third parties in the field of health care – public authorities and business entities of any form of ownership, whose activities are related to medical care; 4) Human Rights Commissioner of the Verkhovna Rada of Ukraine.

Legal means of protection of personal data in the field of health care are defined as measures taken by competent entities aimed at preventing, stopping an offense in the field of medical data protection, restoring the violated right or compensating for the

damage caused by the offense. It is emphasized that preventive measures are aimed at preventing violations of the legislation on the protection of personal data in the field of health care, preventive measures – at the elimination and termination of violations of the legislation on the protection of personal data, restorative measures - at the restoration of the violated right, the elimination of obstacles to its implementation and the threat of violation of sub objective rights by illegal actions. Among such measures, preventive, stopping and restorative ones are singled out, and the peculiarities of their application are also characterized. It was concluded that owners, administrators, third parties and the Commissioner of the Verkhovna Rada of Ukraine for human rights are authorized to apply preventive and termination measures, and restorative measures, in addition to these subjects, can also be applied by the court.

It has been established that in the international and European legal order, the right to the protection of personal data is a fundamental right on a par with the right to privacy. It is proposed to classify the international legal standards for the protection of personal data in the field of health care into international acts of a general nature, which indirectly regulate the protection of personal data in the field of health care, and international documents that directly relate to the protection of personal data in the field of health care. It is noted that international standards contribute to the formation of effective national legislation on personal data protection and health care. European standards of legal regulation of personal data protection in the field of health care are characterized by a significant array of normative acts of the Council of Europe and the European Union, as well as the judicial practice of the European Court of Human Rights. European standards of legal regulation of personal data protection in the field of health care are of fundamental importance for Ukraine in terms of fulfilling the obligation to bring national legislation into line with European legislation. It was emphasized that ensuring an adequate level of protection of personal data in the field of health care in accordance with international and European standards is one of Ukraine's priority tasks.

It was established that the current state of legislation is characterized by inconsistencies and contradictions and does not fully ensure the protection of personal

data in the field of health care in Ukraine. The directions for improving the legal regulation of personal data protection in the field of health care in Ukraine include the following: 1) adoption of the new Law of Ukraine «On the Protection of Personal Data», which will be aimed at regulating social relations related to the protection of personal data in general, as well as the protection of personal data in specific spheres of public relations, including in the sphere of health care; 2) harmonization of the legislation on health protection with the legislation on the protection of personal data; 3) creation of a new special supervisory body independent of other public authorities for compliance with the legislation on the protection of personal data; 4) reforming the institution of legal responsibility for violation of the legislation on the protection of personal data; 5) proper regulation of relations related to the security and confidentiality of personal data in the field of health care; 6) bringing the legislation on personal data protection and health protection into compliance with international and European standards.

It is justified that the new Law of Ukraine «On the protection of personal data» should contain a separate section «Protection of personal data in the field of health care», in which it is necessary to provide a clear understanding of the concept of «medical data», the relationship between the legislation on the protection of personal data and health care I, the purposes of processing medical data, the grounds and requirements for processing medical data, the procedure and conditions for granting the patient's consent to the processing of his medical data, the features of the functioning of the electronic health care system, the rights of the patient as a subject of medical data, the obligations of the subject economic entities in the field of medical services as owners (controllers) and administrators (operators) of medical data, requirements for the procedure for processing medical data as an internal document of economic entities in the field of medical services, requirements for subjects of information provision of the health care system, procedure and conditions of access to medical data of third parties, features of transfer of medical data to the territory of a foreign state or international organization, rules of confidentiality regarding medical data, features of monitoring

compliance with the legality of medical information processing, features of storage of medical data, guarantees of security of medical data.

Key words: personal data, protection, health care, medical data, legal regulation, medical information, medical care, state of health.

СПИСОК ПУБЛІКАЦІЙ ЗДОБУВАЧА ЗА ТЕМОЮ ДИСЕРТАЦІЇ:

в яких опубліковані основні наукові результати дисертації:

1. Санжаровська Л.І. Правова інтерпретація інституту захисту персональних даних у сфері охорони здоров'я. *Прикарпатський юридичний вісник.* 2024. № 1 (54). С. 84–87. DOI: https://doi.org/10.32782/pyuv.v1.2024.16.

2. Санжаровська Л.І. Поняття та сутність персональних даних у сфері охорони здоров'я. *Наука і техніка сьогодні.* 2024. № 3 (31). С. 182-192. DOI: https://doi.org/10.52058/2786-6025-2024-3(31)-182-192.

3. Санжаровська Л.І. Правові особливості захисту фізичних осіб у зв'язку з обробкою персональних даних у сфері охорони здоров'я. *Актуальні питання у сучасній науці.* 2024. № 5 (23). С. 666–676. DOI: https://doi.org/10.52058/2786-6300-2024-5(23)-666-676.

які засвідчують апробацію матеріалів дисертації:

1. Санжаровська Л.І. Вплив застосування технологій штучного інтелекту на захист персональних даних у сфері охорони здоров'я. *Актуальні проблеми приватного та публічного права*: матеріали VI Міжнародної науково-практичної конференції присвяченої 95-річчю від дня народження члена-кореспондента НАПрН України, академіка Міжнародної кадрової академії, Заслуженого діяча науки України, доктора юридичних наук, професора Процевського О.І., Ломжа – Харків, 29 березня 2024 року. Ломжа: Міжнародна Академія Прикладних Наук в Ломжі, Республіка Польща; Харків: Харківський національний педагогічний університет імені Г.С. Сковороди, Україна. Видавництво: MANS w Łomży – Харків: ХНПУ імені Г.С. Сковороди, 2024. С. 317–320.

2. Санжаровська Л.І. Адаптація законодавства про захист персональних даних у сфері охорони здоров'я України до законодавства Європейського Союзу. *Історико-філософські, політико-правові та соціальні засади трансформації України та держав європейської спільноти*: матеріали І Міжнародної науково-практичної конференції (19 квітня 2024 р.). Одеса: ОНМУ, 2024. С. 119–121.

3. Санжаровська Л.І. Принципи обробки персональних даних у сфері охорони здоров'я. *Проблеми захисту прав та свобод людини і громадянина*: матеріали Х Всеукраїнської наук.-практ. конф. молодих учених і студентів (м. Чернігів, 17 травня 2024 р.). Чернігів: НУ «Чернігівська політехніка», 2024. С. 40–42.

4. Санжаровська Л.І. Захист персональних даних у сфері охорони здоров'я Уповноваженим Верховної Ради України з прав людини. *Правові засади організації та здійснення публічної влади*: збірник тез VII Міжнародної науково-практичної конференції, присвяченої світлій пам'яті доктора юридичних наук, професора, академіка-засновника НАПрНУ, першого Голови Конституційного Суду України Леоніда Петровича Юзькова (м. Хмельницький, 17 травня 2024 року). Хмельницький: Хмельницький університет управління та права імені Леоніда Юзькова, 2024. С. 213–214.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

ВР України – Верховна Рада України

ЄС – Європейський Союз

ЄСПЛ – Європейський суд з прав людини

КУпАП – Кодекс України про адміністративні правопорушення

КК України – Кримінальний кодекс України

КМ України – Кабінет Міністрів України

Конвенція 108 – Конвенція про захист осіб у зв'язку з автоматизованою обробкою персональних даних від 28 січня 1981 року

Конвенція 108+ – Конвенція про захист осіб у зв'язку з автоматизованою обробкою персональних даних від 28 січня 1981 року (модернізована)

МОЗ – Міністерство охорони здоров'я України

НСЗУ – Національна служба здоров'я України

Загальний регламент про захист даних ЄС – Регламент Європейського парламенту і Ради (ЄС) 2016/679 від 27 квітня 2016 року про захист фізичних осіб у зв'язку з обробкою персональних даних і про вільний рух таких даних, та про скасування Директиви 95/46/ЄС

РЄ – Рада Європи

ВСТУП

Обґрунтування вибору теми дослідження. У процесі медичного обслуговування відбувається обмін інформацією між учасниками відносин у сфері охорони здоров'я. Отримані від фізичних осіб відомості суб'єктами, які здійснюють медичну діяльність, являють собою конфіденційну інформацію. Збирання, зберігання, використання та поширення такої інформації можливе за їхнім бажанням відповідно до передбачених ними умов. Недотримання принципу конфіденційності даних про стан здоров'я може призвести до незаконного доступу до медичних даних, що зумовить порушення права на невтручання в особисте життя конкретної особи та негативні наслідки для національної безпеки загалом. У зв'язку з тим, що такі правопорушення характеризується високим рівнем латентності випадки несанкціонованого втручання в особисте життя пацієнтів та неправомірного поширення і використання їх персональних даних набувають загрозливого та масштабного характеру.

В умовах інформатизації та цифровізації сфери охорони здоров'я проблема безпеки персональної інформації пацієнтів набуває особливого значення. Використання інформаційно-комунікаційних технологій у сфері охорони здоров'я не тільки сприяє покращенню її функціонуванню, але і породжує новітні виклики та загрози щодо неконтрольованого накопичення і обробки медичних даних, які в подальшому можуть бути використані всупереч інтересам пацієнта. Застосування інформаційних та цифрових технологій у медицині потребує створення належних гарантій для запобігання будь-якому розголошенню персональних даних у сфері охорони здоров'я.

Законодавство про захист персональних даних та охорону здоров'я не дає цілісного уявлення щодо сутності та особливостей захисту персональних даних у сфері охорони здоров'я. Чинний Закон України «Про захист персональних даних» в переважній більшості містить загальні норми дії без чіткого розмежування конкретних сфер суспільних відносин, що призводить до неузгодженості та протиріччя стосовно захисту персональних даних у сфері охорони здоров'я. Це

зумовлено як недостатньою теоретичною розробкою проблеми захисту персональних даних у сфері охорони здоров'я, так і недосконалістю чинного законодавства. За таких обставин необхідний всебічний аналіз національного законодавства, міжнародних та європейських стандартів, який дозволить з'ясувати сутність інституту захисту персональних даних у сфері охорони здоров'я та визначити напрями удосконалення правового регулювання захисту персональних даних у сфері охорони здоров'я. Усі перераховані обставини у їх комплексі зумовлюють нагальну потребу у дослідженні правового регулювання захисту персональних даних у сфері охорони здоров'я.

Науково-теоретичним підґрунтям дослідження стали праці учених у галузі адміністративного, інформаційного, цивільного, міжнародного права, захисту персональних даних та охорони здоров'я, зокрема А.В. Авраменко, Ю.Д. Бєлової, О.О. Бригінця, В.М. Брижка, Г.В. Виноградової, Д.С. Гети, З.С. Гладуна, А.М. Гуза, Т.О. Гуржія, І.С. Демченко, Ю.І. Дем'яненко, І.В. Діордіци, О.А. Дмитренко, О.С. Дяковського, О.В. Клименко, І.А. Коваленко, Ю.О. Коваленко, О.М. Коваль, І.Б. Короля, Р.А. Майданик, К.С. Мельника, Ю.В. Меха, О.І. Миколенка, Ю.В. Назарка, Ю.В. Оніщика, А.В. Пазюка, Р.В. Перелигіної, А.Л. Петрицького, В.В. Пилипчука, І.С. Пономаренка, М.В. Різака, І.І. Романюка, М.І. Саєнка, Ю.С. Самойленко, І.А. Сенюти, І.Б. Сосніна, О.А. Тимошенка, В.І. Тимченка, К.С. Токарєвої, А.В. Туніка, Д.В. Цвірюка, О.Б. Червякової, О.М. Шамича, О.О. Шевчука, А.О. Щербини, М.Ю. Щирба, С.В. Ясечко та ін.

Незважаючи на значне зацікавлення науковців проблематикою захисту персональних даних, необхідно констатувати, що у правовій науці правове регулювання захисту персональних даних у сфері охорони здоров'я не було предметом окремого дослідження. Відсутність комплексного монографічного дослідження правового регулювання захисту персональних даних у сфері охорони здоров'я зумовлює актуальність обраної теми та її важливе наукове та практичне значення.

Зв'язок роботи з науковими програмами, планами, темами, грантами.

Дисертацію виконано відповідно до Стратегії національної безпеки України, затвердженої Указом Президента України від 14 вересня 2020 року № 392/2020, Концепції розвитку штучного інтелекту в Україні, схваленої розпорядженням Кабінету Міністрів України від 2 грудня 2020 року № 1556-р, Концепції розвитку електронної охорони здоров'я, схваленої розпорядженням Кабінету Міністрів України від 28 грудня 2020 року № 1671-р, Національної стратегії у сфері прав людини, затвердженої Указом Президента України від 24 березня 2021 року № 119/2021, Стратегії інформаційної безпеки, затвердженої Указом Президента України від 28 грудня 2021 року № 685/2021, Плану з виконання Угоди про асоціацію між Україною, з однієї сторони, та Європейським Союзом, Європейським співтовариством з атомної енергії і їхніми державами-членами, з іншої сторони, затвердженого постановою Кабінету Міністрів України від 25 жовтня 2017 року № 1106, Плану науково-дослідних робіт Київського національного університету технологій та дизайну за темою «Правове забезпечення реалізації прав, свобод і законних інтересів суб'єктів правових відносин у сфері публічного адміністрування» (номер державної реєстрації 0122U201691).

Мета і завдання дослідження. *Метою* роботи є визначення сутності та особливостей правового регулювання захисту персональних даних у сфері охорони здоров'я, а також формування напрямів удосконалення у цій сфері.

Для досягнення зазначеної мети поставлені такі *завдання*:

– розглянути персональні дані як категорію наукового пізнання та об'єкта правового регулювання у сфері охорони здоров'я;

– визначити поняття та етапи формування інституту захисту персональних даних у сфері охорони здоров'я;

– охарактеризувати сутність та особливості захисту фізичних осіб у зв'язку з обробкою персональних даних у сфері охорони здоров'я;

– встановити суб'єктів забезпечення захисту персональних даних у сфері охорони здоров'я;

– з'ясувати правові засоби захисту персональних даних у сфері охорони

здоров’я;

– проаналізувати міжнародні та європейські стандарти захисту персональних даних у сфері охорони здоров’я;

– сформулювати напрями вдосконалення правового регулювання захисту персональних даних у сфері охорони здоров’я.

Об’єкт дослідження – суспільні відносини, що виникають у процесі захисту персональних даних у сфері охорони здоров’я.

Предмет дослідження – правове регулювання захисту персональних даних у сфері охорони здоров’я.

Методи дослідження. Дослідження проведено з використанням загальнонаукових та спеціальних методів, які були обрані з урахуванням поставленої мети, визначених завдань, об’єкта та предмета дослідження. Застосування *діалектичного* методу дозволило розглянути всі питання дослідження в динаміці, виявити їх взаємозв’язок і взаємозумовленість та сприяло комплексному аналізу правового регулювання захисту персональних даних у сфері охорони здоров’я (розділи 1–3). Метод *термінологічного аналізу* та *логіко-семантичний* метод застосовано під час з’ясування персональних даних як категорії наукового пізнання та об’єкта правового регулювання у сфері охорони здоров’я, сутності інституту захисту персональних даних у сфері охорони здоров’я, а також при визначенні таких понять як «персональні дані у сфері охорони здоров’я», «захист персональних даних у сфері охорони здоров’я», «конфіденційна інформація», «медична інформація», «охорона здоров’я», «дані про стан здоров’я», «стан здоров’я», «таємниця про стан здоров’я», «лікарська таємниця», «медичне обслуговування», «обробка персональних даних у сфері охорони здоров’я», «володілець персональних даних у сфері охорони здоров’я», «розпорядник персональних даних у сфері охорони здоров’я», «треті особи персональних даних у сфері охорони здоров’я», «життєво важливі інтереси суб’єкта персональних даних», «суб’єкти забезпечення захисту персональних даних у сфері охорони здоров’я», «правові засоби захисту персональних даних у сфері охорони здоров’я» (підрозділи 1.1, 1.2, 2.2, 2.3, 3.2). За допомогою *історико-*

правового методу визначено етапи формування інституту захисту персональних даних у сфері охорони здоров'я (підрозділ 1.2). *Формально-юридичний* та *структурно-функціональний* методи дозволили встановити сутність та особливості захисту фізичних осіб у зв'язку з обробкою персональних даних у сфері охорони здоров'я, суб'єктів забезпечення захисту персональних даних у сфері охорони здоров'я, правові засоби захисту персональних даних у сфері охорони здоров'я (підрозділи 2.1, 2.2, 2.3). *Статистичний* метод використано під час дослідження стану безпеки персональної інформації пацієнтів, узагальнення діяльності Уповноваженого Верховної Ради України з прав людини у сфері додержання законодавства про захист персональних даних (підрозділи 1.1, 2.3, 3.2). *Порівняльно-правовий* метод застосовано під час аналізу міжнародних та європейських стандартів захисту персональних даних у сфері охорони здоров'я (підрозділ 3.1). Методи *моделювання, аналізу та синтезу* використані при розробці напрямів удосконалення правового регулювання захисту персональних даних у сфері охорони здоров'я (підрозділ 3.2).

Нормативну основу дослідження склали Конституція України, Закон України «Про захист персональних даних», Закон України «Основи законодавства України про охорону здоров'я», Регламент Європейського парламенту і Ради (ЄС) 2016/679 від 27 квітня 2016 року про захист фізичних осіб у зв'язку з обробкою персональних даних і про вільний рух таких даних, та про скасування Директиви 95/46/ЄС (Загальний регламент про захист даних), Конвенція про захист осіб у зв'язку з автоматизованою обробкою персональних даних, інші нормативно-правові акти.

Емпіричну базу дослідження становлять наукові, публіцистичні, довідкові, енциклопедичні, монографічні видання, узагальнення діяльності Уповноваженого Верховної Ради України з прав людини у сфері додержання законодавства про захист персональних даних, узагальнення діяльності суб'єктів господарювання у сфері медичного обслуговування щодо захисту персональних даних у сфері охорони здоров'я, узагальнення даних електронних медичних інформаційних систем, судова практика щодо захисту персональних даних у сфері охорони

здоров'я, статистичні дані щодо захисту персональних даних загалом та у сфері охорони здоров'я зокрема.

Наукова новизна отриманих результатів полягає в тому, що дисертація є першим в Україні комплексним, науковим, монографічним дослідженням правового регулювання захисту персональних даних у сфері охорони здоров'я. В результаті проведеного дослідження сформульовано низку нових науково-теоретичних та практичних положень, висновків та пропозицій для розвитку правового регулювання захисту персональних даних у сфері охорони здоров'я. Основні з них такі:

вперше:

– сформульовано дефініцію «персональні дані у сфері охорони здоров'я» як конфіденційну інформацію про медичне обслуговування особи, яка дозволяє її ідентифікувати та дізнатися відомості щодо її стану здоров'я;

– визначено поняття «захист персональних даних у сфері охорони здоров'я» як сукупність заходів, спрямованих на гарантування безпеки конфіденційної інформації про медичне обслуговування особи та відомостей щодо її стану здоров'я;

– запропоновано інститут захисту персональних даних у сфері охорони здоров'я розглядати як: право на невтручання в особисте життя, а саме право на конфіденційну інформацію про медичне обслуговування особи та відомості щодо її стану здоров'я; комплексний правовий інститут – сукупність правових норм різної галузевої належності, які регулюють суспільні відносини, пов'язані із захистом і обробкою персональних даних у сфері охорони здоров'я; напрям діяльності – комплекс заходів, спрямованих на забезпечення конфіденційності персональних даних у сфері охорони здоров'я;

– здійснено періодизацію становлення інституту захисту персональних даних у сфері охорони здоров'я в Україні за такими етапами розвитку: 1) 1991-2009 рр. – відсутність належного правового регулювання захисту персональних даних у сфері охорони здоров'я; 2) 2010-2014 рр. – запровадження інституту захисту персональних даних у сфері охорони здоров'я; 3) 2015 – дотепер – удосконалення

інституту захисту персональних даних у сфері охорони здоров'я;

– диференційовано нормативно-правові акти щодо захисту персональних даних у сфері охорони здоров'я за предметом правового регулювання на загальні та спеціальні акти. До загальних нормативних актів щодо захисту персональних даних у сфері охорони здоров'я відносено нормативні акти, які регулюють як питання захисту персональних даних, так і інші суспільні відносини. До спеціальних нормативних актів щодо захисту персональних даних у сфері охорони здоров'я відносено нормативні акти, які регулюють захист персональних даних у сфері охорони здоров'я;

– надано авторську класифікацію суб'єктів забезпечення захисту персональних даних у сфері охорони здоров'я, до яких віднесено: 1) володільців персональних даних у сфері охорони здоров'я – органи публічної влади (Міністерство охорони здоров'я України та Національна служби здоров'я України) та суб'єкти господарювання приватної форми власності, діяльність яких пов'язана з медичним обслуговуванням; 2) розпорядників персональних даних у сфері охорони здоров'я – органи публічної влади та їх посадові особи, співробітники закладів охорони здоров'я публічної форми власності, суб'єкти господарювання приватної форми власності, діяльність яких пов'язана з медичним обслуговуванням, а також медичні працівники, співробітники медичного закладу, працівники, відповідальні за захист персональних даних у лікаря-підприємця; 3) третіх осіб персональних даних у сфері охорони здоров'я – органи публічної влади та суб'єкти господарювання будь-якої форми власності, діяльність яких пов'язана з медичним обслуговуванням; 4) Уповноваженого Верховної Ради України з прав людини;

– обґрунтовано та доведено прикладну значущість напрямів вдосконалення правового регулювання захисту персональних даних у сфері охорони здоров'я в Україні, до яких віднесено: прийняття нового Закону України «Про захист персональних даних», який буде спрямований на регулювання суспільних відносин, пов'язаних із захистом персональних даних загалом, так і захисту персональних даних в конкретних сферах суспільних відносин, у тому числі у

сфері охорони здоров'я; упорядкування законодавства про охорону здоров'я із законодавством про захист персональних даних; належна регламентація відносин, пов'язаних із безпекою та конфіденційністю персональних даних у сфері охорони здоров'я; новий Закон України «Про захист персональних даних» повинен містити окремий розділ «Захист персональних даних у сфері охорони здоров'я»;

удосконалено:

– розуміння поняття «правові засоби захисту персональних даних у сфері охорони здоров'я» як заходів компетентних суб'єктів, які спрямовані на запобігання, припинення правопорушення у сфері захисту медичних даних, відновлення порушеного права чи компенсацію заподіяної правопорушенням шкоди;

– теоретичне обґрунтування впливу міжнародних та європейських стандартів захисту персональних даних на правове регулювання захисту персональних даних у сфері охорони здоров'я в Україні, виокремивши міжнародні та європейські акти загального характеру та, які безпосередньо стосуються захисту персональних даних у сфері охорони здоров'я;

набули подальшого розвитку:

– наукові підходи щодо правової природи персональних даних та підстав їх класифікації;

– наукові положення, що охорона здоров'я характеризується комплексним характером, який зумовлений наявністю приватних і публічних правовідносин;

– особливості правового статусу суб'єктів відносин, пов'язаних із захистом персональних даних;

– погляди науковців стосовно особливостей застосування превентивних, припиняючих та відновлючих заходів захисту персональних даних;

– твердження про суттєві недоліки інституту юридичної відповідальності за порушення законодавства про захист персональних даних;

– пропозиції стосовно вдосконалення правового регулювання захисту персональних даних, у тому числі у сфері охорони здоров'я, а саме: створення нового спеціального незалежного від інших органів публічної влади контролюючого органу за додержанням законодавства про захист персональних

даних; реформування інституту юридичної відповідальності за порушення законодавства про захист персональних даних; приведення законодавства про захист персональних даних та охорону здоров'я у відповідність до міжнародних та європейських стандартів.

Практичне значення отриманих результатів полягає у тому, що сформульовані у роботі висновки і пропозиції можуть бути використані у:

– *науково-дослідній діяльності* – як підґрунтя для проведення подальших наукових досліджень правового регулювання захисту персональних даних у сфері охорони здоров'я;

– *правотворчій діяльності* – для вдосконалення правового регулювання захисту персональних даних у сфері охорони здоров'я;

– *правозастосовній діяльності* – для чіткого розуміння та застосування норм законодавства щодо захисту персональних даних у сфері охорони здоров'я;

– *освітньому процесі* – під час розробки та викладанні навчальних дисциплін «Адміністративне право», «Адміністративний процес» та «Цивільне право».

Особистий внесок здобувача. Дисертація є самостійною завершеною науковою працею. Основні положення, що характеризують наукову новизну дослідження, теоретичне і практичне значення його результатів, розроблені дисертанткою особисто.

Апробація матеріалів дисертації. Основні положення дисертації оприлюднено на таких міжнародних та всеукраїнських науково-практичних конференціях: «Актуальні проблеми приватного та публічного права» (м. Ломжа – Харків, 29 березня 2024 р.); «Історико-філософські, політико-правові та соціальні засади трансформації України та держав європейської спільноти» (м. Одеса, 19 квітня 2024 р.); «Проблеми захисту прав та свобод людини і громадянина» (м. Чернігів, 17 травня 2024 р.); «Правові засади організації та здійснення публічної влади» (м. Хмельницький, 17 травня 2024 р.).

Структура та обсяг дисертації. Структура складається з вступу, трьох розділів, що охоплюють сім підрозділів, висновків, списку використаних джерел і

додатків. Загальний обсяг дисертації становить 230 сторінок. Список використаних джерел містить 234 найменування, розміщених на 30 сторінках.

РОЗДІЛ 1
ТЕОРЕТИЧНІ ЗАСАДИ ПРАВОВОГО РЕГУЛЮВАННЯ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ У СФЕРІ ОХОРОНИ ЗДОРОВ'Я

1.1. Персональні дані як категорія наукового пізнання та об'єкта правового регулювання у сфері охорони здоров'я

Трансформація світового суспільства до інформаційного шляхом впровадження інформаційно-комунікаційних технологій в усі сфери життєдіяльності впливає на умови формування відносин щодо створення, збирання, одержання, зберігання, використання, поширення, охорони та захисту інформації. Основним завданням розвитку інформаційного суспільства в Україні є сприяння кожній людині на засадах широкого використання сучасних інформаційно-комунікаційних технологій можливостей створювати інформацію і знання, користуватися та обмінюватися ними, виробляти товари та надавати послуги, повною мірою реалізовуючи свій потенціал, підвищуючи якість свого життя. Розвиток інформаційного суспільства в Україні та впровадження новітніх інформаційно-комунікаційних технологій в усі сфери суспільного життя і в діяльність органів державної влади та органів місцевого самоврядування визначається одним з пріоритетних напрямів державної політики [1].

Одним з пріоритетних завдань для України є залучення інформаційно-комунікаційних технологій для поліпшення демографічної ситуації, збереження і зміцнення здоров'я населення, підвищення якості та ефективності медико-санітарної допомоги, забезпечення соціальної справедливості та прав громадян на охорону здоров'я. Впровадження інформаційно-комунікаційних технологій у сферу охорони здоров'я потребує розроблення стандартів обміну медичними даними за умови забезпечення недоторканності приватного життя [1].

Інформатизація процесів забезпечення розвитку інформаційного суспільства супроводжується значним зростанням кількості інформаційних систем та об'ємом даних, які містяться в них. Розширене застосування сучасних інформаційних

технологій (технологій великих даних, хмарних обчислень, штучного інтелекту тощо) не тільки сприяє покращенню всіх сфер суспільного життя, але і породжує новітні виклики та загрози щодо неконтрольованого накопичення і обробки особистих даних, які в подальшому можуть бути використані всупереч інтересам особи. Тому за умов швидкого розвитку глобального інформаційного суспільства, широкого використання інформаційно-комунікаційних технологій у всіх сферах життя особливого значення набувають проблеми інформаційної безпеки – стану захищеності життєво важливих інтересів людини, суспільства і держави, при якому запобігається нанесення шкоди через: неповноту, невчасність та невірогідність інформації, що використовується; негативний інформаційний вплив; негативні наслідки застосування інформаційних технологій; несанкціоноване розповсюдження, використання і порушення цілісності, конфіденційності та доступності інформації [1].

В цих умовах постає проблема забезпечення інформаційної безпеки людини як найбільш вразливого суб’єкта суспільних відносин, зокрема конфіденційності особистих даних як права на невтручання в особисте життя.

Важливість проблеми захисту персональних даних зумовили її дослідження представниками різних юридичних наук – інформаційного права, адміністративного права, цивільного права, трудового права, кримінального права, міжнародного права.

Так, серед представників інформаційного права доцільно виокремити праці А.В. Туніка «Правові основи захисту персональних даних» [2], М.В. Різака «Правове регулювання відносин обігу персональних даних» [3], О.С. Дяковського «Правове забезпечення захисту персональних даних» [4]. Особливої уваги заслуговує дослідження О.С. Дяковського «Правове забезпечення захисту персональних даних», в якому з’ясовано структурні та змістовні особливості поняття персональних даних та здійснено їх класифікацію; встановлено коло суб’єктів захисту персональних даних та їх правовий статус; визначено процесуальні особливості обігу інформації, що містить персональні дані; встановлено особливості правового регулювання інформаційних баз даних, що

містять персональні дані; охарактеризовано міжнародний та зарубіжний досвід захисту персональних даних; розглянуто правові форми відповідальності за порушення законодавства про захист персональних даних [4, с.].

В межах адміністративно-правової науки варто виділити праці В.М. Брижка «Організаційно-правові питання захисту персональних даних» [5], Д.В. Цвірюка «Адміністративно-правовий захист персональних даних в Україні» [6], К.С. Мельника «Правові та організаційні засади захисту персональних даних в умовах євроінтеграції України» [7], М.В. Різака «Адміністративно-правове забезпечення відносин обігу та обробки персональних даних в Україні» [8], А.О. Щербини «Адміністративно-правове регулювання використання персональних даних суб'єктами владних повноважень в Україні» [9], Ю.С. Самойленко «Адміністративно-правове забезпечення захисту персональних даних в Україні» [10].

Серед наукових положень В.М. Брижка, на нашу думку, заслуговують значної уваги такі: правова регламентація захисту персональних даних має здійснюватися на основі міжнародного інформаційного законодавства шляхом ухвалення окремого закону, натомість конкретизація механізмів практичного регулювання має відбуватись у підзаконних нормативних документах [11, с. 192]; класифікація баз даних; визначення принципів захисту від неправомірного збирання, обробки, зберігання та поширення інформації; формулювання авторських дефініцій «персональні дані», «власник персональних даних», «володілець персональних даних тощо [12, с. 12].

Доречними вбачаються пропозиції В.М. Брижка практичного забезпечення захисту персональних даних на правовому та організаційному рівнях. Зокрема, фактично вперше до уваги широкої громадськості було запропоновано проєкт рамкового закону «Про захист персональних даних», яким пропонувалося гарантувати право власності на персональні дані, окреслити коло суб'єктів правовідносин у сфері захисту персональних даних, встановити загальні вимоги до операцій з даними, запровадити спеціальний режим доступу, передбачити юридичну відповідальність за порушення законодавства про захист персональних

даних, визначити підстави, форми та напрями міжнародного співробітництва в сфері їх захисту [13, с. 221–236]. Слід зазначити, що ідея ухвалення окремого спеціалізованого закону вирізнялась істотною новизною. І подальший розвиток подій засвідчив її обґрунтованість. Через деякий час (2010 рік) вона втілилась у Законі України «Про захист персональних даних», структура та зміст якого мають багато спільного з проєктом В.М. Брижка [12, с. 12].

Значний практичний інтерес становить авторське бачення системи адміністрування сферою персональних даних. У дисертаційному дослідженні В.М. Брижко обґрунтував доцільність створення незалежного від держави органу, який би провадив дозвільну діяльність у сфері обробки персональних даних, забезпечував реєстрацію відповідних інформаційних баз, розглядав звернення фізичних і юридичних осіб з питань захисту персональних даних в адміністративно-правовому порядку, репрезентував країну на міжнародному рівні, зокрема в Консультативному комітеті Ради Європи та інших міжнародних організаціях з питань захисту персональних даних. Глибина опрацювання цієї пропозиції справляє чимале враження. Поряд з детальним описом функцій і повноважень органу захисту персональних даних автор змоделював його організаційну структуру, здійснив точні розрахунки його матеріально-технічного забезпечення, виклав алгоритм реалізації основних напрямів його діяльності (дозвільної, реєстраційної, контрольної тощо), запропонував багаторівневу схему його нормативно-правового забезпечення [13, с. 237–250; 12, с. 13].

З цього приводу Т.О. Гуржій та А.Л. Петрицький слушно відмічають, що тепер, через десяток років, є всі підстави вважати, що своєчасне втілення цих новел істотно наблизило б Україну до міжнародних стандартів організації захисту персональних даних та сприяло б помітному прогресу у захисті права людини на конфіденційність приватного життя. Однак подібно до багатьох інших прогресивних наукових ідей, викладені пропозиції тривалий час залишалися незатребуваними. Фактично від доктринального оформлення цієї концепції до її практичного втілення минуло десять років. За цей період були марно витрачені значні ресурси, а головне – згаяно час на шляху до інтеграції в європейське

інформаційне суспільство, імплементації міжнародного законодавства та переходу на світові стандарти захисту приватного життя [12, с. 13].

Сутності та системі адміністративно-правового забезпечення відносин обігу та обробки персональних даних в Україні була присвячена робота М.В. Різака [8]. У ній доведено необхідність розподілу правовідносин щодо обігу персональних даних та правовідносин щодо їх обробки, що зумовлено різним змістом та наслідками цих процесів; визначено і запропоновано закріпити на законодавчому рівні такі поняття: «згода суб'єкта персональних даних на обіг його персональних даних» та «згода суб'єкта персональних даних на обробку його персональних даних»; доведено необхідність отримання письмової згоди на обіг та обробку вразливих персональних даних, яка може бути надана також через засоби ЕОМ, за умови правової прив'язки IMEI ЕОМ до ідентифікованої фізичної особи; запропоновано законодавчо унеможливити обробку вразливих персональних даних у загальнодоступних базах персональних даних шляхом доповнення статті 7 Закону України «Про захист персональних даних» частиною третьою такого змісту: «забороняється реєстрація та дія загальнодоступних баз персональних даних, в межах яких здійснюється автоматична обробка «вразливих» персональних даних».

А.О. Щербина охарактеризувала сутність та особливості адміністративно-правового регулювання використання персональних даних суб'єктами владних повноважень [9]. Зокрема, нею визначено ознаки, поняття та елементи адміністративно-правового режиму персональних даних; розкрито правовий статус суб'єктів владних повноважень як користувачів персональних даних; окреслено адміністративно-правові відносини у сфері використання персональних даних суб'єктами владних повноважень; з'ясовано зміст та елементи механізму адміністративно-правового регулювання використання персональних даних суб'єктами владних повноважень; систематизовано організаційно-правові засади використання персональних даних в органах виконавчої влади та в органах місцевого самоврядування; встановлено особливості правового регулювання використання персональних даних суб'єктами владних повноважень в окремих

сферах; окреслено основні засади державного контролю та нагляду за дотриманням законодавства про захист персональних даних суб'єктами владних повноважень; охарактеризовано адміністративну відповідальність за порушення правил використання персональних даних у роботі суб'єктів владних повноважень.

Ю.С. Самойленко досліджено адміністративно-правове забезпечення захисту персональних даних в Україні, в результаті чого запропоновано та обґрунтовано основні напрями нормативно-правового забезпечення захисту персональних даних в Україні шляхом виокремлення таких їх блоків: 1) визначити повноваження Уповноваженого Верховної Ради України з прав людини щодо направлення вимоги до власника вебсайту про видалення незаконно розміщеної інформації про персональні дані особи; 2) з метою обмеження незаконного поширення персональних даних клієнтів банківських установ та використання їх у злочинних схемах встановити законодавче обмеження щодо їх використання; 3) погодити норми Закону України «Про захист персональних даних» та Закону України «Про державну таємницю» стосовно однакового тлумачення понять «персональні дані», «державна таємниця», оскільки такі відомості можуть бути віднесені як до відкритої інформації, так і до конфіденційної та навіть таємної; 4) закріпити юрисдикційні повноваження Уповноваженого Верховної Ради України з прав людини щодо виявлення порушень прав і свобод людини та громадянина, за яке передбачена адміністративна відповідальність, складення протоколу та направлення матеріалів справи до суду, а також участі в розгляді таких справ та права оскарження рішення суду в Законі України «Про Уповноваженого Верховної Ради України з прав людини» [10, с. 5].

Також Ю.С. Самойленко систематизовано шляхи можливого впровадження зарубіжного досвіду правового регулювання та практики діяльності органів публічної адміністрації щодо реалізації механізмів захисту персональних даних у вітчизняну модель захисту персональних даних, зокрема стосовно таких питань: а) запровадження процедури ліцензування дій (робіт) із захисту персональних даних, що стосується лише утримувачів (адміністраторів) систематизованих баз

даних, наприклад автоматизованих баз даних медичних установ, науково-дослідних установ, реєстру виборців, поліцейських баз даних, баз фінансових і банківських установ; б) запровадження реєстру розпорядників персональних даних; в) запровадження сертифікації автоматизованих інформаційних систем, призначених для обробки персональних даних, що має на меті створення необхідного рівня захисту персональних даних; г) покладення на Міністерство цифрової трансформації України обов'язку здійснювати моніторинг інтернетресурсів щодо виявлення порушень законодавства про захист персональних даних та порушувати перед Уповноваженим Верховної Ради України з прав людини питання про застосування відповідних заходів впливу на порушників [10, с. 5].

Серед праць представників науки цивільного права доцільно виділити такі: О.А. Дмитренко «Право фізичної особи на власні персональні дані в цивільному праві України» [14], С.В. Ясечко Цивільно-правова відповідальність за порушення права на інформацію [15], І.І. Романюк «Охорона права на персональні дані в Україні (цивільно-правовий аспект)» [16], Ю.Д. Бєлова «Цивільні правовідносини щодо персональних даних» [17].

Визначальною рисою наукового підходу С.В. Ясечко став акцент на питаннях юридичної відповідальності за порушення права на інформацію та захист персональних даних. На відміну від більшості цивілістів, які ототожнюють право на володіння інформацією із правом на її захист, С.В. Ясечко провела між ними чітку межу: «Право на захист інформації має інші підстави виникнення, зміст і форми, ніж право власності: воно виникає внаслідок загрози порушення або ж фактичного порушення суб'єктивних прав на інформацію, має загальний характер, здебільшого не може бути здійснене поза юрисдикційною формою і охоплює певні процесуальні дії. Тож право на захист інформації слід розглядати окремо» [15, с. 193]. На цій підставі зроблено висновок про принципову відмінність порушень інформаційного законодавства (зокрема пов'язаних з поширенням конфіденційної інформації) та порушень інформаційних зобов'язань, що зумовлює необхідність законодавчого розмежування їх юридичних складів, а

також встановлення різних санкцій за їх учинення. С.В. Ясечко особливу увагу приділено компенсаторним механізмам цивільної відповідальності (компенсації моральної шкоди, заподіяної внаслідок незаконного поширення конфіденційної інформації), а також підставам для звільнення від цивільної відповідальності за інформаційні делікти. Вона довела, що через специфіку цього виду правопорушень звільнення від відповідальності за їх учинення може відбуватися за наявності обмеженого кола підстав, як-то: дія непереборної сили, відсутність вини, крайня необхідність і заподіяння шкоди правомірними діями. У зв'язку з цим істотний теоретичний інтерес становить авторська теза про розмежування категорій «підстави для звільнення від відповідальності» та «підстави, які виключають притягнення до відповідальності». Така постановка питання видається цілком слушною, оскільки звільнення від відповідальності за порушення законодавства про захист персональних даних може мати місце тільки там, де є підстави для такої відповідальності. В іншому разі має йтися про підстави, котрі виключають відповідальність [12, с. 20-21].

З'ясовуючи сутність цивільно-правової охорони права на персональні дані І.І. Романюк охарактеризувала «право особи на власні персональні дані» як особистого немайнового інформаційного права фізичної особи, що становить комплексне утворення у системі особистих немайнових прав фізичної особи; здійснила поділ персональних даних фізичної особи за режимом доступу на відкриті (загальнодоступні) та з обмеженим доступом (конфіденційні та таємні); обґрунтувала, що персональні дані фізичної особи, як інформація про особу, наділені усіма необхідними ознаками для здатності їх виступати об'єктом цивільного обороту; аргументувала, що відносини щодо надання фізичною особою згоди на використання своїх персональних даних третім особам можуть носити і майновий характер, у зв'язку з чим зробила висновок про те, що суб'єктивне цивільне право особи на персональні дані є особистим немайновим інформаційним правом фізичної особи, реалізація якого може відбуватися і в майновій сфері [16].

Досліджуючи особливості цивільних правовідносин стосовно персональних даних Ю.Д. Бєлова поділила цивільні правовідносини щодо персональних даних за їх правовою природою на такі види: 1) абсолютні відносини між суб'єктом персональних даних (управомочена особа) та усіма іншими особами (зобов'язані не порушувати права суб'єкта персональних даних) щодо охорони персональних даних; 2) абсолютні відносини між володільцем, розпорядником персональних даних та третіми особами в розумінні Закону України «Про захист персональних даних» (управомочені особи) та усіма іншими, крім суб'єкта персональних даних (зобов'язані особи) щодо забезпечення захисту персональних даних; 3) відносні відносини між суб'єктом персональних даних з одного боку, і володільцем, розпорядником персональних даних та третіми особами – з іншого боку, котрі виникають з приводу обробки персональних даних; 4) відносні відносини володільця, розпорядника персональних даних та третіх осіб між собою, які виникають з приводу обробки персональних даних. Також нею обґрунтовано доцільність наділення суб'єкта персональних даних правом на забуття [17, с. 25-26].

Захист персональних даних працівників в контексті трудового права був предметом наукових розвідок А.М. Чернобай [18], Д.С. Гети [19], А.В. Авраменко [20].

Так, А.М. Чернобай визначено поняття та нормативний зміст персональних даних працівника, здійснено їх класифікацію; сформульовано поняття та загальні вимоги до обробки персональних даних працівника; встановлено вимоги до збирання, зберігання, використання та передачі персональних даних працівника; розкрито зміст прав працівника з метою забезпечення захисту персональних даних, які зберігаються у роботодавця; окреслено місце норм про захист персональних даних працівника у системі трудового права України; розглянуто питання юридичної відповідальності за порушення норм, які регулюють обробку та захист персональних даних працівника [18]. У свою чергу А.В. Авраменко сформульовано дефініцію поняття «обіг персональних даних працівника»; запропоновано систематизацію завдань обігу персональних даних працівника на

стадії укладення трудового договору, на стадії його виконання (основній стадії) та на стадії після звільнення працівника [20].

Серед представників науки кримінального права необхідно відмітити праці Ю.І. Дем'яненко «Кримінальна відповідальність за порушення недоторканості приватного життя» [21], І.Б. Король «Охорона недоторканості приватного життя: кримінально-правові та кримінологічні аспекти» [22], О.Б. Сосніної «Кримінальна відповідальність за порушення недоторканості приватного життя (ст. 182 КК України)» [23], В.К. Матвійчук, В.В. Матвійчук «Кримінально-правова характеристика діяння порушення недоторканності приватного життя (ст. 182 КК України)» [24].

Предметом дослідження представників міжнародного права були такі праці: А.В. Пазюк «Міжнародно-правовий захист права людини на приватність персоніфікованої інформації» [25], О.О. Шевчук «Правове регулювання охорони персональних даних в Європейському Союзі» [26], Ю.О. Коваленко «Захист персональних даних у практиці Європейського суду з прав людини та Суду Європейського Союзу: порівняльний аналіз» [27].

Систематизувавши ознаки національних систем захисту персональних даних у провідних країнах, А.В. Пазюк виділив три світові моделі забезпечення конфіденційності персоніфікованої інформації: соціальну (більшість європейських країн), ліберальну (США), змішану (Канада, Австралія). Для соціальної моделі властиве поширення правил правового захисту персоніфікованих даних, а також наглядових повноважень не тільки на публічні, а й однаковою мірою на приватноправові відносини. В основу ліберальної моделі покладено принцип невтручання держави у відносини між приватними особами, що зумовлює її суто публічну спрямованість. Змішана модель хоч і спирається на засоби приватного та публічного права, ключову роль у забезпеченні захисту персональних даних відводить саме останнім [11, с. 193; 12, с. 17-18].

А.В. Пазюк обґрунтував необхідність взяття за зразок європейської (соціальної) моделі захисту персональних даних, пріоритетом якої є повага до прав людини, а не ринкові чинники. У цьому контексті на особливу увагу

заслуговують його висновки щодо систематизації та правового закріплення загальноєвропейських принципів захисту персональних даних, імплементації ключових актів інформаційного законодавства Європейського Союзу (далі – ЄС) в національне законодавство України, посилення контролю за виконанням міжнародних зобов'язань України у сфері захисту персональних даних, розширення правової бази регулювання кореспондуючих суспільних відносин, всебічне задіяння в механізмі захисту інформаційних прав громадян (зокрема права на захист персональних даних) інституту омбудсмена та інші [11, с. 193-194; 12, с. 18].

Проблематиці комплексного аналізу системи захисту персональних даних у ЄС та Україні присвячено роботу О.О. Шевчука [26], у якій було проаналізовано історію становлення та розвитку інституту захисту персональних даних у ЄС та Україні; обґрунтовано доцільність реформування існуючої системи захисту персональних даних у ЄС; розглянуто концептуальні засади дослідження особливостей захисту персональних даних у контексті розвитку простору свободи, безпеки та юстиції; систематизовано існуючі підходи до вивчення механізмів захисту персональних даних у ЄС та Україні; з'ясовано критерії транскордонної передачі персональних даних у ЄС; розкрито основні проблеми та прогалини в системі захисту персональних даних в Україні; окреслено варіанти удосконалення системи захисту персональних даних в Україні.

Дослідження теоретичних та практичних проблем, пов'язаних із захистом персональних даних у Раді Європи (далі – РЄ) та ЄС, систематизації застосовуваних у цій сфері підходів і принципів, а також оцінки їх впливу на формування стандартів захисту персональних даних, стало предметом наукової розвідки Ю.О. Коваленко [27], у якій було проаналізовано становлення та розвиток права на захист персональних даних у доктрині та практиці міжнародного права, а також концептуальні підходи до права на захист персональних даних у сучасному міжнародному праві; розглянуто понятійно-категоріальний апарат, зокрема такі ключові поняття, як «персональні дані», «чутливі дані», «обробка даних», «псевдонімізація», «знеособлення», «контролер

даних», «оператор даних», «треті особи» та основні принципи захисту персональних даних; розкрито правові засади регулювання захисту персональних даних у РЄ та підходи Європейського суду з прав людини (далі – ЄСПЛ) у цій сфері; з'ясовано механізми захисту персональних даних в ЄС у світлі практики Суду ЄС; охарактеризовано особливості захисту персональних даних та вплив практики ЄСПЛ та Суду ЄС на формування європейських стандартів захисту персональних даних; окреслено законодавчі гарантії захисту персональних даних та практику їх забезпечення з огляду на виконання Україною міжнародно-правових зобов'язань у цій сфері; визначено стан впровадження європейських стандартів захисту персональних даних у законодавство України та напрями його вдосконалення; охарактеризовано процес еволюції законодавства України у процесі його адаптації до acquis ЄС.

Якщо аналізувати наукові розробки, присвячені захисту персональних даних у сфері охорони здоров'я, то окремі питання містяться в лише наукових та публіцистичних публікаціях, а комплексних досліджень з цієї проблематики не проводилось.

Отже, поняття «персональні дані» підпадає під правовий вплив різних галузей права, тобто воно регулюється сукупністю правових норм різної галузевої належності, а саме нормами таких галузей права як конституційне, інформаційне, адміністративне, цивільне, трудове, кримінальне та міжнародне.

Сучасна тенденція до стрімкого підвищення обсягу даних, які циркулюють у інформаційному просторі, не оминула сферу охорони здоров'я, яка має високий рівень вразливості у зв'язку з чутливістю даних про стан здоров'я людини і громадянина [28, с. 496]. «Охорона здоров'я все більше покладається на інформаційні технології. Усе більше лікарень та закладів охорони здоров'я застосовують інформаційно-комунікаційні технології для підтримки та вдосконалення своєї роботи. Широко застосовуються цифрові технології в державному секторі охорони здоров'я – це й електронні рецепти, запис до сімейного лікаря, записи про надані послуги, госпіталізацію, виписку зі стаціонару та ін. У цьому контексті з'явився широкий спектр інструментів та

послуг у сфері електронного здоров'я. Електронні медичні записи створюються таким чином, щоб можна було передавати дані пацієнтів між різними медичними працівниками. Незважаючи на те, що цифрові технології в галузі охорони здоров'я мають таку велику кількість важливих функцій, їх висока залежність від конфіденційної інформації щодо здоров'я пацієнтів може спричинити проблеми із захистом інформації. При цьому значну частину персональних даних щодо здоров'я часто збирають без інформування про це пацієнтів. Вони не можуть контролювати свої дані та не мають достатнього рівня обізнаності, щоб дати вільну та поінформовану згоду. Розробка складних алгоритмів ще більше поглибила цю проблему, оскільки створює серйозні ризики для захисту персональних даних про здоров'я» [29].

Поряд з цим, слід враховувати, що впровадження новітніх технологій суттєво впливає на розвиток суспільства, в тому числі медичної сфери. За останні 20 років у медичній практиці почали активно застосовуватися телемедичні технології, значно зросла кількість малоінвазійних втручань, широкого застосування набули комп'ютери, ноутбуки, інформатизовано медико-правову документацію. Новітнє медичне обладнання дає змогу відстежити найдрібніші зміни в стані здоров'я пацієнтів у стаціонарних закладах охорони здоров'я у режимі теперішнього часу, залучати до складних хірургічних втручань провідних фахівців з усього світу, не зважаючи на відстані. Використання різного роду датчиків, браслетів та інших досягнень ІТ-сфери значно розширило можливості людини як у контролі за станом власного здоров'я, так і у відносинах з лікарем. Використання мобільних телефонів чи то для безпосереднього зв'язку з лікарем, чи для активації додатків, пов'язаних зі здоров'ям, також можна віднести до е-здоров'я. Відповідно, й правове регулювання, принаймні, частини цієї інформаційної сфери потребує унормування [30].

На нашу думку, інформатизація сфери охорони здоров'я сприяла покращенню її функціонуванню. Разом з тим, у процесі використання інформаційно-комунікаційних технологій у галузі охорони здоров'я виникли нові технічні та морально-етичні питання та проблеми. Тоді як перед законодавцем

постало питання розробки заходів, які здатні відмежувати особу та суспільство від небажаних і шкідливих наслідків впровадження інформатизації у галузь охорони здоров'я [28, с. 497].

Цифровізація та інформатизація охоплюють усе більший перелік відносин, які складаються у процесі надання медичних послуг. На сьогодні в медичній інфраструктурі впроваджуються телесистеми для дистанційного надання послуг, поширюється онлайн-діагностика, оператори медичних послуг стають учасниками цифрових платформ, медичний документообіг здійснюється в електронному форматі. Ці явища впливають на ефективність і якість медичної допомоги в Україні, виконуючи завдання з забезпечення нормальної взаємодії пацієнтів, медичних працівників і медичних установ за допомогою сучасних технологій. Занепокоєння щодо правового захисту електронних даних у цифрову епоху виникає на фоні гучних випадків втручання в дані користувачів. До основних негативних проявів інформатизації та цифровізації відносять навмисне вторгнення в державні та недержавні комп'ютерні мережі, неадекватну практику кібербезпеки та корпоративної конфіденційності, які розкривають особисту інформацію мільйонів користувачів небажаним отримувачам. Медична сфера діяльності є особливо чутливою до подібних ризиків, оскільки таємниця про стан здоров'я включає як інформацію про стан здоров'я пацієнта, так і факти чи обставини, які у процесі надання медичної допомоги стали відомі медичним працівникам. Приватність і конфіденційність у медицині враховує також культурні, соціальні та релігійні традиції. Таким чином, дані про стан здоров'я людини стали об'єктом інформаційних відносин, а отже виникає інтерес у забезпеченні належного захисту таких даних, інформаційній безпеці пацієнтів [28, с. 497].

В умовах цифрової трансформації сфери охорони здоров'я випадки несанкціонованого втручання в особисте життя осіб та неправомірного поширення і використання їх медичних даних набувають загрозливого та масштабного характеру.

На початку 2021 року у Франції стався витік даних майже півмільйона пацієнтів: їхні імена, адреси, номери телефонів, стан здоров'я, вагітність, проблеми з фертильністю, ВІЛ-позитивний статус. Інформація перебувала в групах месенджеру Telegram, де продавалася за допомогою зашифрованих повідомлень. У Сполучених Штатах витоки медичних даних відбуваються періодично. 2015 року зловмисники отримали доступ до серверу компанії Medical Informatics Engineering, яка створює програмне забезпечення для онлайн-записів у сфері охорони здоров'я. Постраждали близько 3,9 млн людей, чиї персональні дані стали доступними, зокрема й діагнози. У 2019 році компанія погодилася сплатити $100 тисяч штрафу за порушення HIPAA. Йдеться про недостатній аналіз ризиків для конфіденційності з боку Medical Informatics Engineering. На думку спеціаліста у сфері ІТ Пола Робертса, підвищений "попит" на незаконний доступ до медичної інформації у США з'явився після впровадження програми Obamacare, яка передбачає перенесення масиву паперових даних в електронний формат. Причинами можуть бути як незахищене передавання даних між медичними установами, так і їх незахищене зберігання [31].

В Україні серед відомих випадків був витік даних пацієнтів однієї з найбільших клінік Дніпра, причиною якого були помилки в системах самого закладу. Так, Національний координаційний центр кібербезпеки при Раді національної безпеки і оборони України під час моніторингу кіберпростору виявив витік інформації з однієї із найбільших приватних клінік міста Дніпро. Серед інформації, що опинилася у відкритому доступі, - персональні дані працівників та клієнтів цієї клініки, зокрема ПІБ, дати народження, адреси проживання, телефон, e-mail, діагнози, дані медичної картки (що становить медичну таємницю), включаючи результати аналізів, діагнози, інформація про захворювання, результати проведення ПЛР-тестів, списки хворих на COVID-19. Аналіз інформації витоку показав, що до вільного доступу потрапили десятки тисяч записів про пацієнтів. За результатами дослідження було встановлено, що витік стався внаслідок помилок конфігурації в інформаційних системах та базах даних медичного закладу, які мали доступ до мережі Інтернет. Слід зазначити, що

вільний доступ до баз даних надавав можливість не тільки викрадення персональної інформації, але й несанкціонованого внесення змін, включно з модифікацією призначень ліків, результатів аналізів та обстежень, редагування записів в протоколі «Надання медичної допомоги для лікування коронавірусної хвороби (COVID-19)». З моменту виявлення витоку клініка пасивно реагувала на повідомлення фахівців Національного координаційного центру кібербезпеки при Раді національної безпеки і оборони України щодо витоку та вразливостей і не докладала зусиль до їх усунення. Дані щодо клієнтів приватної клініки досить довго перебували у вільному доступі [32].

У цьому контексті згадаємо новину в медіа про те, що під час повномасштабного вторгнення компанія «Київстар» викупила 69,99 % акцій «Хелсі Україна». «HELSI» – масштабний приватний медтек-стартап, запущений у 2016 році, ключовий гравець на ринку медичних інформаційних систем, що працюють з державними та приватними лікарнями. Цей стартап має амбітні цілі – задовольнити всі потреби людини в її здоров'ї. Якісна, сучасна взаємодія лікарів і пацієнтів дозволить більше робити акцент на профілактику, ніж лікування серйозних хвороб. Сервіс справді якоюсь мірою полегшив доступ до державної медицини. Через нього можна знайти будь-якого лікаря та записатися на прийом, отримати електронне направлення тощо. Усі ці дані автоматично підтягуються в особистий кабінет користувача із центральної бази Єдиної системи електронного здоров'я [33, с. 41].

На травень 2023 року на платформі було зареєстровано понад 25 млн користувачів. До системи підключено медичні заклади по всій країні та приблизно 50 тисяч медпрацівників. Для багатьох українців стало несподіванкою те, що ця інформаційна система приватна, а не державна, і саме приватні структури отримують доступ до стану здоров'я українців. У серпні 2022 року «HELSI» поглинув найбільший в Україні мобільний оператор «Київстар», який належить «Альфа Груп». Медичний стартап «HELSI» став частиною медичної інфраструктури в Україні. У громадськості почали з'являтися питання: хто побудував цей ІТсервіс, просуває його на державному рівні та навіщо він компанії

«Київстар» під час війни? Особливе занепокоєння викликав той факт, що серед співвласників компанії «Київстар» є підприємці, які після початку повномасштабного вторгнення потрапили в санкційні списки Великої Британії. «Київстар» і «HELSI» давно співпрацюють. Наприклад, оператор допомагав абонентам вакцинуватися, розсилаючи таргетовані SMS. Раніше на це особливо ніхто не звертав уваги, тільки зараз постало питання: як обробляються персональні дані мільйонів українців, хто здійснює контроль і має до них доступ? [33, с. 42].

На додаток до цього, у травні 2023 року в мережі спалахнув скандал навколо фейкових записів у Helsi-кабінетах. Українці в соціальних мережах ділилися історіями, що хтось без їхнього відома записував їх на консультації до лікарів, отримував направлення, діагнози тощо. Кількість акаунтів з фейковими записами у «HELSI» не уточнювали. Проблема могла існувати роками. Чому про неї стало відомо лише зараз? Більшість українців не часто заходить до особистого кабінету «HELSI», але публікації в соцмережах спричинили ефект лавини, і багато людей почали перевіряти свої облікові записи та виявляти, що хтось незаконно використовує їхні чутливі персональні дані [33, с. 42].

Володіючи інформацією про здоров’я людей, з’являється можливість збільшити прибутки у фармацевтиці, рекламному бізнесі, сфері медичних послуг. Можна тиснути на конкретних осіб, погрожувати розкриттям сенситивних даних тощо. Тому така інформація є цінною для кіберзлочинців [29]. При цьому, слід зазначити, що обробка персональних даних, які зберігаються в медичних інформаційних системах, має велике значення не тільки для захисту приватності конкретної особи, а й національної безпеки загалом [33, с. 43].

Отже, інформатизація та цифровізація сфери охорони здоров’я зумовила виникнення проблеми безпеки персональної інформації пацієнтів. У зв’язку з цим питання захисту персональних даних у сфері охорони здоров’я набуло особливого значення.

З’ясовуючи сутність персональних даних як об’єкта правового регулювання у сфері охорони здоров’я необхідно відмітити, що охорона здоров’я є

загальносоціальною цінністю, забезпечення якої вимагає від держави застосування різноманітних засобів правового регулювання. В той же час, охорона здоров'я є складною сферою суспільного життя, яка з метою поліпшення здоров'я населення вимагає від законодавця забезпечити в сфері охорони здоров'я реалізацію публічного та приватного інтересу [34, с. 244].

Охорона здоров'я є ключовим елементом національної безпеки держави [35, с. 453]. Відповідно до ст. 12 Закону України «Основи законодавства України про охорону здоров'я» охорона здоров'я є одним з пріоритетних напрямів державної діяльності. Держава формує політику охорони здоров'я в Україні та забезпечує її реалізацію [36].

У літературі поняття «охорона здоров'я» визначають як систему засобів, що спрямовані на збереження, зміцнення, розвиток та, у випадку порушення, відновлення максимально досяжного рівня фізичного й психічного стану людського організму, які зобов'язані здійснювати органи державної влади й органи місцевого самоврядування, громадські організації, а також людина та населення як в інтересах кожної фізичної особи, так і суспільства в цілому [37, с. 2]; як систему заходів, спрямованих на збереження, зміцнення, розвиток та, у разі порушення, відновлення максимально досяжного рівня фізичного і психічного стану людського організму, яких зобов'язані вживати органи державної влади й органи місцевого самоврядування, підприємства, установи й організації, а також людина і населення в інтересах як кожної фізичної особи, так і всього суспільства [38, с. 26; 39, с. 22]; систему засобів, котрі людина має та використовує для збереження, розвитку та, у випадку порушення, відновлення максимально досяжного рівня фізичного, психічного та душевного стану її організму [40, с. 39].

Закон України «Основи законодавства України про охорону здоров'я» під охороною здоров'я розуміє систему заходів, спрямованих на збереження та відновлення фізіологічних і психологічних функцій, оптимальної працездатності та соціальної активності людини при максимальній біологічно можливій індивідуальній тривалості її життя. Такі заходи здійснюють органи державної

влади та органи місцевого самоврядування, їх посадові особи, заклади охорони здоров'я; фізичні особи - підприємці, які зареєстровані у встановленому законом порядку та одержали ліцензію на право провадження господарської діяльності з медичної практики; медичні та фармацевтичні працівники, фахівці з реабілітації, громадські об'єднання і громадяни [36].

Сфера охорони здоров'я характеризується комплексним характером, який зумовлений наявністю приватних і публічних правовідносин, що становлять предмет цього правового утворення, уможливлює поширення на ці відносини норм фундаментальних (базових) галузей права, які регулюють однорідні відносини (сфери цивільного, адміністративного, фінансового, кримінального, процесуального права) [41, с. 64]. Це означає, що до сфери охорони здоров'я входять правові норми різної галузевої приналежності: конституційного, адміністративного, фінансового, цивільного, трудового, кримінального права [42, с. 128; 43, с. 65].

Особливостями законодавства про охорону здоров'я є широкий спектр суспільних відносин, які регулюють його норми, а також їх величезна кількість та ієрархія [44, с. 139-140]. Законодавство про охорону здоров'я − це частина законодавства України, яка складається з системи правових актів і норм, що за допомогою специфічних правових методів регулюють суспільні відносини (організаційно-управлінські, майнові, трудові та ін.) у сфері охорони здоров'я [44, с. 23].

Систему законодавства у сфері охорони здоров'я становлять п'ять груп (рівнів) нормативно-правових актів: 1) Конституція України (а саме ст. 49, якою гарантується право на охорону здоров'я, медичну допомогу і медичне страхування); 2) галузеві кодекси, які містять загальні норми, що застосовуються в медичній сфері (Цивільний і Кримінальний кодекси, Кодекс про адміністративні правопорушення, Кодекс законів про працю, процесуальні кодекси тощо); 3) основи законодавства України про охорону здоров'я як основний (базовий) закон у сфері охорони здоров'я; 4) спеціальні закони, що регулюють окремі сфери медичної діяльності (донорство, психічна допомога, окремі інфекційні

захворювання тощо); 5) акти центральних і місцевих органів державної виконавчої влади (укази та розпорядження президента України, постанови і розпорядження Кабінету Міністрів України, накази і розпорядження Міністерства охорони здоров'я України, нормативно-правові акти інших органів влади) [41, с. 64]. Практично кожен предмет чи явище, а також правовий акт, що регулює ті чи інші суспільні відносини, має відношення до здоров'я людини. У складі цієї галузі законодавства є норми багатьох галузей права. Тому є підстави вважати законодавство про охорону здоров'я комплексною галуззю законодавства [44, с. 31-33].

Здійснюючи заходи щодо збереження та відновлення фізіологічних і психологічних функцій, оптимальної працездатності та соціальної активності людини при максимальній біологічно можливій індивідуальній тривалості її життя, потрібно також забезпечити належний рівень захисту персональних даних особи. Законодавство України про охорону здоров'я та захист персональних даних не визначає в повному обсязі сутність персональних даних та конкретні відомості, які відносяться до персональних даних [45, с. 184].

У законодавстві України про захист персональних даних персональні дані визначено як відомості чи сукупність відомостей про фізичну особу, яка ідентифікована або може бути конкретно ідентифікована [46]. Визначення персональних даних структурно охоплює чотири ознаки: 1) відомості чи сукупність відомостей; 2) стосуються фізичної особи («про фізичну особу»); 3) їх суб'єктом є фізична особа; 4) фізична особа є ідентифікована або може бути конкретно ідентифікована [17, с. 43].

Виходячи із законодавчого закріплення терміну «персональні дані» Ю.Д. Бєлова зазначає, що правова природа персональних даних полягає у наступному: персональні дані належать до нематеріальних благ як об'єктів цивільних відносин (не мають матеріальної (фізичної) субстанції, не мають геометричних форм, розмірів, кольору); персональні дані є різновидом інформації (інформаційний продукт, ресурс, документ, тобто об'єкт, що може бути інформаційним товаром і предметом будь-яких правочинів, з урахуванням

особливостей і специфіки його як об’єкту особливого роду); персональні дані належать до особистих немайнових благ (ст. 11 Закону України «Про інформацію» прирівнює їх до «інформації про фізичну особу», ст. 8 Закону України «Про захист персональних даних» кваліфікує права суб’єкта персональних даних як особисті немайнові права, однією з ознак яких є їх специфічний об’єкт, тобто те, на що спрямоване дане право. Таким об’єктом є особисте немайнове благо) [17, с. 31-33].

Водночас у літературі цілком слушно законодавче визначення персональних даних підлягає критиці, оскільки воно не є вичерпним і не дає чітких критеріїв того, які саме дані про фізичну особу можна вважати персональними [47, с. 220]. При цьому персональні дані можуть використовуватися без згоди суб’єкта персональних даних, що характерно, насамперед, для сфери охорони здоров’я, де здійснюється використання персональних даних хворого, зокрема даних про історію хвороби чи інших даних [48, с. 54].

У юридичній літературі дефініція «персональні дані» трактується як: сукупність документованих або публічно оголошених відомостей про фізичну особу [49, с. 176]; дані про живу людину, котра ідентифікована або може бути ідентифікована на основі цих даних чи на основі додаткової інформації, що може потрапити до особи, яка контролює дані, що містять вираження становлення до цієї людини й указівку на певну мету або плани стосовно цієї людини з боку особи, яка контролює дані, або іншої особи [50, с. 103]; відомості чи сукупність відомостей про живу фізичну особу, яка ідентифікована або може бути конкретно ідентифікована з урахуванням встановленого законом поділу персональних даних та поняття «обіг персональних даних» [4, с. 4]; відомості чи їх сукупність, що характеризує соціальний, майновий, політичний, релігійний статус фізичної особи, за якими вона ідентифікується іншими суб’єктами, у тому числі суб’єктами владних повноважень в процесі реалізації їх компетенції, і незаконне використання яких може завдати фізичну, моральну чи матеріальну шкоду суб’єкту персональних даних [51, с. 48]; виражена в об’єктивній (матеріальній) формі охоронювана законом інформація або масив інформації, за допомогою якої

можна чітко ідентифікувати конкретну особу стосовно якої вчинені протиправні дії, тобто дії, на які суб'єкт персональних даних не давав дозволу та які заборонені законом [52, с. 58]; як будь-яка інформація, яка ідентифікує та індивідуалізує особу як учасника суспільних відносин [16, с. 10].

У сфері трудових відносин персональні дані працівника характеризуються як: будь-яка інформація, яка стосується конкретного працівника та необхідна роботодавцю у зв'язку із використанням праці цього працівника на підставі трудового договору [18, с. 16-17]; система відомостей про особу, з якою укладається трудовий договір, що формується, накопичується, зберігається, використовується тощо роботодавцем у порядку, визначеному законодавством, з метою ідентифікації особи працівника, прийняття рішень, пов'язаних з виконанням його трудової функції, зміною або розірванням трудового договору [20, с. 183].

Ю.Д. Бєлова під персональними даними розуміє відомості або сукупність відомостей, котрі безпосередньо чи опосередковано стосуються фізичної особи, незалежно від її громадянства, постійного місця проживання чи іншого правового зв'язку з державою, що є їх носієм, та дозволяють «прямо» або «опосередковано» її ідентифікувати за умови, що такі відомості було оброблено шляхом збирання, реєстрації, накопичення, зберігання, адаптування, зміни, поновлення, використання, поширення знеособлення, знищення, у тому числі – із використанням інформаційних (автоматизованих) систем. На її думку таке визначення персональних даних структурно охоплює п'ять ознак: 1) відомості чи сукупність відомостей (включає будь-яку інформацію про особу); 2) стосуються безпосередньо чи опосередковано фізичної особи («про фізичну особу»); 3) їх суб'єктом є фізична особа незалежно від її громадянства, постійного місця проживання чи іншого правового зв'язку з державою; 4) фізична особа є ідентифікована (в групі осіб вона «виділяється» з-поміж інших членів групи або може бути конкретно ідентифікована, виходячи із обставин кожного окремого випадку (в групі осіб вона «виділяється» з-поміж інших членів групи); 5) відомості про особу набувають правового режиму персональних даних із

початком обробки персональних даних, тобто, будь-якої дії або сукупності дій, таких як збирання, реєстрація, накопичення, зберігання, адаптування, зміна, поновлення, використання і поширення (розповсюдження, реалізація, передача), знеособлення, знищення персональних даних, у тому числі з використанням інформаційних (автоматизованих) систем [17, с. 52-53].

Науковцями пропонуються різні підходи до класифікації персональних даних залежно від тих чи інших підстав. Так, К.С. Мельник залежно від режиму конфіденційності персональних даних, який встановлює сам суб'єкт персональних даних шляхом вчинення певних правочинів у письмовій або усній формі, у формі конклюдентних дій, виокремлює загальнодоступні персональні дані, конфіденційні персональні дані та спеціальні персональні дані, статус, вимоги до обробки та захисту яких визначаються національним законодавством на основі вимог міжнародного права [7, с. 16].

У свою чергу О.С. Дяковський класифікує персональні дані за такими критеріями як вид, наявність біологічних ознак, правовий режим доступу до інформації, нормативне закріплення, національні ознаки під час здійснення обігу персональних даних в суспільстві та державі. За критерієм виду персональні дані поділяються на загальні та вразливі. В залежності від біологічних ознак вразливі персональні дані виокремлюються на ідентифікуючі персональні дані, що містять генетичну інформацію, біометричну інформацію, антропологічну інформацію. Персональні дані, що містять генетичну інформацію поділяються на вроджені та набуті. За критерієм правового режиму доступу до інформації персональні дані поділяються на ті, які місять конфіденційну інформацію, таємну інформацію та службову інформацію. За критерієм нормативного поділу персональні дані поділяються на конституційні, цивільні, інформаційні дані, що ідентифікують особу. В залежності від національних ознак персональні є такими, що притаманні громадянам, іноземцям, особам без громадянства, біженцям, мігрантам [4, с. 10-11].

З приводу законодавчого розуміння дефініції «персональні дані» М.В. Різак зауважує, що зміст, який вкладається законом в поняття «персональні дані», є

дуже широким, що підтверджується відкритістю переліку відомостей, віднесених до числа персональних даних. Зважаючи на саму природу персональних даних, повністю їх перерахувати досить складно, це обумовило необхідність формування таких нормативних приписів, згідно з якими суб'єкт має право частково самостійно формувати свій «інформаційний портрет», вирішуючи, які з характеристик, що його ідентифікують, слід віднести до числа персональних даних, а які – ні. У зв'язку з цим ним запропоновано в Законі України «Про захист персональних даних» класифікувати персональні дані на такі: 1) загальні персональні дані (прізвище, ім'я та по батькові, дата народження, інші персональні дані, які за згодою суб'єкта цих даних розміщені в загальнодоступних базах персональних даних та які на момент їх обігу та/або обробки не були вилучені або знищені з цих баз); 2) вразливі персональні дані (відомості про расове або етнічне походження, політичні, релігійні або світоглядні переконання, членство в політичних партіях та професійних спілках, звинувачення у скоєнні злочину або засудження до кримінального покарання, а також даних, що стосуються здоров'я чи статевого життя); 3) спеціальні персональні дані (персональні дані, які не входять до вразливих чи загальних персональних даних, межі обігу яких визначаються суб'єктом цих даних) [8, с. 25].

А.О. Щербина доповнює класифікацію персональних даних ще такими критеріями як: 1) за режимом доступу: відкриті, конфіденційні, таємні; 2) за «правовим режимом» – відомості, до яких застосовуються загальні правила використання (більшість персональних даних) або особливі персональні дані, обробка яких становить особливий ризик для прав і свобод суб'єктів персональних даних: відомості про расове, етнічне та національне походження; світоглядні переконання особи; стан здоров'я особи; статеве життя; біометричні дані; генетичні дані; вчинення щодо особи тих чи інших видів насильства; місцеперебування та або шляхи пересування особи; факт притягнення до адміністративної чи кримінальної відповідальності, застосування щодо особи заходів в рамках досудового розслідування та заходів, передбачених Законом

України «Про оперативно-розшукову діяльність», вчинення щодо особи тих чи інших видів насильства [51, с. 47].

Ю.Д. Бєлова звертає увагу на те, що насамперед, слід розрізняти загальні та особливі (так звані чутливі чи вразливі) персональні дані. До останніх належать дані про расове або етнічне походження, політичні, релігійні або світоглядні переконання, членство в політичних партіях та професійних спілках, засудження до кримінального покарання, а також даних, що стосуються здоров'я, статевого життя, біометричних або генетичних даних. Цей перелік встановлюється в законі (ч. 1 ст. 7 Закону України «Про захист персональних даних»), є вичерпним та не підлягає розширеному тлумаченню. Значення виокремлення чутливих персональних даних полягає в тому, що законодавство встановлює особливі вимоги до обробки таких даних [17, с. 49].

Перелік підстав класифікації персональних даних може бути продовжений, але враховуючи тематику нашого дослідження персональні дані у сфері охорони здоров'я доцільно віднести до особливих, так званих чутливих чи вразливих, персональних даних, оскільки саме до них відносяться дані про здоров'я.

У ст. 4 Загального регламенту про захист персональних даних в країнах ЄС (General Data Protection Regulation (GDPR) персональні дані визначено як будь-яку інформацію, що стосується фізичної особи, яку ідентифіковано чи можна ідентифікувати («суб'єкт даних»); 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 [53].

В цій же статті цього ж Регламенту наведено поняття «дані стосовно стану здоров'я» - персональні дані, що стосуються стану фізичного чи психічного здоров'я фізичної особи, в тому числі надання медичних послуг, що відображають інформацію про її стан здоров'я [53].

У Загальному регламенті про захист персональних даних в країнах ЄС зазначено також, що персональні дані стосовно стану здоров'я повинні містити всі дані, що пов'язані зі станом здоров'я суб'єкта даних та розкривають інформацію про минулий, поточний або майбутній стан фізичного або психічного здоров'я суб'єкта даних. Це включає інформацію про фізичну особу, зібрану під час реєстрації на надання послуг, або надання послуг, у сфері охорони здоров'я; номер, символьний знак або опис, що приписують фізичній особі для того, щоб однозначно ідентифікувати фізичну особу для цілей охорони здоров'я; інформацію, отриману внаслідок дослідження або огляду частини тіла чи речовини, що міститься в тілі, у тому числі з генетичних даних або біологічних проб; а також будь-яку інформацію, наприклад, про захворювання, недієздатність, ризик захворювання, історію хвороби, клінічне лікування або фізіологічний чи біомедичний стан здоров'я суб'єкта даних, незалежно від джерела її надходження, наприклад, від лікаря або іншого медичного працівника, від лікарні, медичного обладнання або тестів лабораторної діагностики [53].

У Роз'ясненні основних положень Порядку повідомлення Уповноваженого щодо визначення обробки персональних даних, яка становить особливий ризик для прав і свобод суб'єктів персональних даних від 8 січня 2014 року стан здоров'я особи трактується як медична інформація про особу, що містить не лише свідчення про стан здоров'я, а й про історію її хвороби, про запропоновані дослідження і лікувальні заходи, прогноз можливого розвитку захворювання, в тому числі і про наявність ризику для життя і здоров'я (виняток становлять медичні довідки, листи працездатності і т. д., які обробляються володільцем при реалізації трудових відносин) [54].

Згідно ст. 3 Закону України «Основи законодавства України про охорону здоров'я» медична інформація – це інформація про медичне обслуговування особи або його результати, викладена в уніфікованій формі відповідно до вимог, встановлених законодавством, у тому числі інформація про стан здоров'я, діагнози та будь-які документи, що стосуються здоров'я та обмеження повсякденного функціонування/ життєдіяльності людини [36].

Відповідно до ст. 32 Конституції 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 [55].

Згідно ч. 2 ст. 21 Закону України «Про інформацію» конфіденційною є інформація про фізичну особу, інформація, доступ до якої обмежено фізичною або юридичною особою, крім суб'єктів владних повноважень, а також інформація, визнана такою на підставі закону. Конфіденційна інформація може поширюватися за бажанням (згодою) відповідної особи у визначеному нею порядку відповідно до передбачених нею умов, якщо інше не встановлено законом [56]. У ч. 2 ст. 11 Закону України «Про інформацію» встановлено, що 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 [56].

У Рішенні Конституційного Суду України у справі щодо офіційного тлумачення статей 3, 23, 31, 47, 48 Закону України «Про інформацію» та статті 12 Закону України «Про прокуратуру» (справа К.Г. Устименка) від 30 жовтня 1997 року № 5-зп зазначено, що частину четверту статті 23 Закону України «Про інформацію» треба розуміти так, що забороняється не лише збирання, а й зберігання, використання та поширення конфіденційної інформації про особу без її попередньої згоди, крім випадків, визначених законом, і лише в інтересах національної безпеки, економічного добробуту, прав та свобод людини. До конфіденційної інформації, зокрема, належать свідчення про особу (освіта, сімейний стан, релігійність, стан здоров'я, дата і місце народження, майновий стан та інші персональні дані). Медична інформація, тобто свідчення про стан здоров'я людини, історію її хвороби, про мету запропонованих досліджень і лікувальних заходів, прогноз можливого розвитку захворювання, в тому числі і про наявність ризику для життя і здоров'я, за своїм правовим режимом належить до конфіденційної, тобто інформації з обмеженим доступом [57].

Відповідно до Рішення Конституційного Суду України у справі у справі за конституційним поданням Жашківської районної ради Черкаської області щодо офіційного тлумачення положень частин 1, 2 ст. 32, частин 2, 3 ст. 34 Конституції України від 20 січня 2012 року № 1-9/2012 встановлено, що персональні дані – це будь-які відомості чи сукупність відомостей про фізичну особу, яка ідентифікована або може бути конкретно ідентифікована, а саме: національність, освіта, сімейний стан, релігійні переконання, стан здоров'я, матеріальний стан, адреса, дата і місце народження, місце проживання та перебування тощо, дані про особисті майнові та немайнові відносини цієї особи з іншими особами, зокрема, із членами сім'ї, а також відомості про події та явища, що відбувалися або відбуваються у побутовому, інтимному, товариському, професійному, діловому та інших сферах життя особи, за винятком даних стосовно виконання повноважень особою, яка займає посаду, пов'язану зі здійсненням функцій держави або органів місцевого самоврядування. Така інформація про фізичну особу та членів її сім'ї є конфіденційною і може бути поширена лише за їх згодою, крім випадків, визначених законом, і лише в інтересах національної безпеки, економічного добробуту та прав людини [58].

З огляду на викладене, доходимо до висновку, що персональні дані у сфері охорони здоров'я належать до конфіденційної інформації та можуть оброблятися виключно за згодою пацієнта або на підставі закону.

У Законі України «Про захист персональних даних» передбачено, що обробка персональних даних у сфері охорони здоров'я неможлива без згоди пацієнта, за виключенням, коли медичні відомості необхідні в цілях охорони здоров'я для: 1) встановлення медичного діагнозу, для забезпечення піклування чи лікування або надання медичних послуг, моніторингу відповідності встановленим умовам надання таких послуг (у тому числі умовам договорів про медичне обслуговування населення та договорів про реімбурсацію за програмою медичних гарантій), функціонування електронної системи охорони здоров'я за умови, що такі дані обробляються медичним працівником, фахівцем з реабілітації або іншою особою закладу охорони здоров'я, реабілітаційного закладу 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 поширюється дія законодавства про лікарську таємницю, працівниками центрального органу виконавчої влади, що реалізує державну політику у сфері державних фінансових гарантій медичного обслуговування населення, працівниками закладу, що здійснює державний санітарно-епідеміологічний нагляд та діяльність у галузі громадського здоров'я, який одержав ліцензію на провадження господарської діяльності з медичної практики, на яких покладено обов'язки щодо забезпечення захисту персональних даних; 2) контролю якості надання медичних послуг за умови, що такі дані обробляються працівниками центрального органу виконавчої влади, що реалізує державну політику у сфері контролю якості надання медичних послуг; 3) обміну інформацією про фінансування медичних послуг та послуг у сфері охорони здоров'я за умови, що такі дані обробляються працівниками Фонду соціального страхування України, Пенсійного фонду України, Фонду соціального захисту осіб з інвалідністю, центрального органу виконавчої влади, що забезпечує формування та реалізує державну фінансову та бюджетну політику, на яких покладено обов'язки щодо забезпечення захисту персональних даних [46].

Враховуючи ст. 3 Закону України «Основи законодавства України про охорону здоров'я» обробка персональних даних у сфері охорони здоров'я без згоди пацієнта є законною якщо вона проводиться в цілях охорони здоров'я встановленим колом осіб, а саме збереження та відновлення фізіологічних і психологічних функцій, оптимальної працездатності та соціальної активності людини при максимальній біологічно можливій індивідуальній тривалості її життя. При цьому слід враховувати, що згідно ч. 7 ст. 6 Закону України «Про захист персональних даних» якщо обробка персональних даних у сфері охорони здоров'я є необхідною для захисту життєво важливих інтересів суб'єкта персональних даних, обробляти персональні дані без його згоди можна до часу, коли отримання згоди стане можливим [46].

Підсумовуючи викладене, на нашу думку, персональні дані у сфері охорони здоров'я – це конфіденційна інформація про медичне обслуговування особи, яка дозволяє її ідентифікувати та дізнатися відомості щодо її стану здоров'я. Істотними ознаками персональних даних у сфері охорони здоров'я є такі: 1) конфіденційна інформація; 2) стосується фізичної особи; 3) містить інформацію про медичне обслуговування особи та відомості про її стан здоров'я; 4) фізична особа є ідентифікованою.

До конфіденційної інформації про медичне обслуговування особи відноситься: інформація про фізичну особу, зібрана під час реєстрації на надання медичних послуг або надання медичних послуг; номер, символьний знак або опис, що приписують фізичній особі для того, щоб ідентифікувати фізичну особу для цілей охорони здоров'я; інформація, отримана внаслідок дослідження або огляду частини тіла чи речовини, що міститься в тілі, у тому числі з генетичних даних або біологічних проб; будь-яка медична інформація (про медичні обстеження, про захворювання, про лікувальні заходи, про прогноз розвитку захворювання, про недієздатність, про ризик захворювання, про історію хвороби, про фізіологічний чи біомедичний стан здоров'я особи, про діагнози та будь-які документи, що стосуються здоров'я та обмеження повсякденного функціонування/життєдіяльності людини). Така інформація викладається у формалізованому вигляді, що забезпечує можливість обробки персональних даних у сфері охорони здоров'я в інформаційних системах [45, с. 189].

1.2. Поняття, становлення та еволюція інституту захисту персональних даних у сфері охорони здоров'я

Інститут захисту персональних даних у сфері охорони здоров'я пройшов певний шлях свого становлення й розвитку. Цей період характеризувався

необхідністю захисту персональних даних, розширенням конституційних прав та свобод людини і громадянина, визначенням правових засад охорони здоров'я та формуванням інформаційного суспільства.

Вперше в українському законодавстві інститут захисту персональних даних знайшов своє відображення в 1992 році з прийняттям Закону України «Про інформацію». У цьому Законі в редакції від 02 жовтня 1992 року до видів інформації було віднесено інформацію про особу. У ст. 23 Закону України «Про інформацію» в редакції від 02 жовтня 1992 року було зазначено, що інформація про особу – це сукупність документованих або публічно оголошених відомостей про особу. Основними даними про особу (персональними даними) є: національність, освіта, сімейний стан, релігійність, стан здоров'я, а також адреса, дата і місце народження. Забороняється збирання відомостей про особу без її попередньої згоди, за винятком випадків, передбачених законом. Кожна особа має право на ознайомлення з інформацією, зібраною про неї. Інформація про особу охороняється Законом [59].

Однак цим нормативно-правовим актом лише здійснювалося наведення кола інформації котра може свідчити про існування «персональних даних», але сам Закон не містив визначення «персональних даних» та не надавав всього переліку персональних даних, а лише констатував основні дані про особу через критерій відомостей про дану особу, що утворювало проблему захисту цих даних від неправомірного використання [60, с. 30].

В подальшому в Закон України «Про інформацію» внесено значну кількість змін (починаючи з 2000 року і до 2023 року). Станом на сьогодні у цьому Законі передбачено визначення поняття «інформація» (будь-які відомості та/або дані, які можуть бути збережені на матеріальних носіях або відображені в електронному вигляді), розуміння категорії «захист інформації» (сукупність правових, адміністративних, організаційних, технічних та інших заходів, що забезпечують збереження, цілісність інформації та належний порядок доступу до неї), такий основний принцип інформаційних відносин як захищеність особи від втручання в її особисте та сімейне життя, право на інформацію (кожен має право на

інформацію, що передбачає можливість вільного одержання, використання, поширення, зберігання та захисту інформації, необхідної для реалізації своїх прав, свобод і законних інтересів), основні види інформаційної діяльності (створення, збирання, одержання, зберігання, використання, поширення, охорона та захист інформації), доступ до інформації (за порядком доступу інформація поділяється на відкриту інформацію (будь-яка інформація, крім тієї, що віднесена законом до інформації з обмеженим доступом) та інформацію з обмеженим доступом (конфіденційна, таємна та службова) [56].

У ст. 11 Закону України «Про інформацію» встановлено, що інформація про фізичну особу (персональні дані) – це відомості чи сукупність відомостей про фізичну особу, яка ідентифікована або може бути конкретно ідентифікована. 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. Кожному забезпечується вільний доступ до інформації, яка стосується його особисто, крім випадків, передбачених законом [56].

Цього ж року було прийнято основний нормативно-правовий акт у сфері охорони здоров'я – Закон України «Основи законодавства України про охорону здоров'я». З моменту набуття чинності і до цього часу в цей Закон внесено понад 70 змін. Закон України «Основи законодавства України про охорону здоров'я» містить такі важливі поняття для сфери захисту персональних даних у сфері охорони здоров'я: електронна охорона здоров'я (е-здоров'я, eHealth), електронна система охорони здоров'я, загальний заклад охорони здоров'я, засіб телемедицини (телемедичний засіб), здоров'я, заклад охорони здоров'я, кластерний заклад охорони здоров'я, медична допомога, медична інформація, медичне обслуговування, мережа закладів охорони здоров'я, метод телемедицини (телемедичний метод), надкластерний заклад охорони здоров'я, невідкладний

стан людини, обмеження життєдіяльності, охорона здоров'я, оцінка медичних технологій, пацієнт, послуга з медичного обслуговування населення (медична послуга), домедична допомога, реабілітаційна допомога у сфері охорони здоров'я, реабілітаційна послуга, реабілітація, рідкісне (орфанне) захворювання, стан здоров'я, теледіагностика, телеконсультування (телевідеоконсультування), телемедицина, телемедична мережа, телеметрія, цифрова компетентність працівників сфери охорони здоров'я.

Серед прав на охорону здоров'я в Законі України «Основи законодавства України про охорону здоров'я» передбачено, що кожний громадянин України має право на кваліфіковану медичну та реабілітаційну допомогу із забезпеченням належного рівня захисту персональних даних, а також на достовірну та своєчасну інформацію про стан свого здоров'я і здоров'я населення, включаючи існуючі і можливі фактори ризику та їх ступінь (ст. 6). Особливості захисту персональних даних в електронній системі охорони здоров'я визначено у ст. 24^2 Закону України «Основи законодавства України про охорону здоров'я». У ст. 35^2 цього Закону встановлено, що надання медичної та/або реабілітаційної допомоги із застосуванням телемедицини здійснюється з дотриманням вимог щодо збереження лікарської таємниці та конфіденційності інформації про стан здоров'я пацієнта, з дотриманням вимог законів України «Про інформацію», «Про захист персональних даних», «Про захист інформації в інформаційно-комунікаційних системах».

У Законі України «Основи законодавства України про охорону здоров'я» регламентовано умови надання медичної інформації (ст. 39), право на таємницю про стан здоров'я (ст. 39^1), питання, пов'язані з лікарської таємницею (ст. 40), загальні умови медичного втручання (ст. 42), умови згоди на медичне втручання (ст. 43), умови застосування методів профілактики, діагностики, лікування та лікарських засобів (ст. 44), умови застосування лікарських засобів у межах програм розширеного доступу пацієнтів до незареєстрованих лікарських засобів та програм доступу суб'єктів дослідження (пацієнтів) до досліджуваного лікарського засобу після завершення клінічного випробування (ст. 44^1), умови

медико-біологічних експериментів на людях (ст. 45), умови штучного запліднення та імплантація ембріона (ст. 48) тощо. Отже, сьогодні Законом України «Основи законодавства України про охорону здоров'я» врегульовано значну кількість питань, пов'язаних із захистом персональних даних у сфері охорони здоров'я.

Важливу роль у становленні інституту захисту персональних даних у сфері охорони здоров'я відіграло прийняття Основного Закону – Конституції України. Так, у ст. 3 передбачено, що людина, її життя і здоров'я, честь і гідність, недоторканність і безпека визнаються в Україні найвищою соціальною цінністю. Права і свободи людини та їх гарантії визначають зміст і спрямованість діяльності держави. Держава відповідає перед людиною за свою діяльність. Утвердження і забезпечення прав і свобод людини є головним обов'язком держави [55]. Згідно ст. 32 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. Кожний громадянин має право знайомитися в органах державної влади, органах місцевого самоврядування, установах і організаціях з відомостями про себе, які не є державною або іншою захищеною законом таємницею. Кожному гарантується судовий захист права спростовувати недостовірну інформацію про себе і членів своєї сім'ї та права вимагати вилучення будь-якої інформації, а також право на відшкодування матеріальної і моральної шкоди, завданої збиранням, зберіганням, використанням та поширенням такої недостовірної інформації [55]. Відповідно до ст. 49 кожен має право на охорону здоров'я, медичну допомогу та медичне страхування [55]. Наведені положення Конституції України є конституційною основою інституту захисту персональних даних у сфері охорони здоров'я.

З'ясовуючи поняття персональних даних О.С. Дяковський звертає увагу на те, що «норми Конституції України не розкривають в повному обсязі поняття персональних даних використовуючи замість нього інший термін, а саме інформацію про особу, що, в свою чергу, утворило законодавчу невизначеність та

необхідність прийняття спеціального нормативного правового акту, котрий регулював би дане коло суспільних відносин. За таких обставин закріплення права на невтручання в особисте життя в національних нормативних актах не вирішило питання в повному обсязі щодо захисту персональних даних та не визначило правового механізму захисту даних прав. Правові норми Конституції України здійснювали забезпечення захисту персональних даних через органи судової влади шляхом розгляду судових спорів та прийняття по суті спору відповідних рішень. Проте відсутність відповідного правового підґрунтя у даній сфері зумовлювало виникнення суспільних проблем, які не знаходили правового регулювання та вимагали прийняття відповідних законів, утворення спеціалізованого органу котрий здійснював би захист персональних даних. За таких обставин з урахуванням розвитку суспільства, зміни засобів та способів виробництва, поява електронних обчислювальних пристроїв призвело до накопичення інформації про фізичну особу та необхідності прийняття спеціального закону щодо захисту персональних даних в національному законодавстві» [60, с. 31].

Протягом 1996-1998 рр. було підготовлено першу версію проєкту Закону України «Про захист персональних даних», який неодноразово розглядався в органах державної влади. У цей період з урахуванням пропозицій державних і недержавних структур було опрацьовано 8 версій цього законопроєкту, а 27 грудня 1998 року він був спрямований до Кабінету Міністрів України (далі – КМ України). Варто звернути увагу на деякі особливості проведення експертних оцінок цього документа у центральних органах виконавчої влади того часу, насамперед, відсутність системності та послідовності в організації роботи з проведення експертизи, що було пов’язано з постійними змінами виконавців та керівництва державних органів, а також те, що багато виконавців не мали жодного уявлення стосовно предмета законопроєкту та суті суспільних відносин у цій сфері. Крім цього, не враховувались положення ст. 11 Конвенції РЄ «Про захист осіб у зв’язку з автоматизованою обробкою персональних даних» від 28 січня 1981 року № 108, ст. 3 Конституції України, а також поширення

несанкціонованих дій із персональними даними (незаконне збирання, реалізація тощо, тобто їх фактичне перетворення у товарноінформаційний продукт, що надходив у товарно-грошовий обіг) [61, с. 37].

Подальший розвиток нормативного закріплення визначення персональних даних тривав з урахуванням уточнень та поправок. Через шість років, після того як законопроєкт пройшов додаткову експертизу, було враховано понад 600 зауважень та пропозицій, отримано позитивний висновок Головного наукового–експертного управління Апарату Верховної Ради України, 16 березня 2006 року він був підтриманий у другому читанні та і в цілому абсолютною більшістю народних депутатів України [60, с. 32]. Однак 11 квітня 2006 року Президентом України було застосовано право «вето» щодо цього законопроєкту. Однією з основних причин вказаного рішення можна вважати те, що фахівці Міністерства юстиції України та інші посадові особи не підтримали положення абз. 3 і абз. 4 ст. 2 цього Закону (в частині запровадження норми щодо «права власності людини на свої персональні дані»), а також ст. 7 Закону, яка це право конкретизувала. По суті законом пропонувалося посилити права людини щодо захисту її приватного життя в умовах стрімкого впровадження інформаційно-комунікаційних технологій та розбудови інформаційного суспільства з використанням правових механізмів інституту власності. Це вимагало певної зміни правової ментальності та внесення змін до чинного законодавства, зокрема, до Цивільного кодексу України, Закону України «Про інформацію» та ін., у т. ч. в частині визначення понятійного апарату, пов’язаного з «особистими немайновими правами фізичної особи». Після доопрацювання із тексту цього Закону було вилучено норми стосовно «права власності людини на свої персональні дані», збільшено кількість термінів щодо інформатизації тощо, а 9 січня 2007 року цей законодавчий акт підтримали вже 329 народних депутатів України. Водночас 30 січня 2007 року Закон знову було повернуто до Верховної Ради України (далі – ВР України) з іншими зауваженнями Президента України щодо «невідповідності Закону положенням статті 32 Конституції України та міжнародно-правовим актам». У 2008 році за пропозиціями групи народних

депутатів України та Міністерства юстиції України був зареєстрований новий проєкт Закону «Про захист персональних даних» (реєстр. № 2273 від 25 березня 2008 року). 25 червня 2009 року він був прийнятий ВР України у першому читанні, а 1 червня 2010 року – як закон № 2297-VI, який набрав чинності з 01 січня 2011 року [61, с. 38-39].

Після прийняття Закону України «Про захист персональних даних», 06 липня 2010 року Україною було ратифіковано [62] Конвенцію РЄ «Про захист осіб у зв'язку з автоматизованою обробкою персональних даних» від 28 січня 1981 року № 108 [63] та Додатковий протокол до цієї Конвенції стосовно органів нагляду та транскордонних потоків даних від 08 листопада 2001 року [64].

Отже, до 2010 року була відсутня ефективна діюча організаційно-правова база у сфері захисту персональних даних, незважаючи на наявність загальних норм конституційного, цивільного, міжнародного права і деяких інших законодавчих актів. Причинами цього є як недостатнє теоретичне проопрацювання окремих фундаментальних нормативних положень, так і суб'єктивно насторожене відношення до проблеми захисту прав людини з боку деяких осіб та органів держаної влади [65, с. 23].

На виконання Закону України «Про захист персональних даних» в редакції 2010 року було утворено уповноважений державний орган з питань захисту персональних даних – Державну службу України з питань захисту персональних даних як центральний орган виконавчої влади, діяльність якої спрямовується і координується КМ України через Міністра юстиції України. Основними завданнями Державної служби України з питань захисту персональних даних України встановлено такі: 1) внесення пропозицій щодо формування державної політики у сфері захисту персональних даних; 2) реалізація державної політики у сфері захисту персональних даних; 3) контроль за додержанням вимог законодавства про захист персональних даних; 4) здійснення міжнародно-правового співробітництва у сфері захисту персональних даних [66].

Згодом Державну службу України з питань захисту персональних даних було ліквідовано, а повноваження щодо захисту конфіденційної інформації про особу передано до Уповноваженого Верховної Ради України з прав людини [67, 68, 69].

У Секретаріаті Уповноваженого Верховної Ради України з прав людини функціонує самостійний структурний підрозділ – Департамент у сфері захисту персональних даних, основними завданнями якого є: забезпечення реалізації повноважень Уповноваженого зі здійснення парламентського контролю за дотриманням прав людини і громадянина та вимог законодавства у сфері захисту персональних даних; забезпечення в межах повноважень розгляду повідомлень про обробку персональних даних, звернень з питань захисту персональних даних, надання рекомендацій щодо практичного застосування законодавства про захист персональних даних, а також роз'яснень прав і обов'язків відповідних суб'єктів; здійснення в межах повноважень нормативно-правового забезпечення у сфері захисту персональних даних; здійснення моніторингу стану дотримання прав людини і громадянина у сфері захисту персональних даних; забезпечення поновлення порушених прав людини і громадянина; забезпечення у межах повноважень виконання міжнародних зобов'язань України щодо імплементації міжнародних правових норм та стандартів, зокрема законодавства ЄС, у сфері захисту персональних даних; забезпечення розробки та впровадження критеріїв і порядку оцінювання стану захищеності персональних даних при їх обробці, а також механізмів сертифікації захисту персональних даних з метою підтвердження відповідності вимогам чинного законодавства України та міжнародних правових норм у сфері захисту персональних даних; забезпечення у межах повноважень просвітницької роботи у сфері захисту персональних даних [70].

Слід також зазначити, що Законом України «Про внесення змін до деяких законодавчих актів України щодо удосконалення системи захисту персональних даних» від 3 липня 2013 року № 383-VII [67] було внесено суттєві зміни до Закону України «Про захист персональних даних» щодо правового режиму персональних даних.

У 2011 році Законом України «Про внесення змін до деяких законодавчих актів України щодо посилення відповідальності за порушення законодавства про захист персональних даних» [71] внесено зміни до Кодексу України про адміністративні правопорушення (далі – КупАП) і Кримінального кодексу України (далі – КК України) стосовно адміністративної та кримінальної відповідальності за порушення законодавства про захист персональних даних. Зокрема, КупАП доповнено статтями 188^{39} (порушення законодавства у сфері захисту персональних даних) і 188^{40} (невиконання законних вимог посадових осіб спеціально уповноваженого центрального органу виконавчої влади з питань захисту персональних даних, згодом назву цієї статті змінено на невиконання законних вимог Уповноваженого Верховної Ради України з прав людини) [72], а у КК України в іншій редакції викладено ст. 182 (порушення недоторканості приватного життя) [73].

До кодифікованих актів, які регулюють захист персональних даних у сфері охорони здоров'я, доцільно також віднести Цивільний кодекс України (передбачає право власності на персональні дані та гарантії дотримання такого права, право на інформацію про стан свого здоров'я, право на таємницю про стан свого здоров'я, право на особисте життя та його таємницю, право на інформацію) [74], Цивільний процесуальний кодекс України (визначає порядок відшкодування шкоди завданої порушенням права особи на персональні дані) [75], Кодекс адміністративного судочинства України (регламентує порядок оскарження рішень, дій чи бездіяльності суб'єкта владних повноважень, що порушують права суб'єкта персональних даних) [76], Кримінальний процесуальний кодекс України (встановлює порядок кримінального провадження у зв'язку із вчиненням діяння щодо порушення недоторканості приватного життя) [77].

Серед нормативно-правових актів інформаційної сфери, які регулюють відносини пов'язані з захистом персональних даних, необхідно виділити Закон України «Про захист інформації в інформаційно-телекомунікаційних системах» (цей Закон регулює відносини у сфері захисту інформації в інформаційних, електронних комунікаційних та інформаційно-комунікаційних системах) [78],

Закон України «Про електронні комунікації» (цей Закон визначає правові та організаційні основи державної політики у сферах електронних комунікацій та радіочастотного спектра, а також права, обов'язки та відповідальність фізичних і юридичних осіб, які беруть участь у відповідній діяльності або користуються електронними комунікаційними послугами) [79], Закон України «Про доступ до публічної інформації» (цей Закон визначає порядок здійснення та забезпечення права кожного на доступ до інформації, що знаходиться у володінні суб'єктів владних повноважень, інших розпорядників публічної інформації, визначених цим Законом, та інформації, що становить суспільний інтерес) [80], Закон України «Про електронні документи та електронний документообіг» (цей Закон встановлює основні організаційно-правові засади електронного документообігу та використання електронних документів) [81], Закон України «Про електронну ідентифікацію та електронні довірчі послуги» (цей Закон визначає правові та організаційні засади електронної ідентифікації та надання електронних довірчих послуг, права та обов'язки суб'єктів відносин у сферах електронної ідентифікації та електронних довірчих послуг, порядок здійснення державного контролю за дотриманням вимог законодавства у сферах електронної ідентифікації та електронних довірчих послуг) [82], Закон України «Про публічні електронні реєстри» (цей Закон встановлює правові, організаційні і фінансові засади створення та функціонування публічних електронних реєстрів з метою захисту прав та інтересів фізичних та юридичних осіб під час створення, зберігання, оброблення та використання інформації у публічних електронних реєстрах) [83], Закон України «Про національну безпеку України» (цей Закон визначає основи та принципи національної безпеки і оборони, цілі та основні засади державної політики, що гарантуватимуть суспільству і кожному громадянину захист від загроз) [84], Закон України «Про основні засади забезпечення кібербезпеки України» (цей Закон визначає правові та організаційні основи забезпечення захисту життєво важливих інтересів людини і громадянина, суспільства та держави, національних інтересів України у кіберпросторі, основні цілі, напрями та принципи державної політики у сфері кібербезпеки, повноваження державних

органів, підприємств, установ, організацій, осіб та громадян у цій сфері, основні засади координації їхньої діяльності із забезпечення кібербезпеки) [85], постанову КМ України «Про функціонування Реєстру публічних електронних реєстрів» (визначає функціональні можливості Реєстру публічних електронних реєстрів, вимоги до його ведення та адміністрування, процедуру внесення інформації до Реєстру реєстрів) [86] тощо.

Після того як Уповноважений Верховної Ради України з прав людини став суб'єктом відносин, пов'язаних із персональними даними, прийнято підзаконні нормативні акти щодо його діяльності у цій сфері, а саме: наказ Уповноваженого Верховної Ради України з прав людини від 8 січня 2014 року № 1/02-14 «Про затвердження документів у сфері захисту персональних даних», яким затверджено Типовий порядок обробки персональних даних; Порядок здійснення Уповноваженим Верховної Ради України з прав людини контролю за додержанням законодавства про захист персональних даних; Порядок повідомлення Уповноваженого Верховної Ради України з прав людини про обробку персональних даних, яка становить особливий ризик для прав і свобод суб'єктів персональних даних, про структурний підрозділ або відповідальну особу, що організовує роботу, пов'язану із захистом персональних даних при їх обробці, а також оприлюднення вказаної інформації [87], наказ Уповноваженого Верховної Ради України з прав людини від 14 жовтня 2022 року № 79.15/22 «Про затвердження Положення про Секретаріат Уповноваженого Верховної Ради України з прав людини» (до 2022 року діяв наказ Уповноваженого Верховної Ради України з прав людини від 20 червня 2012 року № 4/8-12 «Про затвердження Положення про Секретаріат Уповноваженого Верховної Ради України з прав людини» [88]) [89], наказ Уповноваженого Верховної Ради України з прав людини від 20 жовтня 2022 року № 84.15/22 «Про затвердження Положення про представників Уповноваженого Верховної Ради України з прав людини» (до 2022 року діяв наказ Уповноваженого Верховної Ради України з прав людини від 26 липня 2012 року № 7/8-12 «Положення про представників Уповноваженого Верховної Ради України з прав людини» [90]) [91], наказ Уповноваженого

Верховної Ради України з прав людини від 19 лютого 2013 року № 14/02-13 «Про затвердження Положення регіональних представництв Уповноваженого Верховної Ради України з прав людини» [92], наказ Уповноваженого Верховної Ради України з прав людини від 16 лютого 2015 року № 3/02-15 «Про затвердження Порядку оформлення матеріалів про адміністративне правопорушення» [93].

На формування інституту захисту персональних даних у сфері охорони здоров'я значний вплив відіграли підзаконні нормативні акти КМ України та Міністерства охорони здоров'я України (далі – МОЗ України).

Порядок функціонування електронної системи охорони здоров'я (визначає механізм функціонування електронної системи охорони здоров'я та її компонентів, реєстрації користувачів, внесення та обміну інформацією і документами в електронній системі охорони здоров'я) та Порядок опублікування відомостей з електронної системи охорони здоров'я Національною службою здоров'я України (далі – НСЗ України) (встановлює механізм та визначає обсяг опублікування інформації з електронної системи охорони здоров'я НСЗ України), затверджені постановою КМ України від 25 квітня 2018 року № 411 «Деякі питання електронної системи охорони здоров'я» [94]. Порядок організації ведення Електронного реєстру листків непрацездатності та надання інформації з нього затверджений постановою КМ України від 17 квітня 2019 року № 328 [95]. Концепція розвитку електронної охорони здоров'я схвалена розпорядженням КМ України від 28 грудня 2020 року № 1671-р [96].

До підзаконних нормативних актів МОЗ України, які регулюють захист персональних даних у сфері охорони здоров'я, доцільно віднести такі: наказ МОЗ України від 14 лютого 2012 року № 110 «Про затвердження форм первинної облікової документації та Інструкцій щодо їх заповнення, що використовуються у закладах охорони здоров'я незалежно від форми власності та підпорядкування» [97], наказ МОЗ України від 30 липня 2012 року № 577 «Про затвердження форм первинної облікової документації, що використовується в медико-соціальних експертних комісіях» [98], наказ МОЗ України від 29 травня 2013 року № 435

«Про затвердження форм первинної облікової документації та інструкцій щодо їх заповнення, що використовуються у закладах охорони здоров'я, які надають амбулаторно-поліклінічну та стаціонарну допомогу населенню, незалежно від підпорядкування та форми власності» [99], наказ МОЗ України від 19 жовтня 2015 року № 681 «Про затвердження нормативних документів щодо застосування телемедицини у сфері охорони здоров'я» [100], наказ МОЗ України від 19 березня 2018 року № 503 «Про затвердження Порядку вибору лікаря, який надає первинну медичну допомогу, та форми декларації про вибір лікаря, який надає первинну медичну допомогу [101], наказ МОЗ України від 19 березня 2018 року № 504 «Про затвердження Порядку надання первинної медичної допомоги» [102], наказ МОЗ України від 30 листопада 2020 року № 2755 «Про затвердження Порядку ведення Реєстру пацієнтів в електронній системі охорони здоров'я» [103], наказ МОЗ України від 18 вересня 2020 року № 2136 «Деякі питання ведення Реєстру медичних висновків в електронній системі охорони здоров'я» [104], наказ МОЗ України від 28 лютого 2020 року № 587 «Деякі питання ведення Реєстру медичних записів, записів про направлення та рецептів в електронній системі охорони здоров'я» [105].

У результаті проведеного аналізу можна виокремити три етапи становлення інституту захисту персональних даних у сфері охорони здоров'я: 1) 1991-2009 рр. – відсутність належного правового регулювання захисту персональних даних у сфері охорони здоров'я; 2) 2010-2014 рр. – запровадження інституту захисту персональних даних у сфері охорони здоров'я (прийняття Закону України «Про захист персональних даних», Закону України «Про ратифікацію Конвенції про захист осіб у зв'язку з автоматизованою обробкою персональних даних та Додаткового протоколу до Конвенції про захист осіб у зв'язку з автоматизованою обробкою персональних даних стосовно органів нагляду та транскордонних потоків даних», Закону України «Про внесення змін до деяких законодавчих актів України щодо удосконалення системи захисту персональних даних», Закону України «Про внесення змін до деяких законодавчих актів України щодо посилення відповідальності за порушення законодавства про захист персональних

даних», створення та ліквідація Державної служби України з питань захисту персональних даних, повноваження щодо захисту конфіденційної інформації про особу передано до Уповноваженого Верховної Ради України з прав людини, прийняття підзаконних нормативних актів щодо діяльності Уповноваженого Верховної Ради України з прав людини у сфері захисту персональних даних); 3) 2015 – дотепер – удосконалення інституту захисту персональних даних у сфері охорони здоров'я (прийняття Закону України «Про електронну ідентифікацію та електронні довірчі послуги»; Закону України «Про публічні електронні реєстри»; постанови КМ України «Деякі питання електронної системи охорони здоров'я»; наказів МОЗ України «Про затвердження нормативних документів щодо застосування телемедицини у сфері охорони здоров'я», «Про затвердження Порядку вибору лікаря, який надає первинну медичну допомогу, та форми декларації про вибір лікаря, який надає первинну медичну допомогу», «Про затвердження Порядку надання первинної медичної допомоги», «Про затвердження Порядку ведення Реєстру пацієнтів в електронній системі охорони здоров'я»).

Наявність значної кількості різних нормативно-правових актів щодо захисту персональних даних у сфері охорони здоров'я дає підстави для класифікації їх за предметом правового регулювання на загальні та спеціальні акти. До загальних нормативних актів щодо захисту персональних даних у сфері охорони здоров'я відносяться нормативні акти, які регулюють як питання захисту персональних даних, так і інші суспільні відносини (Конституція України, Закон України «Про інформацію», Закон України «Про захист інформації в інформаційно-телекомунікаційних системах», Закон України «Про електронну ідентифікацію та електронні довірчі послуги», Закон України КУпАП України про адміністративні правопорушення, Цивільний кодекс України, КК України тощо). До спеціальних нормативних актів щодо захисту персональних даних у сфері охорони здоров'я відносяться нормативні акти, які регулюють захист персональних даних у сфері охорони здоров'я (Закон України «Про захист персональних даних», Закон України «Основи законодавства України про охорону здоров'я», постанова КМ

України від 25 квітня 2018 року № 411 «Деякі питання електронної системи охорони здоров'я», наказ Уповноваженого Верховної Ради України з прав людини від 8 січня 2014 року № 1/02-14 «Про затвердження документів у сфері захисту персональних даних», наказ МОЗ України від 30 листопада 2020 року № 2755 «Про затвердження Порядку ведення Реєстру пацієнтів в електронній системі охорони здоров'я» тощо).

Законодавство про захист персональних даних та охорону здоров'я не містять чіткого розуміння конструкції «захист персональних даних у сфері охорони здоров'я». Ефективне правове забезпечення захисту персональних даних у сфері охорони здоров'я неможливе без з'ясування сутності цього інституту. Тому постає нагальна потреба правової визначеності сутності інституту захисту персональних даних у сфері охорони здоров'я [106, с. 84].

У юридичній науці відсутній єдиний підхід до визначення сутності категорії «захист персональних даних». Так, з'ясовуючи особливості правового регулювання відносин із захисту персональних даних працівника, А.М. Чернобай захист персональних даних визначає як сукупність організаційно-правових, інженерно-технічних, криптографічних та інших заходів, яких вживає власник цих даних або інші особи на його замовлення, для запобігання заподіянню шкоди інтересам власника та особи, якої вона стосується, її неконтрольованому поширенню. Захист персональних даних працівника містить передбачену законодавством діяльність відповідних державних органів щодо визнання, поновлення прав, а також усунення перешкод, що заважають реалізації прав та законних інтересів суб'єктів права у сфері персональних даних [107, с. 125].

У свою чергу, досліджуючи правові основи захисту персональних даних, А.В. Тунік щодо поняття «захист персональних даних» зазначає наступне. По-перше, захист персональних даних як діяльність здійснюють певні суб'єкти (державні і недержавні), він має цілеспрямований характер та втілюється в певному результаті – захищеності персональних даних. По-друге, така діяльність зумовлена конкретно історичними та соціально-культурними умовами, отже залежить від рівня розвиненості держави та інститутів громадянського

суспільства. По-третє, така діяльність регулюється насамперед правом (різними його галузями: кримінальним, цивільним, адміністративним), а також іншими соціальними засобами, вибір яких залежить від специфіки об'єкта, суб'єкта, мети діяльності тощо [2, с. 35–37].

Окреслюючи поняття та склад персональних даних працівників за трудовим законодавством України Р.В. Куценко зазначає, що поняття захисту персональних даних є доволі широким та зазвичай включає два ключових елемента. По-перше, це зобов'язання володільця вживати організаційних та технічних заходів з метою запобігання їх випадкової втрати або знищення, незаконної обробки, у тому числі незаконного знищення чи доступу до персональних даних (стаття 24 Закону України «Про захист персональних даних»). По-друге, це зобов'язання кожного працівника, володільця та розпорядника не допускати розголошення персональних даних, які стали йому відомі у зв'язку з виконанням професійних, службових або трудових обов'язків, так– зване зобов'язання конфіденційності (стаття 10 Закону України «Про захист персональних даних»). Володілець персональних даних самостійно повинен визначати, яких заходів слід вживати з метою забезпечення захисту персональних даних. При цьому слід враховувати вимоги законодавства у сфері захисту персональних даних та інформаційної безпеки. Вказана вимога стосується усіх володільців [108, с. 105].

Характеризуючи правове регулювання відносин щодо обігу та захисту персональних даних працівника в трудовому праві України А.В. Авраменко визначає захист персональних даних працівників як систему нормативно визначених заходів та способів організаційно-розпорядчого, технічно-облікового та іншого характеру, що вживаються роботодавцем для забезпечення непорушності, недоторканності та цілісності конфіденційних відомостей про особу працівника, а також з метою дотримання порядку обробки вказаної інформації [20, с. 24].

Натомість Ю.С. Самойленко під адміністративно-правовим забезпеченням захисту персональних даних в Україні розуміє здійснюване уповноваженими суб'єктами за допомогою норм адміністративного права через спеціальний

механізм упорядкування, закріплення, реалізації, захисту та охорони суспільних відносин у сфері систематизації, обігу й використання персональних даних [109, с. 23-24].

На нашу думку, наведені визначення не розкривають сутність конструкції «захист персональних даних». Зміст дефініції «захист персональних даних» утворює така складова як «захист». Тому необхідно з‘ясувати сутність поняття «захист» [106, с. 84].

У тлумачних словниках [110, с. 432; 111, с. 370] та теорії права [112, с. 63], як правило, поняття «захист» розуміється як тотожне дефініції «охорона». Водночас С.М. Тараненко вважає, що основою розмежування дефініцій «захист» і «охорона» є критерії наявності чи відсутності порушеного права та його відновлення [113, с. 6-7]. На думку Є.О. Гіда охорона включає заходи, що застосовують до моменту порушення прав людини, а захист – після вчинення правопорушення [114, с. 140]. На наш погляд, найбільш вдало розмежовує дефініції «охорона» і «захист» О.М. Миколенко, який виділяє три критерії як такі, що не охоплюють один одне за змістом, а саме: 1) факт порушення норм права; 2) приналежність цих понять до «права в об’єктивному розумінні» чи «права в суб’єктивному розумінні»; 3) прив’язка зазначених понять до норм матеріального чи норм процесуального (процедурного) права [115, с. 81].

О.М. Миколенко вважає, що охорона права можлива лише до того моменту, коли виникають у зв’язку з порушенням норм права процесуальні (процедурні) правовідносини, в межах яких і відбувається безпосередньо захист порушених суб’єктивних прав або ліквідується реальна загроза їх порушення [115, с. 80–81]. У зв’язку з цим О.М. Миколенко охорону визначає як систему законодавчо встановлених матеріальних правових гарантій, а також діяльність уповноважених на те органів щодо їх реалізації для запобігання порушенням норм чинного законодавства. Захист прав насамперед – це сукупність заходів організаційно-правового характеру, що реалізують компетентні державні органи та організації, яким таке право надано чинним законодавством, у межах юридичного процесу (юридичних процедур) для відновлення порушеного права, усунення перешкод

під час його реалізації, усунення реальної загрози порушення суб'єктивних прав протиправними діями, а також для застосування до порушника заходів правового примусу [115, с. 81].

Аналіз положень Закону України «Про захист персональних даних» (сфера дії Закону; суб'єкти відносин, пов'язаних із персональними даними; об'єкти захисту; вимоги та підстави до обробки персональних даних; права суб'єкта персональних даних; збирання, накопичення, поширення, використання, видалення, знищення персональних даних; доступ до персональних даних; повідомлення про дії з персональними даними; контроль за додержанням законодавства про захист персональних даних; забезпечення захисту персональних даних; відповідальність за порушення законодавства про захист персональних даних) дозволяє стверджувати, що поняття «захист» доцільно трактувати у широкому розумінні, оскільки захист персональних даних в трактуванні законодавця передбачає не тільки протидію порушенням, але й широкий комплекс організаційних та забезпечувальних заходів [12, с. 36]. При цьому у ст. 1 Закону України «Про захист персональних даних» встановлено, що цей Закон спрямований на захист основоположних прав і свобод людини і громадянина, зокрема права на невтручання в особисте життя, у зв'язку з обробкою персональних даних [46].

Відповідно до ст. 3 Закону України «Основи законодавства України про охорону здоров'я» охорона здоров'я – це система заходів, спрямованих на збереження та відновлення фізіологічних і психологічних функцій, оптимальної працездатності та соціальної активності людини при максимальній біологічно можливій індивідуальній тривалості її життя [36].

Слід зазначити, що юридична конструкція охорони здоров'я, що відображена в Законі України «Основи законодавства України про охорону здоров'я» містить цивільні, адміністративні, трудові нормативно-правові приписи, які об'єднані в одному законодавчому акті й відтворюють нормативно-правовий інститут охорони здоров'я [116, с. 23]. При цьому якщо конструкція «охорони здоров'я» є комплексним правовим інститутом, то категорія «захист персональних даних» -

міжгалузевим інститутом права, який реалізує важливу соціальну функцію та посідає окреме місце у структурі права. Захист персональних даних являє собою відносно відокремлену сукупність правових норм, які регулюють певну сферу суспільних відносин. Ця група норм регламентує відносини на стику регулювання різних юридичних галузей, забезпечує вирішення їх завдань, несе відбиток їх іманентних властивостей, тож має комплексний міжгалузевий характер. Захист персональних даних – і як діяльність, і як система правових норм – реалізується в багатьох царинах суспільного життя, охоплює різноманітні сфери суспільних відносин, інтегрується в різні галузі правового регулювання. Зважаючи на це, відповідний нормативний блок має тісні взаємопроникні зв'язки з кількома галузями права. Його першочергова мета – захист конституційного права людини на конфіденційність приватного життя. В основі предмета його регламентації лежать цивільно-правові відносини власності та користування. Кореспондуюча група правових норм акумульована в актах інформаційного законодавства. Провідною сферою їх застосування виступають трудові відносини [12, с. 39-56].

Підсумовуючи викладене, вважаємо, що інститут захисту персональних даних у сфері охорони здоров'я доцільно розглядати як: право на невтручання в особисте життя, а саме право на конфіденційну інформацію про медичне обслуговування особи та відомості щодо її стану здоров'я; комплексний правовий інститут – сукупність правових норм різної галузевої належності, які регулюють суспільні відносини, пов'язані із захистом і обробкою персональних даних у сфері охорони здоров'я; напрям діяльності – комплекс заходів, спрямованих на забезпечення конфіденційності персональних даних у сфері охорони здоров'я. Враховуючи широке розуміння поняття «захист», на наш погляд, захист персональних даних – це сукупність заходів, спрямованих на гарантування безпеки конфіденційної інформації про особу. Для чіткого розуміння конструкції «захист персональних даних» доцільно таке визначення передбачити у ст. 2 Закону України «Про захист персональних даних». Якщо здійснювати акцент на медичну сферу, то захист персональних даних у сфері охорони здоров'я – це сукупність заходів, спрямованих на гарантування безпеки конфіденційної

інформації про медичне обслуговування особи та відомостей щодо її стану здоров'я [106, с. 85-86].

Висновки до розділу 1

1. Інформатизація та цифровізація сфери охорони здоров'я зумовила виникнення проблеми безпеки персональної інформації пацієнтів. В умовах цифрової трансформації сфери охорони здоров'я випадки несанкціонованого втручання в особисте життя осіб та неправомірного поширення і використання їх медичних даних набувають загрозливого та масштабного характеру. Важливість проблеми захисту персональних даних зумовили її дослідження представниками різних юридичних наук, однак питанням правового регулювання захисту персональних даних у сфері охорони здоров'я увага на рівні фундаментальних правових досліджень не приділялася.

2. Поняття «персональні дані» підпадає під правовий вплив різних галузей права, тобто воно регулюється сукупністю правових норм різної галузевої належності, а саме нормами таких галузей права як конституційне, інформаційне, адміністративне, цивільне, трудове, кримінальне та міжнародне. Комплексний характер властивий і сфері охорони здоров'я, який зумовлений наявністю приватних і публічних правовідносин, що становлять предмет цього правового утворення, уможливлює поширення на ці відносини норм таких галузей права, як цивільне, адміністративне, фінансове, трудове, кримінальне, процесуальне права.

3. Персональні дані у сфері охорони здоров'я – це конфіденційна інформація про медичне обслуговування особи, яка дозволяє її ідентифікувати та дізнатися відомості щодо її стану здоров'я. Істотними ознаками персональних даних у сфері охорони здоров'я є такі: 1) конфіденційна інформація; 2) стосується фізичної

особи; 3) містить інформацію про медичне обслуговування особи та відомості про її стан здоров'я; 4) фізична особа є ідентифікованою.

4. До конфіденційної інформації про медичне обслуговування особи відноситься: інформація про фізичну особу, зібрана під час реєстрації на надання медичних послуг або надання медичних послуг; номер, символьний знак або опис, що приписують фізичній особі для того, щоб ідентифікувати фізичну особу для цілей охорони здоров'я; інформація, отримана внаслідок дослідження або огляду частини тіла чи речовини, що міститься в тілі, у тому числі з генетичних даних або біологічних проб; будь-яка медична інформація (про медичні обстеження, про захворювання, про лікувальні заходи, про прогноз розвитку захворювання, про недієздатність, про ризик захворювання, про історію хвороби, про фізіологічний чи біомедичний стан здоров'я особи, про діагнози та будь-які документи, що стосуються здоров'я та обмеження повсякденного функціонування/життєдіяльності людини). Така інформація викладається у формалізованому вигляді, що забезпечує можливість обробки персональних даних у сфері охорони здоров'я в інформаційних системах.

5. У результаті проведеного аналізу законодавства про захист персональних даних та охорону здоров'я виокремлено три етапи становлення інституту захисту персональних даних у сфері охорони здоров'я: 1) 1991-2009 рр. – відсутність належного правового регулювання захисту персональних даних у сфері охорони здоров'я; 2) 2010-2014 рр. – запровадження інституту захисту персональних даних у сфері охорони здоров'я; 3) 2015 – дотепер – удосконалення інституту захисту персональних даних у сфері охорони здоров'я.

6. Наявність значної кількості різних нормативно-правових актів щодо захисту персональних даних у сфері охорони здоров'я дає підстави для класифікації їх за предметом правового регулювання на загальні та спеціальні акти. До загальних нормативних актів щодо захисту персональних даних у сфері охорони здоров'я відносяться нормативні акти, які регулюють як питання захисту персональних даних, так і інші суспільні відносини. До спеціальних нормативних актів щодо захисту персональних даних у сфері охорони здоров'я відносяться

нормативні акти, які регулюють захист персональних даних у сфері охорони здоров’я.

7. Інститут захисту персональних даних у сфері охорони здоров’я доцільно розглядати як: право на невтручання в особисте життя, а саме право на конфіденційну інформацію про медичне обслуговування особи та відомості щодо її стану здоров’я; комплексний правовий інститут – сукупність правових норм різної галузевої належності, які регулюють суспільні відносини, пов’язані із захистом і обробкою персональних даних у сфері охорони здоров’я; напрям діяльності – комплекс заходів, спрямованих на забезпечення конфіденційності персональних даних у сфері охорони здоров’я. Захист персональних даних у сфері охорони здоров’я – це сукупність заходів, спрямованих на гарантування безпеки конфіденційної інформації про медичне обслуговування особи та відомостей щодо її стану здоров’я.

РОЗДІЛ 2
ПРАВОВИЙ РЕЖИМ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ У СФЕРІ ОХОРОНИ ЗДОРОВ'Я

2.1. Сутність та особливості захисту фізичних осіб у зв'язку з обробкою персональних даних у сфері охорони здоров'я

Однією з проблем суспільних відносин, пов'язаних із збиранням, зберіганням, використанням та поширенням конфіденційної інформації про особу, є захист фізичних осіб у зв'язку з обробкою персональних даних у сфері охорони здоров'я, що зумовлено ризиком несанкціонованого втручання в особисте життя осіб та неправомірним поширенням і використанням їх медичних даних. У зв'язку з цим особливої актуальності набуває питання належного правового регулювання відносин, пов'язаних із захистом і обробкою персональних даних у сфері охорони здоров'я [117, с. 668].

Згідно ст. 2 Закону України «Про захист персональних даних» обробка персональних даних – це будь-яка дія або сукупність дій, таких як збирання, реєстрація, накопичення, зберігання, адаптування, зміна, поновлення, використання і поширення (розповсюдження, реалізація, передача), знеособлення, знищення персональних даних, у тому числі з використанням інформаційних (автоматизованих) систем [46]. Відповідно до законодавства про захист персональних даних обробка персональних даних охоплює такі її види: обробка персональних даних, що ведеться повністю або частково із застосуванням автоматизованих засобів; обробка персональних даних, що містяться у картотеці; обробка персональних даних, що призначені до внесення до картотеки [46].

Обробка персональних даних у сфері охорони здоров'я здійснюється у випадках та на умовах, передбачених ст. 7 та ст. 11 Закону України «Про захист персональних даних», згідно яких обробка медичних даних можлива за умови надання пацієнтом однозначної згоди на обробку таких даних або на підставі закону [117, с. 669].

Згода суб'єкта персональних даних – це 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 [46]. У ч. 1 ст. 7 Закону України «Про захист персональних даних» передбачено, що забороняється обробка персональних даних, що стосуються здоров'я, статевого життя, біометричних або генетичних даних [46]. Наприклад, декларація про вибір лікаря, який надає первинну медичну допомогу є документом, що підтверджує реалізацію права пацієнта (його законного представника) на вибір лікаря, заповнюється і підписується за умови згоди на обробку персональних даних, що містяться в електронній системі охорони здоров'я, обраному лікарю, а також іншим лікарям за його направленням у межах, необхідних для надання медичних послуг такими лікарями [103]. Тому обробка персональних даних у сфері охорони здоров'я, за виключенням умов, встановлених законодавством про захист персональних даних (п. 3, п. 6 ч. 2 ст. 7 Закону України «Про захист персональних даних»), здійснюється виключно за згодою пацієнта на обробку його персональних даних [117, с. 669].

Слід відмітити, що у ч. 1 ст. 11 Закону України «Про захист персональних даних» серед підстав для обробки персональних даних наведено такі: дозвіл на обробку персональних даних, наданий володільцю персональних даних відповідно до закону виключно для здійснення його повноважень; 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; необхідність виконання обов'язку володільця персональних даних, який передбачений законом; необхідність захисту законних інтересів володільця персональних даних або третьої особи, якій передаються персональні дані, крім випадків, коли потреби захисту основоположних прав і свобод суб'єкта персональних даних у зв'язку з обробкою його даних переважають такі інтереси [46]. Зауважимо, що всі ці підстави обробки персональних даних у сфері охорони

здоров’я можливі за умови згоди суб’єкта персональних даних на обробку його персональних даних.

Наприклад, розглянемо таку підставу обробки персональних даних як дозвіл на обробку персональних даних, наданий володільцю персональних даних відповідно до закону виключно для здійснення його повноважень. Володілець персональних даних – це фізична або юридична особа, яка визначає мету обробки персональних даних, встановлює склад цих даних та процедури їх обробки, якщо інше не визначено законом [46]. Володільцем персональних даних у сфері охорони здоров’я можуть бути органи публічної влади (наприклад, володільцем персональних даних, які містяться в Реєстрі пацієнтів в електронній системі охорони здоров’я, є НСЗ України [103]), заклади охорони здоров’я (юридична особа будь-якої форми власності та організаційно-правової форми або її відокремлений підрозділ, що забезпечує медичне обслуговування населення на основі відповідної ліцензії та професійної діяльності медичних (фармацевтичних) працівників і фахівців з реабілітації) та фізичні особи – підприємці, які зареєстровані та одержали відповідну ліцензію у встановленому законом порядку, у сфері охорони здоров’я, що не обов’язково обмежується медичною допомогою та/або реабілітаційною допомогою, але безпосередньо пов’язана з їх наданням [36]. Така обробка персональних даних у сфері охорони здоров’я можлива виключно за умови згоди пацієнта на обробку його персональних даних, тобто дозвіл на обробку персональних даних надає суб’єкт персональних даних володільцю виключно для здійснення його повноважень.

Сьогодні зручним сервісом для суб’єктів відносин у сфері охорони здоров’я є електронна система охорони здоров’я (е-здоров’я, eHealth) – екосистема гармонічних та взаємоприйнятних інформаційних відносин усіх учасників медичного середовища держави, які базуються на економічно ефективному та безпечному використанні інформаційно-комунікаційних технологій, спрямованих на підтримку системи охорони здоров’я, включаючи медичні послуги, профілактичний нагляд за здоров’ям, медичну літературу та медичну освіту, знання та дослідження [96]. Метою функціонування електронної системи охорони

здоров’я є забезпечення виконання завдань та функцій у сфері охорони здоров’я [36]. Електронна система охорони здоров’я складається з центральної бази даних (інформаційно-комунікаційна система, яка реєстри, програмні модулі, електронну медичну інформаційно-аналітичну систему з оптимізації роботи оперативно-диспетчерських служб центрів екстреної медичної допомоги та медицини катастроф, електронні кабінети пацієнтів і посадових осіб НСЗ України та МОЗ України, інформаційну систему НСЗ України в частині, необхідній для реалізації державних фінансових гарантій медичного обслуговування населення, а також забезпечує можливість створення, перегляду, обміну інформацією та документами між реєстрами, державними електронними інформаційними ресурсами, електронними медичними інформаційними системами) та електронних медичних інформаційних систем (інформаційно-комунікаційна система, яка забезпечує функціонування електронних кабінетів користувачів, автоматизацію їх роботи, створення, перегляд інформації, обмін інформацією в електронній формі, зокрема із центральною базою даних (у разі підключення), між якими забезпечено автоматизований обмін інформацією, даними та документами через відкритий програмний інтерфейс (API) [94].

У центральній базі даних ведуться такі реєстри [94]:

1) Реєстр пацієнтів, що містить інформацію про пацієнтів, до якого включаються такі відомості про пацієнта: унікальний номер запису в Єдиному державному демографічному реєстрі (у разі наявності); реєстраційний номер облікової картки платника податків (у разі наявності) або серія та номер паспорта (для фізичних осіб, які через релігійні переконання відмовляються від прийняття реєстраційного номера облікової картки платника податків та повідомили про це відповідному контролюючому органу і мають відмітку у паспорті); прізвище, ім’я, по батькові; дата та місце народження; адреса фактичного місця проживання або перебування; серія та номер (у разі наявності) документа, що посвідчує особу (паспорт громадянина України, тимчасове посвідчення громадянина України, свідоцтво про народження (для осіб, які не досягли 14-річного віку), посвідка на постійне проживання в Україні, посвідчення біженця, посвідчення особи, яка

потребує додаткового захисту, посвідка на тимчасове проживання), орган, що видав документ, дата видачі, строк дії; номер телефону, адреса електронної пошти (у разі надання); інформація про законного представника особи (прізвище, ім’я, по батькові, документи, що посвідчують його особу та повноваження законного представника відповідно до законодавства) (у разі наявності); номер телефону, адреса електронної пошти (далі - контактні дані) (у разі надання); інформація про довірену особу для повідомлення в разі настання екстреного випадку з пацієнтом (прізвище, ім’я, по батькові (за наявності), контактні дані); інформація про обраний метод(и) автентифікації, а саме: за номером мобільного телефону пацієнта; за електронними копіями оригіналів документів шляхом їх завантаження до системи; за унікальним ідентифікатором іншого пацієнта в Реєстрі; статус запису про пацієнта в Реєстрі: «активний» («active»); «неактивний» («inactive»); статус верифікації запису про пацієнта в Реєстрі: «потребує верифікації» («VERIFICATION_NEEDED»); «на верифікації» («IN_REVIEW»); «успішна верифікація» («VERIFIED»); «неуспішна верифікація» («NOT_VERIFIED»); інформація щодо підтвердження підстави верифікації запису про пацієнта в Реєстрі. Відомості з Реєстру пацієнтів є інформацією з обмеженим доступом [103];

2) Реєстр декларацій про вибір лікаря, який надає первинну медичну допомогу, що містить записи про декларації, внесені до зазначеного реєстру. До зазначеного Реєстру включаються такі відомості: посилання на запис про пацієнта у Реєстрі пацієнтів; посилання на запис про медичного працівника, обраного пацієнтом (його законним представником) як лікаря, який надає первинну медичну допомогу, у Реєстрі медичних працівників; посилання на запис про надавача медичних послуг у Реєстрі суб’єктів господарювання у сфері охорони здоров’я; посилання на запис про місце надання медичних послуг, обране пацієнтом, у Реєстрі суб’єктів господарювання у сфері охорони здоров’я;

3) Реєстр суб’єктів господарювання у сфері охорони здоров’я, що містить інформацію про заклади охорони здоров’я, фізичних осіб - підприємців, які мають ліцензію на провадження господарської діяльності з медичної практики, та

лабораторії, які уклали або мають намір подати заяву про укладення договору за програмою медичних гарантій або залучені надавачами медичних послуг до надання медичних послуг. До зазначеного Реєстру включаються такі відомості: повне та скорочене (у разі наявності) найменування юридичної особи або прізвище, ім'я, по батькові фізичної особи - підприємця; код згідно з ЄДРПОУ чи реєстраційний номер облікової картки платника податків (у разі наявності) або серія та номер паспорта (для фізичних осіб, які через релігійні переконання відмовляються від прийняття реєстраційного номера облікової картки платника податків та повідомили про це відповідному контролюючому органу і мають відмітку у паспорті) суб'єкта господарювання у сфері охорони здоров'я; форма власності (для юридичних осіб); місцезнаходження; прізвище, ім'я, по батькові, найменування посади, контактні дані керівника суб'єкта господарювання у сфері охорони здоров'я; прізвище, ім'я, по батькові, найменування посади осіб, яким суб'єкт господарювання у сфері охорони здоров'я надав права доступу до електронної системи охорони здоров'я, передбачені пунктом 43 Порядку ведення Реєстру пацієнтів в електронній системі охорони здоров'я, із зазначенням обсягу таких прав; відомості про чинні та анульовані ліцензії, акредитацію, інші дозвільні документи суб'єкта господарювання у сфері охорони здоров'я; інформація про місця надання медичних послуг або відокремлені підрозділи аптечних закладів (адреса, контактні дані);

4) Реєстр медичних спеціалістів, що містить інформацію про осіб, які надають медичну та/або реабілітаційну допомогу. До зазначеного Реєстру включаються такі відомості: посилання на запис про медичного спеціаліста у Реєстрі пацієнтів; освітньо-кваліфікаційний рівень медичного спеціаліста; спеціальність медичного спеціаліста; дата початку роботи за спеціальністю та інформація про періоди, протягом яких медичний спеціаліст не працював за спеціальністю; інформація про підвищення кваліфікації та перепідготовку медичного спеціаліста. Інформація до зазначеного Реєстру вноситься, зокрема, шляхом електронної взаємодії та обміну відомостями з Єдиною державною електронною базою з питань освіти;

5) Реєстр медичних працівників, що містить інформацію про професійно підготовлених осіб, які відповідно до законодавства мають право здійснювати медичне обслуговування. До зазначеного Реєстру включаються такі відомості: посилання на запис у Реєстрі медичних спеціалістів про медичного працівника; посилання на запис про суб'єкта господарювання у сфері охорони здоров'я у Реєстрі суб'єктів господарювання у сфері охорони здоров'я; найменування посади та спеціалізація медичного працівника; контактні дані медичного працівника для запису на прийом до нього;

6) Реєстр медичних записів, записів про направлення та рецептів. До зазначеного Реєстру включаються такі відомості: номер запису у Реєстрі медичних записів, записів про направлення та рецептів; дата та час внесення запису в Реєстр медичних записів, записів про направлення та рецептів; посилання на запис у Реєстрі суб'єктів господарювання у сфері охорони здоров'я про місце надання медичних послуг, де здійснювалося медичне обслуговування пацієнта, або зазначення «за місцем перебування пацієнта»; посилання на запис у Реєстрі суб'єктів господарювання у сфері охорони здоров'я про суб'єкта господарювання, який здійснює медичне обслуговування; посилання на запис у Реєстрі медичних працівників про медичного працівника, який вніс запис до Реєстру медичних записів, записів про направлення та рецептів; посилання на запис у Реєстрі пацієнтів про пацієнта; вік пацієнта; стать пацієнта; інші відомості, передбачені порядком ведення Реєстру медичних записів, записів про направлення та рецептів, затвердженим МОЗ України;

9) Реєстр медичних висновків. До зазначеного Реєстру включаються такі відомості: посилання на запис про пацієнта в Реєстрі пацієнтів; посилання на запис про лікаря, що сформував та підписав медичний висновок, у Реєстрі медичних працівників; посилання на запис про суб'єкта господарювання в Реєстрі суб'єктів господарювання у сфері охорони здоров'я; дата та час формування і реєстрації медичного висновку в Реєстрі медичних висновків; вид медичного висновку; суть висновку лікаря відповідно до виду медичного висновку; строк дії медичного висновку або зазначення «безстроково»; інші відомості, передбачені

порядками формування та видачі медичних висновків відповідного виду, затвердженими МОЗ України;

7) інші реєстри, набір даних в яких визначається НСЗ України.

У п. 23 постанови КМ України від 25 квітня 2018 року № 411 передбачено, що персональні дані у реєстрах можуть оброблятися у цілях охорони здоров'я, встановлення медичного діагнозу, забезпечення лікування або надання медичних послуг, функціонування електронної системи охорони здоров'я. Персональні дані, що стосуються здоров'я, можуть оброблятися за умови, що вони 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 поширюється дія законодавства про лікарську таємницю, працівниками НСЗ України, на яких покладено обов'язки щодо забезпечення захисту персональних даних. Оператори електронної медичної інформаційної системи обробляють персональні дані за наявності правових підстав відповідно до вимог Закону України «Про захист персональних даних» [94].

Для надання або отримання медичних послуг, лікарських засобів та медичних виробів за програмою медичних гарантій користувачі зобов'язані зареєструватися у відповідних реєстрах. Реєстрація суб'єкта господарювання у сфері охорони здоров'я та уповноважених осіб такого суб'єкта господарювання здійснюється його керівником або фізичною особою - підприємцем, яка одержала ліцензію на провадження господарської діяльності з медичної практики. Реєстрація пацієнтів та медичних спеціалістів здійснюється ними самостійно або шляхом звернення до суб'єкта господарювання у сфері охорони здоров'я. Законний представник пацієнта може зареєструвати пацієнта шляхом звернення до надавача медичних послуг для забезпечення проведення перевірки документів, що посвідчують повноваження законного представника. Під час реєстрації повинно бути однозначно встановлено (ідентифіковано) особу користувача, а у разі реєстрації суб'єкта господарювання у сфері охорони здоров'я - відповідну

юридичну особу та її керівника або фізичну особу - підприємця, яка одержала ліцензію на провадження господарської діяльності з медичної практики. У разі самостійної реєстрації здійснюється електронна ідентифікація користувача відповідно до законодавства. Пацієнт використовує для електронної ідентифікації кваліфікований електронний підпис або удосконалений електронний підпис, що базується на кваліфікованому сертифікаті електронного підпису. Під час реєстрації шляхом звернення до суб'єкта господарювання у сфері охорони здоров'я встановлення особи користувача здійснюється шляхом пред'явлення документа, що посвідчує особу відповідно до Закону України «Про Єдиний державний демографічний реєстр та документи, що підтверджують громадянство України, посвідчують особу чи її спеціальний статус». Після реєстрації користувача автоматично формується запис у центральній базі даних. Вхід до електронного кабінету здійснюється користувачем після його автентифікації відповідно до законодавства [94].

Доступ користувачів до функціональних можливостей електронної системи охорони здоров'я здійснюється через електронні кабінети. Електронні кабінети керівників та уповноважених осіб суб'єкта господарювання у сфері охорони здоров'я, медичних працівників функціонують в електронних медичних інформаційних системах, підключених до центральної бази даних відповідно до Порядку ведення Реєстру пацієнтів в електронній системі охорони здоров'я, із дотриманням вимог Закону України «Про захист персональних даних». Особистий кабінет пацієнта забезпечує доступ пацієнтів (їх законних представників) до електронної системи охорони здоров'я через електронний кабінет пацієнта, що входить до складу центральної бази даних, або через електронні кабінети пацієнта, що функціонують в електронних медичних інформаційних системах, підключених до центральної бази даних відповідно до Порядку ведення Реєстру пацієнтів в електронній системі охорони здоров'я, у тому числі на Порталі Дія, зокрема із використанням мобільного додатка Порталу Дія (Дія), із дотриманням вимог Закону України «Про захист персональних даних» [94].

Під реєстрації, внесення та обміну інформацією і документами в електронній системі охорони здоров'я, пацієнт має право: 1) реєструвати себе в центральній базі даних, подавати заяви про внесення змін і доповнень до відповідних відомостей у Реєстрі пацієнтів; 2) вносити та переглядати інформацію про себе, що міститься в центральній базі даних; 3) подавати декларацію через електронну систему охорони здоров'я в порядку, установленому МОЗ України, вносити інформацію про припинення дії декларації до Реєстру декларацій про вибір лікаря, який надає первинну медичну допомогу, переглядати записи про всі подані декларації в зазначеному Реєстрі; 4) переглядати перелік електронних медичних інформаційних систем, яким пацієнт надав доступ до інформації про себе, що міститься в центральній базі даних, із метою використання функціональних можливостей електронної системи охорони здоров'я, за умови автентифікації пацієнта в електронному кабінеті пацієнта, що функціонує у відповідній електронній медичній інформаційній системі, а також припиняти такий доступ. Законний представник пацієнта, зареєстрований у центральній базі даних, від імені та в інтересах пацієнта реалізує права пацієнта, передбачені Порядком ведення Реєстру пацієнтів в електронній системі охорони здоров'я та нормативно-правовими актами, що регулюють порядок ведення відповідних реєстрів центральної бази даних [94].

Реєстрація пацієнтів в Реєстрі пацієнтів здійснюється відповідно до Порядку ведення Реєстру пацієнтів в електронній системі охорони здоров'я, затвердженого наказом МОЗ України від 30 листопада 2020 року № 2755 [103].

На підставі документів та інформації, наданих пацієнтом (його законним представником), медичний працівник або уповноважена особа суб'єкта господарювання здійснює ідентифікацію пацієнта, виконує пошук пацієнта у Реєстрі та, у разі відсутності такого пацієнта в Реєстрі, створює запит на реєстрацію пацієнта в Реєстрі. Для пацієнтів, реєстрація яких здійснюється законним представником – основним методом автентифікації зазначається унікальний ідентифікатор законного представника в Реєстрі. Для пацієнтів, реєстрація яких здійснюється особисто – основним методом автентифікації не

може бути зазначено унікальний ідентифікатор іншого пацієнта, зареєстрованого в Реєстрі. Для пацієнтів, у яких відсутній активний метод автентифікації, при першому наступному зверненні до суб'єкта господарювання, такий суб'єкт зобов'язаний внести інформацію про обраний метод автентифікації до Реєстру [103].

Пацієнт (його законний представник) перевіряє внесену інформацію, та у разі виявлення помилок повідомляє про це особі, яка цю інформацію внесла, після чого вона зобов'язана виправити помилки у внесених відомостях про пацієнта. Після внесення інформації пацієнт (його законний представник), за допомогою обраного методу автентифікації підтверджує достовірність внесених даних, запит на реєстрацію пацієнта в Реєстрі та факт ознайомлення з повідомленням про обробку персональних даних, у такому порядку: 1) для пацієнтів, що обрали метод автентифікації за допомогою номеру мобільного телефону або пацієнтів, реєстрація яких здійснюється законним представником, для якого методом автентифікації є автентифікація за допомогою номеру мобільного телефону – шляхом надання медичному представнику або уповноваженій особі суб'єкта господарювання, що вносить інформацію про пацієнта, одноразового чотиризначного коду отриманого від системи в текстовому повідомленні на номер мобільного телефону пацієнта або його законного представника; 2) для пацієнтів, що обрали метод автентифікації за допомогою документів або для пацієнтів, реєстрація яких здійснюється законним представником, для якого методом автентифікації є автентифікація за допомогою документів – інформація про пацієнта роздруковується. Пацієнт (його законний представник) підтверджує достовірність внесених даних та факт ознайомлення з повідомленням про обробку персональних даних особистим підписом. Підтвердження реєстрації пацієнта в Реєстрі відбувається шляхом завантаження до системи електронних копій оригіналів документів, наданих пацієнтом або його законним представником [103].

У разі реєстрації пацієнта в Реєстрі через суб'єкта господарювання інформація про пацієнта, внесена до Реєстру, роздруковується в двох примірниках

та підписується пацієнтом та особою, яка внесла цю інформацію до Реєстру. Один примірник надається пацієнту (його законному представнику), інший залишається у відповідного суб'єкта господарювання та зберігається три роки. У разі відсутності помилок медичний працівник (лікар) суб'єкта господарювання накладає на створений у Реєстрі запит свій кваліфікований електронний підпис та передає його до центральної бази даних системи, після чого запиту присвоюється унікальний номер, який є унікальним ідентифікатором пацієнта в Реєстрі. У разі зміни документів, що посвідчують особу пацієнта, інформація про які внесена до Реєстру, у тому числі отримання неповнолітньою особою паспорту громадянина України, при першому наступному зверненні до суб'єкта господарювання, такий суб'єкт господарювання зобов'язаний внести оновлені відомості до Реєстру при отриманні таких відомостей від пацієнта. Пацієнт може змінити інформацію про себе, що міститься в Реєстрі: самостійно, через електронний кабінет пацієнта, окрім відомостей про РНОКПП, прізвище, ім'я, по батькові (за наявності), дату народження, методи автентифікації; шляхом звернення, у тому числі через законного представника, до суб'єкта господарювання. Дані, внесені до Реєстру автоматично при реєстрації в інших державних реєстрах у випадках, передбачених законодавством, змінюються у разі внесення змін до відповідних державних реєстрів [103].

У ч. 2 ст. 24^2 Закону України «Основи законодавства України про охорону здоров'я» передбачено, що доступ до відомостей 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. Без згоди доступ до відомостей про пацієнта можливий лише: за наявності ознак прямої загрози життю пацієнта; у разі неможливості отримання згоди такого пацієнта чи його законного представника (до часу, коли отримання згоди стане можливим); за рішенням суду [36].

Персональні дані пацієнтів в Україні збираються за їхньою письмовою згодою. Підпис декларації про вибір лікаря, який надає первинну медичну

допомогу, є згодою особи на обробку її персональних даних у електронній системі охорони здоров'я.

Пацієнт (його законний представник) подає Декларацію шляхом безпосереднього звернення до надавача первинної медичної допомоги. Декларація про вибір лікаря, який надає первинну медичну допомогу (далі - Декларація) – документ, що підтверджує реалізацію права пацієнта (його законного представника) на вибір лікаря, який надає первинну медичну допомогу, за умови його подання у встановленому цим нормативно-правовим актом порядку [101].

Подання Декларації здійснюється в такому порядку [101]:

1) пацієнт (його законний представник) надає уповноваженій особі або безпосередньо обраному лікарю, який надає первинну медичну допомогу: документ, що засвідчує реєстрацію пацієнта в Державному реєстрі фізичних осіб - платників податків за наявності (крім фізичних осіб, які через свої релігійні переконання відмовляються від прийняття РНОКПП та повідомили про це відповідний контролюючий орган і мають відмітку у паспорті), та один з таких документів, що посвідчують особу: паспорт громадянина України; тимчасове посвідчення громадянина України; свідоцтво про народження (для осіб, які не досягли 14-річного віку) або документ, що підтверджує факт народження, виданий компетентними органами іноземної держави, легалізований у встановленому законодавством порядку; посвідка на постійне проживання в Україні; посвідчення біженця; посвідчення особи, яка потребує додаткового захисту;

2) законний представник пацієнта додатково подає документи, що посвідчують його особу та повноваження законного представника відповідно до законодавства України;

3) на підставі документів та інформації, наданих пацієнтом (його законним представником), уповноважена особа або лікар, який надає первинну медичну допомогу, здійснює пошук запису про пацієнта в Реєстрі пацієнтів центральної бази даних системи. У разі відсутності запису про такого пацієнта надавачем

первинної медичної допомоги забезпечується його невідкладна реєстрація відповідно до Порядку ведення Реєстру пацієнтів в електронній системі охорони здоров'я, затвердженого наказом МОЗ України від 30 листопада 2020 року № 2755;

4) у разі наявності запису про такого пацієнта в Реєстрі пацієнтів центральної бази даних системи уповноважена особа або лікар, який надає первинну медичну допомогу, вносить інформацію про Декларацію до Реєстру декларацій про вибір лікаря, який надає первинну медичну допомогу, центральної бази даних системи відповідно до Порядку ведення Реєстру декларацій про вибір лікаря, який надає первинну медичну допомогу, в електронній системі охорони здоров'я, та роздруковує Декларацію, заповнену за формою, затвердженою наказом МОЗ України від 19 березня 2018 року № 503. Пацієнт (його законний представник) перевіряє інформацію, що міститься в Декларації, та у разі виявлення помилок повідомляє про це особу, яка створювала запит на реєстрацію, для внесення необхідних змін до відповідних реєстрів системи, створення нового запиту на реєстрацію із виправленими помилками та формування нової Декларації. Особа, яка створювала запит на реєстрацію, повідомляє пацієнта (його законного представника) про його права відповідно до Закону України «Про захист персональних даних» та про мету збирання та обробки його персональних даних, зазначених у Декларації;

5) Декларація вважається поданою з дотриманням зазначених умов у такій послідовності: проставлення підпису пацієнтом (його законним представником) на двох примірниках роздрукованої Декларації, яким підтверджується правильність наданої ним інформації, зазначеної в Декларації, а також надання згоди на доступ до відомостей про нього, що містяться в системі, обраному лікарю, який надає первинну медичну допомогу, а також іншим лікарям за його направленням у межах, необхідних для надання медичних послуг такими лікарями; завершення процедури внесення інформації про Декларацію до Реєстру декларацій про вибір лікаря, який надає первинну медичну допомогу, центральної бази даних системи відповідно до Порядку ведення Реєстру декларацій про вибір

лікаря, який надає первинну медичну допомогу, в електронній системі охорони здоров'я;

6) один примірник Декларації залишається у пацієнта (його законного представника), інший – у надавача первинної медичної допомоги, який має зберігатися протягом трьох років з дня припинення дії такої Декларації.

У ч. 3 ст. 24^2 Закону України «Основи законодавства України про охорону здоров'я» передбачено, що підписуючи декларацію про вибір лікаря, який надає первинну медичну допомогу, пацієнт (його законний представник) надає згоду на доступ до відомостей про нього, що містяться в електронній системі охорони здоров'я, такому лікарю, а також іншим лікарям за його направленням у межах, необхідних для надання медичних послуг такими лікарями [36]. Згідно ч. 4 ст. 24^2 Закону України «Основи законодавства України про охорону здоров'я» під час інформаційної взаємодії між електронною системою охорони здоров'я та Єдиним державним демографічним реєстром, Державним реєстром актів цивільного стану громадян та Державним реєстром фізичних осіб – платників податків, доступ до медичної інформації щодо пацієнта не допускається [36].

Обробка персональних даних у сфері охорони здоров'я без згоди пацієнта здійснюється: 1) коли медичні відомості необхідні в цілях охорони здоров'я для: а) встановлення медичного діагнозу, для забезпечення піклування чи лікування або надання медичних послуг, моніторингу відповідності встановленим умовам надання таких послуг (у тому числі умовам договорів про медичне обслуговування населення та договорів про реімбурсацію за програмою медичних гарантій), функціонування електронної системи охорони здоров'я за умови, що такі дані обробляються медичним працівником, фахівцем з реабілітації або іншою особою закладу охорони здоров'я, реабілітаційного закладу 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 поширюється дія законодавства про лікарську таємницю, працівниками центрального органу виконавчої влади, що реалізує державну політику у сфері державних фінансових гарантій медичного

обслуговування населення, працівниками закладу, що здійснює державний санітарно-епідеміологічний нагляд та діяльність у галузі громадського здоров’я, який одержав ліцензію на провадження господарської діяльності з медичної практики, на яких покладено обов’язки щодо забезпечення захисту персональних даних; б) контролю якості надання медичних послуг за умови, що такі дані обробляються працівниками центрального органу виконавчої влади, що реалізує державну політику у сфері контролю якості надання медичних послуг; в) обміну інформацією про фінансування медичних послуг та послуг у сфері охорони здоров’я за умови, що такі дані обробляються працівниками Фонду соціального страхування України, Пенсійного фонду України, Фонду соціального захисту осіб з інвалідністю, центрального органу виконавчої влади, що забезпечує формування та реалізує державну фінансову та бюджетну політику, на яких покладено обов’язки щодо забезпечення захисту персональних даних; 2) для захисту життєво важливих інтересів суб’єкта персональних даних [46].

Прикладом захисту життєво важливих інтересів суб’єкта персональних даних є надання невідкладної медичної допомоги. У ст. 37 Закону України «Основи законодавства України про охорону здоров’я» передбачено, що медичні працівники зобов’язані невідкладно надавати необхідну медичну допомогу у разі виникнення невідкладного стану людини [36]. Невідкладний стан людини – це раптове погіршення фізичного або психічного здоров'я, яке становить пряму та невідворотну загрозу життю та здоров'ю людини або оточуючих її людей і виникає внаслідок хвороби, травми, отруєння або інших внутрішніх чи зовнішніх причин [36]. Згідно ст. 43 Закону України «Основи законодавства України про охорону здоров’я» згода пацієнта чи його законного представника на медичне втручання не потрібна лише у разі наявності ознак прямої загрози життю пацієнта за умови неможливості отримання з об’єктивних причин згоди на таке втручання від самого пацієнта чи його законних представників [36]. Тому у випадку надання невідкладної медичної допомоги за умови неможливості отримання з об’єктивних причин згоди від пацієнта медичне втручання та обробка персональних даних здійснюється без згоди суб’єкта персональних даних. Однак, слід зауважити, що

обробляти персональні дані без згоди пацієнта можна до часу, коли отримання згоди стане можливим [46].

Необхідно звернути увагу на те, що згідно ч. 1 ст. 25 Закону України «Про захист персональних даних» обмеження щодо обробки персональних даних у сфері охорони здоров'я може здійснюватися у випадках, передбачених законом, наскільки це необхідно у демократичному суспільстві в інтересах національної безпеки, економічного добробуту або захисту прав і свобод суб'єктів персональних даних чи інших осіб [46]. Відповідно, у разі дотримання цих умов обробка персональних даних у сфері охорони здоров'я може здійснюватися у випадках, не передбачених ч. 2 ст. 7 Закону України «Про захист персональних даних». Наприклад, застосування ч. 1 ст. 25 Закону України «Про захист персональних даних» можливе у разі звернення Пенсійного фонду України до суб'єкта господарювання у сфері охорони здоров'я щодо надання доступу до медичних документів, що стали підставою для видачі особі листка непрацездатності, з метою перевірки обґрунтованості його видачі та наявності підстав для нарахування відповідних виплат [117, с. 672].

Законом України «Про захист персональних даних» [46] передбачено, що володільці, розпорядники персональних даних та треті особи зобов'язані забезпечити захист цих даних від випадкових втрати або знищення, від незаконної обробки, у тому числі незаконного знищення чи доступу до персональних даних (ч. 1 ст. 24); володілець персональних даних зобов'язаний повідомляти Уповноваженого Верховної Ради України з прав людини про обробку персональних даних, яка становить особливий ризик для прав і свобод суб'єктів персональних даних, упродовж тридцяти робочих днів з дня початку такої обробки (ч. 1 ст. 9); володільцю забороняється розголошувати відомості стосовно суб'єктів персональних даних, доступ до персональних даних яких надається іншим суб'єктам відносин, пов'язаних з такими даними (ч. 2 ст. 10); працівники суб'єктів відносин, що пов'язані з персональними даними, зобов'язані не допускати розголошення у будь-який спосіб персональних даних, які їм було довірено або які стали відомі у зв'язку з виконанням професійних чи службових

або трудових обов'язків (ч. 3 ст. 10). Заходи захисту персональних даних, спрямовані на запобігання їх випадкових втрати або знищення, незаконної обробки, у тому числі незаконного знищення чи доступу до персональних даних, які повинні вживати всі володільці, передбачені Типовим порядком обробки персональних даних, затвердженим наказом Уповноваженого Верховної Ради України з прав людини від 8 січня 2014 року № 1/02-14 [87].

Порядок доступу до персональних даних у сфері охорони здоров'я третіх осіб визначається умовами згоди суб'єкта персональних даних на обробку цих даних, наданої володільцю персональних даних, або відповідно до вимог закону. Доступ до персональних даних третій особі не надається, якщо зазначена особа відмовляється взяти на себе зобов'язання щодо забезпечення виконання вимог Закону України «Про захист персональних даних» або неспроможна їх забезпечити. Персональні дані у сфері охорони здоров'я третім особам можуть бути надані володільцем таких даних на підставі запиту [46]. Отже, персональні дані у сфері охорони здоров'я третім особам можуть бути надані за згодою особи або за наявності підстав, визначених ст. 7 Закону України «Про захист персональних даних» [117, с. 672].

Транскордонна передача персональних даних у сфері охорони здоров'я здійснюється лише за умови забезпечення відповідною державою належного захисту персональних даних у випадках, встановлених законом або міжнародним договором України. Держави – учасниці Європейського економічного простору, а також держави, які підписали Конвенцію РЄ про захист осіб у зв'язку з автоматизованою обробкою персональних даних, визнаються такими, що забезпечують належний рівень захисту персональних даних. Кабінет Міністрів України визначає перелік держав, які забезпечують належний захист персональних даних. Персональні дані не можуть поширюватися з іншою метою, ніж та, з якою вони були зібрані. Персональні дані можуть передаватися іноземним суб'єктам відносин, пов'язаних з персональними даними, також у разі: 1) надання суб'єктом персональних даних однозначної згоди на таку передачу; 2) необхідності укладення чи виконання правочину між володільцем

персональних даних та третьою особою - суб'єктом персональних даних на користь суб'єкта персональних даних; 3) необхідності захисту життєво важливих інтересів суб'єктів персональних даних; 4) необхідності захисту суспільного інтересу, встановлення, виконання та забезпечення правової вимоги; 5) надання володільцем персональних даних відповідних гарантій щодо невтручання в особисте і сімейне життя суб'єкта персональних даних [46].

Передача персональних даних у сфері охорони здоров'я до України здійснюється в межах Конвенції РЄ про захист осіб у зв'язку з автоматизованою обробкою персональних даних від 28 січня 1981 року [63]; Регламенту 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) [53]; національного законодавства окремих країн.

Що стосується інформації про стан здоров'я пацієнта, то на особливу увагу заслуговують встановлені законами (легітимні) умови та підстави для втручання держави в приватне життя пацієнта [118, с. 164].

Так, у ст. 17 Закону України «Про подолання туберкульозу в Україні» передбачено, що інформація стосовно людей, які хворіють на туберкульоз, вноситься до електронної системи охорони здоров'я. Ведення первинної облікової медичної документації стосовно пацієнтів, які хворіють на туберкульоз, здійснюється з дотриманням вимог Закону України «Про захист персональних даних». За згодою людини, яка хворіє на туберкульоз або отримує профілактичне лікування туберкульозу, або її законного представника з метою організації комплексної та всебічної допомоги такій людині можуть надаватися послуги у сфері громадського здоров'я організаціями, що працюють у сфері подолання туберкульозу, в порядку, встановленому центральним органом виконавчої влади, що забезпечує формування та реалізує державну політику у сфері охорони здоров'я. За письмовою інформованою згодою людини, яка хворіє на туберкульоз або отримує профілактичне лікування туберкульозу, або її законного представника відомості про встановлений діагноз і отримуване лікування,

інформація про пацієнта та фактичне місце його перебування можуть передаватися надавачам послуг у сфері громадського здоров'я лише в інтересах та в обсязі, визначеному самим пацієнтом, для захисту його прав і законних інтересів, надання психологічної підтримки, соціального супроводу та правової допомоги, якщо поінформованість про ці обставини має істотне значення для надання такої допомоги [119].

Згідно ст. 13 Закону України «Про протидію поширенню хвороб, зумовлених вірусом імунодефіциту людини (ВІЛ), та правовий і соціальний захист людей, які живуть з ВІЛ» відомості про результати тестування на ВІЛ, про наявність або відсутність в особи ВІЛ-інфекції є конфіденційними та становлять лікарську таємницю. Медичні працівники зобов'язані вживати необхідних заходів для забезпечення дотримання встановленого законодавством порядку зберігання конфіденційної інформації про людей, які живуть з ВІЛ, захисту такої інформації від розголошення та розкриття третім особам. Будь-які особи, яким стала відомою інформація про результати тестування на ВІЛ, зобов'язані не розголошувати її, крім випадків, встановлених законом. Передача медичним працівником цих відомостей дозволяється лише: особі, стосовно якої проведено тестування, батькам чи іншим законним представникам такої особи якщо послуги з тестування на ВІЛ дітей віком до 14 років та осіб, визнаних у встановленому законом порядку недієздатними, надаються на прохання їхніх батьків або законних представників та за наявності усвідомленої інформованої згоди. Батьки та законні представники зазначених осіб мають право бути присутніми під час проведення такого тестування, ознайомлені з його результатами та зобов'язані забезпечити збереження умов конфіденційності даних про ВІЛ-статус осіб, інтереси яких вони представляють; іншим медичним працівникам та закладам охорони здоров'я, фізичним особам – підприємцям, які провадять господарську діяльність з медичної практики, виключно у зв'язку з наданням усіх видів медичної допомоги людям, які живуть з ВІЛ, та закладам громадського здоров'я з метою здійснення епідеміологічного нагляду за ВІЛ-інфекцією; іншим особам – лише за рішенням суду в установлених законом випадках. Передача відомостей

іншим медичним працівникам та закладам охорони здоров'я допускається лише для цілей, пов'язаних з лікуванням хвороб, зумовлених ВІЛ, та у разі якщо поінформованість лікаря щодо ВІЛ-статусу пацієнта має істотне значення для його лікування. За усвідомленою письмовою згодою людини, яка живе з ВІЛ, або її законного представника відомості про ВІЛ-статус можуть передаватися іншим особам лише в її інтересах та в обсязі, визначеному людиною, яка живе з ВІЛ, для захисту її прав і законних інтересів, надання психологічної підтримки, правової допомоги та проведення соціальної роботи, в тому числі надання соціальних послуг, якщо поінформованість щодо ВІЛ-статусу пацієнта має істотне значення для надання такої допомоги. Розкриття медичним працівником відомостей про позитивний ВІЛ-статус особи партнеру (партнерам) дозволяється, якщо: 1) людина, яка живе з ВІЛ, звернеться до медичного працівника з відповідним письмово підтвердженим проханням; 2) людина, яка живе з ВІЛ, померла, знепритомніла або існує ймовірність того, що вона не опритомніє та не відновить свою здатність надавати усвідомлену інформовану згоду [120].

Відповідно до ст. 6 Закону України «Про психіатричну допомогу» право на одержання і використання конфіденційних відомостей про стан психічного здоров'я особи та надання їй психіатричної допомоги має сама особа чи її законний представник. За усвідомленою письмовою згодою особи або її законного представника відомості про стан психічного здоров'я цієї особи та надання їй психіатричної допомоги можуть передаватися іншим особам лише в інтересах особи, яка страждає на психічний розлад, для проведення обстеження та лікування чи захисту її прав і законних інтересів, для здійснення наукових досліджень, публікацій в науковій літературі, використання у навчальному процесі. Допускається передача відомостей про стан психічного здоров'я особи та надання їй психіатричної допомоги без згоди особи або без згоди її законного представника для: 1) організації надання особі, яка страждає на тяжкий психічний розлад, психіатричної допомоги; 2) провадження досудового розслідування, складання досудової доповіді щодо обвинувачених або судового розгляду за письмовим запитом слідчого, прокурора, суду та представника уповноваженого

органу з питань пробації. У листку непрацездатності, що видається особі, яка страждає на психічний розлад, діагноз психічного розладу вписується за згодою цієї особи, а у разі її незгоди - лише причина непрацездатності (захворювання, травма або інша причина). Забороняється без письмової згоди особи або без письмової згоди її законного представника та лікаря-психіатра, який надає психіатричну допомогу, публічно демонструвати особу, яка страждає на психічний розлад, фотографувати її чи робити кінозйомку, відеозапис, звукозапис та прослуховувати співбесіди особи з медичними працівниками чи іншими фахівцями при наданні їй психіатричної допомоги. Забороняється вимагати відомості про стан психічного здоров'я особи та про надання їй психіатричної допомоги, за винятком випадків, передбачених законами. Документи, що містять відомості про стан психічного здоров'я особи та надання їй психіатричної допомоги, повинні зберігатися з додержанням умов, що гарантують конфіденційність цих відомостей. Вилучення оригіналів цих документів та їх копіювання може здійснюватися лише у випадках, встановлених законом [121].

У ч. 2 ст. 26 Закону України «Про захист населення від інфекційних хвороб» встановлено, що відомості про зараження особи інфекційною хворобою, що передається статевим шляхом, проведені медичні огляди та обстеження з цього приводу, дані інтимного характеру, отримані у зв'язку з виконанням професійних обов'язків посадовими особами та медичними працівниками закладів охорони здоров'я, становлять лікарську таємницю. Надання таких відомостей дозволяється у випадках, передбачених законами України [122]. У ч. 1 ст. 26 Закону України «Про захист населення від інфекційних хвороб» передбачено, що облік інфекційних хвороб базується на системі обов'язкової реєстрації кожного їх випадку незалежно від місця і обставин виявлення та оперативного (екстреного) повідомлення про нього закладів охорони здоров'я визначених, центральним органом виконавчої влади, що забезпечує формування державної політики у сфері охорони здоров'я для здійснення протиепідемічних заходів [122].

Вміщення (акумулювання) інформації про здоров'я пацієнта без його згоди у відповідні реєстри, бази та банки даних має розглядатися як втручання у його

приватне життя, тому мета такого втручання має бути визначена окремими законами. В іншому випадку існує реальна загроза широкого застосування адміністративного розсуду з боку посадових осіб під час вирішення питання про співвідношення балансу між приватними та суспільними інтересами. Тому невипадково в рішенні у справі «Z проти Фінляндії» від 25 січня 1997 року [123] ЄСПЛ суд наголосив на основних принципах, які можуть бути застосовані до захисту лікарської таємниці, а саме: внутрішнє законодавство має забезпечити гарантії з тим, щоб перешкодити будь-якому передаванню чи оприлюдненню персональних даних, пов'язаних із здоров'ям, відповідно до гарантій, передбачених ст. 8 Конвенції про захист прав людини і основоположних свобод [124]. Разом із тим під час аналізу вітчизняного законодавства в цій царині впадають в око різні підходи до встановлення підстав та порядку здійснення такого втручання, кола третіх осіб, а також надання по суті необмежених повноважень МОЗ України щодо регулювання відносин, які виникають у зазначеній сфері тощо [118, с. 165].

Контроль за додержанням законодавства про захист персональних даних, в тому числі у сфері охорони здоров'я, здійснюють Уповноважений Верховної Ради України з прав людини та суди. Перелік повноважень Уповноваженого Верховної Ради України з прав людини у сфері захисту персональних даних визначено у ст. 23 Закону України «Про захист персональних даних» [46]. Порядок здійснення Уповноваженим Верховної Ради України з прав людини контролю за додержанням законодавства про захист персональних даних регламентовано наказом Уповноваженого Верховної Ради України з прав людини від 8 січня 2014 року № 1/02-14 [87].

За порушення законодавства про захист персональних даних, в тому числі у сфері охорони здоров'я, передбачена адміністративна (ст. 188^{39} «Порушення законодавства у сфері захисту персональних даних» і ст. 188^{40} «Невиконання законних вимог Уповноваженого Верховної Ради України з прав людини» КУпАП) [72] та кримінальна відповідальність (ст. 182 «Порушення недоторканності приватного життя» КК України) [73].

Отже, обробка персональних даних у сфері охорони здоров'я здійснюється за умови надання пацієнтом однозначної згоди на обробку таких даних або на підставі закону. Обробка персональних даних у сфері охорони здоров'я без згоди пацієнта здійснюється: 1) коли медичні відомості необхідні в цілях охорони здоров'я; 2) для захисту життєво важливих інтересів суб'єкта персональних даних. Обробляти персональні дані без згоди пацієнта можна до часу, коли отримання згоди стане можливим. Обмеження щодо обробки персональних даних у сфері охорони здоров'я може здійснюватися у випадках, передбачених законом, наскільки це необхідно у демократичному суспільстві в інтересах національної безпеки, економічного добробуту або захисту прав і свобод суб'єктів персональних даних чи інших осіб. Законодавством про захист персональних даних регламентовано умови захисту персональних даних у сфері охорони здоров'я володільцями, розпорядниками, третіми особами, у разі транскордонної передачі таких даних, а також передбачено здійснення контролю за додержанням законодавства про захист персональних даних та встановлено юридичну відповідальність за порушення законодавства про захист персональних даних, в тому числі у сфері охорони здоров'я. Втім, необхідно відмітити, що окремі положення законодавства про захист персональних даних та охорону здоров'я щодо захисту фізичних осіб у зв'язку з обробкою медичних даних потребують удосконалення, що зумовлено відсутністю чіткого розуміння конструкції «захист персональних даних», необхідністю унормування ст. 7 та ст. 11 Закону України «Про захист персональних даних» стосовно умов обробки персональних даних, прогресом інформаційних технологій, необхідністю оновлення Закону України «Про захист персональних даних» відповідно до вимог Загального регламенту захисту персональних даних ЄС від 27 квітня 2016 року № 2016/679 [117, с. 674].

2.2. Суб'єкти забезпечення захисту персональних даних у сфері охорони здоров'я

Сьогодні захист персональних даних, у тому числі у сфері охорони здоров'я, є одним із пріоритетних напрямів діяльності держави. Ключовим елементом забезпечення захисту персональних даних у сфері охорони здоров'я є відповідна система суб'єктів. Ефективне функціонування таких суб'єктів неможливе без належним чином відпрацьованих механізмів їх діяльності. Тому актуальним питанням є встановлення кола суб'єктів забезпечення захисту персональних даних у сфері охорони здоров'я та з'ясування правових засад їх діяльності.

Суб'єкт – це особа, що має свідомість і волю, здатність до цілеспрямованої діяльності, скерованої на той чи інший суб'єкт; особа або група осіб, колектив, організація, які є активними діячами у якому-небудь акті, процесі; людина як носій яких-небудь властивостей; особа чи організація, які мають певні права та обов'язки [125, с. 728; 126, с. 634]. Суб'єктами відносин у сфері захисту медичних даних є реальні учасники цих відносин.

У ч. 1 ст. 4 Закону України «Про захист персональних даних» передбачено, що суб'єктами відносин, пов'язаних із персональними даними, є: суб'єкт персональних даних; володілець персональних даних; розпорядник персональних даних; третя особа; Уповноважений Верховної Ради України з прав людини [46].

Суб'єкт персональних даних – це фізична особа, персональні дані якої обробляються [46]. У сфері охорони здоров'я суб'єктом персональних даних є пацієнт – фізична особа, яка звернулася за медичною та/або реабілітаційною допомогою або медичною послугою та/або якій така допомога або послуга надається [36]. Пацієнт отримує статус суб'єкта персональних даних у сфері охорони здоров'я при здійсненні процедури його ідентифікації. Слід зазначити, що пацієнт не відноситься до суб'єктів забезпечення захисту персональних даних у сфері охорони здоров'я, оскільки він не наділений конкретним, визначеним на законодавчому рівні обсягом повноважень, тобто не має юридичного обов'язку щодо здійснення діяльності із забезпечення захисту медичних даних, а має

виключно права, встановлені ч. 2 ст. 8 Закону України «Про захист персональних даних» [46] та ст. 6 Закону України «Основи законодавства України про охорону здоров'я» [36].

Згідно ст. 2 Закону України «Про захист персональних даних» володілець персональних даних – це фізична або юридична особа, яка визначає мету обробки персональних даних, встановлює склад цих даних та процедури їх обробки, якщо інше не визначено законом [46]. Відповідно до Конвенції про захист осіб у зв'язку з автоматизованою обробкою персональних даних від 28 січня 1981 року володілець («контролер») – це фізична або юридична особа, державний орган, установа чи будь-яка інша установа, що уповноважена відповідно до національного законодавства вирішувати, якою повинна бути мета файлу даних для автоматизованої обробки, які категорії персональних даних повинні зберігатися та які операції повинні виконуватися з ними [63]. У ст. 4 Регламенту Європейського парламенту і Ради (ЄС) 2016/679 від 27 квітня 2016 року володілець («контролер») трактується як фізична чи юридична особа, орган публічної влади, агентство чи інший орган, який самостійно чи спільно з іншими визначає цілі та засоби опрацювання персональних даних [53]. Володільцем персональних даних можуть бути підприємства, установи і організації усіх форм власності, органи державної влади чи органи місцевого самоврядування, фізичні особи – підприємці, які обробляють персональні дані відповідно до закону [46]. З наведених визначень слідує, що володілець персональних даних є обов'язковим учасником відносин, пов'язаних із захистом і обробкою персональних даних, та суб'єктом забезпечення захисту персональних даних, оскільки він безпосередньо визначає мету обробки персональних даних, встановлює склад цих даних та процедури їх обробки.

Законодавство України про охорону здоров'я до володільців персональних даних у сфері охорони здоров'я дає підстави віднести органи публічної влади, заклади охорони здоров'я (будь-якої форми власності та організаційно-правової форми або її відокремлений підрозділ), фізичних осіб – підприємців, діяльність яких пов'язана з медичним обслуговуванням.

Так, відповідно до Порядку функціонування електронної системи охорони здоров'я, затвердженого постановою КМ України від 25 квітня 2018 року № 411, володільцем відомостей реєстру є уповноважений орган державної влади, який визначає мету та порядок обробки даних у відповідному реєстрі центральної бази даних. Володільцем відомостей Реєстру медичних спеціалістів, Реєстру суб'єктів господарювання у сфері охорони здоров'я, Реєстру медичних висновків є МОЗ України [94]. Слід зазначити, що МОЗ України також є володільцем інших інформаційних систем у сфері охорони здоров'я. Наприклад, МОЗ України є володільцем персональних даних, що містяться в інформаційній системі «Моніторинг соціально значущих хвороб» (комплекс засобів, який дає змогу автоматизувати роботу суб'єктів господарювання, що здійснюють профілактику, діагностику та лікування соціально значущих хвороб, реєстрацію та облік пацієнтів із соціально значущими хворобами) [127]. У Порядку функціонування електронної системи охорони здоров'я, затвердженого постановою КМ України від 25 квітня 2018 року № 411, встановлено, що володільцем інших реєстрів та їх відомостей є НСЗУ [94]. Наприклад, НСЗ України є володільцем персональних даних, які містяться в Реєстрі пацієнтів [103].

МОЗ України є головним органом у системі центральних органів виконавчої влади, що забезпечує формування та реалізує державну політику у сфері охорони здоров'я, а також захисту населення від інфекційних хвороб, протидії ВІЛ-інфекції/СНІДу та іншим соціально небезпечним захворюванням, попередження та профілактики неінфекційних захворювань, забезпечує формування та реалізує державну політику у сферах: епідеміологічного нагляду (спостереження), імунопрофілактики, промоції здорового способу життя, відповідального ставлення до свого здоров'я та запобігання факторам ризику, попередження та зниження рівня вживання тютюнових виробів і їх шкідливого впливу на здоров'я населення, безпеки харчових продуктів, регламентації факторів середовища життєдіяльності населення, гігієнічної регламентації небезпечних факторів, створення національної системи крові, управління системою якості щодо безпеки крові, біологічної безпеки та біологічного захисту, боротьби із стійкістю до

протимікробних препаратів, реагування на небезпеки для здоров'я та надзвичайні стани в сфері охорони здоров'я, а також забезпечення формування державної політики у сферах санітарного та епідемічного благополуччя населення; розвитку медичних послуг, забезпечення державних фінансових гарантій медичного обслуговування населення; технічного регулювання медичних виробів, медичних виробів для діагностики in vitro, активних медичних виробів, які імплантують, косметичної продукції; забезпечення населення якісними, ефективними та безпечними лікарськими засобами, створення, виробництва, контролю якості та реалізації лікарських засобів, медичних імунобіологічних препаратів, обігу наркотичних засобів, психотропних речовин, їх аналогів і прекурсорів, протидії їх незаконному обігу, а також безпечних медичних виробів та косметичної продукції; розвитку кадрового потенціалу системи охорони здоров'я, вищої медичної, фармацевтичної освіти та науки [128].

Міністр охорони здоров'я та уповноважені ним посадові особи МОЗ України у межах своїх повноважень в електронній системі охорони здоров'я мають право: 1) реєструвати у центральній базі даних себе, МОЗ України та уповноважених осіб МОЗ України, вносити зміни до відповідних відомостей; 2) створювати, вносити, переглядати інформацію та документи у реєстрах, розпорядником яких є МОЗ України, вносити зміни та доповнення до них з дотриманням вимог Закону України «Про захист персональних даних» [94].

НСЗ України є центральним органом виконавчої влади, діяльність якого спрямовується і координується КМ України через Міністра охорони здоров'я, який реалізує державну політику у сфері державних фінансових гарантій медичного обслуговування населення. Основними завданнями НСЗ України є: 1) реалізація державної політики у сфері державних фінансових гарантій медичного обслуговування населення за програмою державних гарантій медичного обслуговування населення (програма медичних гарантій); 2) виконання функцій замовника медичних послуг, лікарських засобів та медичних виробів за програмою медичних гарантій та за бюджетними програмами, розпорядником яких є НСЗ України; 3) внесення на розгляд Міністра

охорони здоров'я пропозицій щодо забезпечення формування державної політики у сфері державних фінансових гарантій медичного обслуговування населення [129].

Серед інших покладених на НСЗ України завдань, зокрема, у сфері захисту медичних даних, доцільно виділити такі: отримує та обробляє необхідні для здійснення своїх повноважень персональні дані та іншу інформацію про пацієнтів (у тому числі інформацію про стан здоров'я, діагноз, відомості, одержані під час медичного обстеження пацієнтів), надавачів медичних послуг, суб'єктів господарювання, які провадять господарську діяльність на підставі ліцензії на провадження господарської діяльності з роздрібної торгівлі лікарськими засобами та уклали договір про реімбурсацію, незалежно від форми власності та підпорядкування з дотриманням вимог Закону України «Про захист персональних даних»; забезпечує функціонування електронної системи охорони здоров'я, визначає напрями її розвитку, проводить верифікацію даних у системі, затверджує технічні вимоги до електронних медичних інформаційних систем; забезпечує ведення реєстрів, що входять до складу електронної системи охорони здоров'я, інших державних електронних баз та реєстрів, інших інформаційних систем у сфері, що належить до її компетенції; надає особі інформацію про неї, що міститься в електронній системі охорони здоров'я, та відомості про осіб, які подавали запити щодо зазначеної інформації відповідно до законодавства; опубліковує на своєму офіційному веб-сайті дані, накопичені в електронній системі охорони здоров'я, за умови знеособлення персональних даних відповідно до вимог Закону України «Про захист персональних даних» в обсязі та в порядку, встановлених КМ України [129].

Голова НСЗ України та уповноважені ним посадові особи НСЗ України у межах своїх повноважень в електронній системі охорони здоров'я мають право: 1) реєструвати у центральній базі даних себе, НСЗ України та уповноважених осіб НСЗ України, вносити зміни до відповідних відомостей; 2) вчиняти дії щодо укладення, зміни та припинення договорів за програмою медичних гарантій; 3) отримувати доступ до інформації про дії, вчинені адміністратором, що

стосуються електронної системи охорони здоров’я, запитувати та отримувати від адміністратора пояснення щодо вчинених дій, що стосуються електронної системи охорони здоров’я; 4) отримувати від адміністратора інформацію та документи щодо підключення, відключення, зупинення доступу електронної медичної інформаційної системи до центральної бази даних, інформації про результати тестування електронної медичної інформаційної системи; 5) подавати запити та отримувати доступ до даних про пацієнта, що містяться у центральній базі даних, у цілях охорони здоров’я, встановлення медичного діагнозу, забезпечення лікування або надання медичних послуг, функціонування електронної системи охорони здоров’я, якщо на таку особу покладено обов’язки щодо забезпечення захисту персональних даних у разі надання пацієнтом (його законним представником) на це згоди або без такої згоди у випадках, передбачених законом; 6) створювати, вносити, переглядати інформацію та документи у центральній базі даних, вносити зміни та доповнення до них з дотриманням вимог Закону України «Про захист персональних даних»; 7) реєструвати у центральній базі даних уповноважених посадових осіб Національного антикорупційного бюро в порядку, визначеному протоколом взаємодії між НСЗ України та Національним антикорупційним бюро [94].

Законом України «Основи законодавства України про охорону здоров’я» встановлено, що НСЗ України під час забезпечення функціонування електронної системи охорони здоров’я та здійснення інформаційної взаємодії між центральною базою даних цієї системи та іншими відповідними державними інформаційними електронними ресурсами забезпечує захист центральної бази даних електронної системи охорони здоров’я від несанкціонованого доступу до інформації щодо пацієнта, захист персональних даних пацієнтів відповідно до законів України «Основи законодавства України про охорону здоров’я», «Про захист інформації в інформаційно-комунікаційних системах», «Про захист персональних даних», міжнародних договорів у сфері захисту інформації, згода на обов’язковість яких надана ВР України [36].

Варто звернути увагу на те, що володільцем персональних даних у сфері охорони здоров’я можуть бути також інші органи публічної влади.

У ч. 1 ст. 41 Закону України «Про реабілітацію осіб з інвалідністю в Україні» встановлено, що інформаційні ресурси у сфері реабілітації осіб з інвалідністю формуються у вигляді централізованого банку даних з проблем інвалідності, що містить дані про реабілітаційні заклади, характер і причини інвалідності, освітній і професійний рівень осіб з інвалідністю, дітей з інвалідністю, склад сім'ї, рівень доходів, потребу і забезпечення допоміжними засобами реабілітації, медичними виробами, реабілітаційними послугами, санаторно-курортним лікуванням, автомобілем тощо [130]. Відповідно до ч. 2 ст. 41 цього Закону інформаційні ресурси у сфері реабілітації осіб з інвалідністю формуються і підтримуються в межах своїх повноважень: на центральному рівні – центральними органами виконавчої влади, які беруть участь у здійсненні державної політики у сфері реабілітації осіб з інвалідністю; на місцевому рівні – органами виконавчої влади Автономної Республіки Крим, відповідними підрозділами обласних, Київської та Севастопольської міських, районних, районних у містах Києві та Севастополі державних адміністрацій та органами місцевого самоврядування [130].

Відповідно до п. 3 Положення про централізований банк даних з проблем інвалідності, затвердженого постановою КМ України від 16 лютого 2011 року № 121, користувачами банку даних є органи виконавчої влади, органи місцевого самоврядування, Фонд соціального захисту осіб з інвалідністю та його територіальні відділення, державна служба зайнятості, підприємства, що виготовляють, постачають і ремонтують технічні та інші засоби реабілітації, що призначені для безоплатного забезпечення осіб з інвалідністю, дітей з інвалідністю, інших осіб за рахунок коштів державного бюджету, та відповідають кваліфікаційним вимогам, установленим Міністерством соціальної політики України, реабілітаційні установи, суб’єкти, що надають соціальні послуги, та інші установи, організації, що забезпечують функціонування та ведення банку даних у межах своїх повноважень [131].

У п. 9 цього Положення встановлено, що держателем банку даних є Міністерство соціальної політики України. Цей орган виконавчої влади забезпечує підтримку, оновлення, адміністрування, модернізацію, доопрацювання банку даних. Адміністратором банку даних є державне підприємство «Інформаційно-обчислювальний центр Міністерства соціальної політики України», яке здійснює заходи із супроводження програмного забезпечення банку даних, відповідає за його технічне забезпечення, збереження та захист даних банку даних, технічні та технологічні заходи з надання, блокування анулювання доступу до банку даних на запит Фонду соціального захисту осіб з інвалідністю, пошук і відбір даних для підготовки аналітичних звітів, ведення довідників банку даних [131].

Необхідно зазначити, що Положенням про централізований банк даних з проблем інвалідності передбачено держателя, користувачів, адміністратора банку даних, однак у цьому Положенні нічого не зазначено про володільця банку даних. Враховуючи, що відповідно до ч. 4 ст. 41 Закону України «Про реабілітацію осіб з інвалідністю в Україні» на підставі даних інформаційних ресурсів органи виконавчої влади здійснюють соціальний моніторинг, планування і прогнозування потреб осіб з інвалідністю, дітей з інвалідністю у допоміжних засобах реабілітації, медичних виробах та реабілітаційних послугах [130], можна констатувати, що саме КМ України як вищий орган у системі органів виконавчої влади [132] і є володільцем персональних даних у централізованому банку. Решта названих суб’єктів лише розпорядники – роль кожного з них у забезпеченні функціонування банку даних та обробки наявних у ньому відомостей визначена КМ України [133, с. 34].

Загалом же при визначенні того, хто володілець, якщо, звісно, його не визначено законом, необхідно виходити з реальних повноважень того чи іншого суб’єкта. Окрім того, слід зазначити, що залежно від наявних повноважень, володільців персональних даних може бути декілька. Очевидно, що якщо одні і ті ж дані окремо зберігаються в кількох суб’єктів (наприклад, юридичних осіб), і кожен з них наділений повноваженнями володільця, то кожен з них незалежний

один від одного володілець. Наприклад, одна компанія передає (чи продає) базу персональних даних своїх клієнтів іншій компанії. Після цього кожна з вказаних компаній незалежно одна від одної продовжують використовувати цю базу даних для власних потреб. Отже, кожна з них володілець наявних у цих базах персональних даних. Якщо ж двоє чи більше володільців з огляду на спільні потреби створюють єдину базу персональних даних (спільно визначають мету, склад даних, порядок їх обробки), то їх слід вважати співволодільцями. Саме про це йде мова у ст. 4 Регламенту Європейського парламенту і Ради (ЄС) 2016/679 від 27 квітня 2016 року (володілець («контролер») – це фізична чи юридична особа, орган публічної влади, агентство чи інший орган, який самостійно чи спільно з іншими визначає цілі та засоби опрацювання персональних даних) [53]. При цьому, не важливо, чи мають вони рівний доступ до таких даних чи різний, вони залишаються їхніми співволодільцями [133, с. 36-37].

Разом з тим доволі поширені і ситуації, коли двоє чи більше суб'єктів частково здійснюють повноваження володільця, тобто кожен з них частково визначає мету обробки, склад персональних даних і порядок їх обробки. У такому разі кожен з них також співволоділець, однак кожен з них нестиме відповідальність лише тією мірою, якою він відповідальний за здійснення повноважень володільця [133, с. 38].

Так, у п. 20 Порядку функціонування електронної системи охорони здоров'я, затвердженого постановою КМ України від 25 квітня 2018 року № 411, передбачено, які відомості вносяться до реєстрів в електронній системі охорони здоров'я. Однак щодо кожного з реєстрів перелік даних не вичерпний та закінчується пунктом, де йдеться про «інші відомості, визначені МОЗ України» [133, с. 39]. У п.п. 10 п. 20 цього Порядку передбачено можливість створення інших реєстрів, набір даних, у яких визначає НСЗ України. Розпорядники реєстрів та володільці їх відомостей, перелік відомостей, що вноситься до них, а також порядок їх ведення затверджуються МОЗ України [94]. У п. 21 цього Порядку встановлено, що особливості ведення окремих реєстрів, у тому числі відомості, що вносяться до таких реєстрів, та права доступу користувачів до інформації у

таких реєстрах, затверджуються МОЗ України [94]. Розширений список відомостей про особу, що підлягає внесенню до Реєстру пацієнтів, визначено Порядком ведення Реєстру пацієнтів в електронній системі охорони здоров'я, який затверджений наказом МОЗ України від 30 листопада 2020 року № 2755 [103]. Отже, КМ України та МОЗ України – співволодільці Реєстру пацієнтів, оскільки кожен із цих органів державної влади визначає окремі аспекти обробки персональних даних у цьому Реєстрі. Однак кожен з них відповідає лише за ті аспекти обробки персональних даних, які ним визначені. Якщо на виконання п.п. 10 п. 20 Порядку функціонування електронної системи охорони здоров'я, затвердженого постановою КМ України від 25 квітня 2018 року № 411, НСЗ України та МОЗ України будуть створені інші реєстри, то співволодільцями наявних у них даних будуть як КМ України, так і МОЗ України та НСЗ України [133, с. 39].

Володільцями персональних даних у сфері охорони здоров'я також можуть бути заклади охорони здоров'я приватної власності або їх відокремлені підрозділи та фізичні особи – підприємці, діяльність яких пов'язана з медичним обслуговуванням. Електронні медичні інформаційні системи таких суб'єктів забезпечення захисту персональних даних у сфері охорони здоров'я повинні відповідати технічним вимогам центральної бази даних електронної системи охорони здоров'я.

Для підключення електронної медичної інформаційної системи до центральної бази даних оператор подає адміністратору відповідну заявку, до якої додаються: відомості та документи (у разі наявності), що підтверджують право власності на електронну медичну інформаційну систему, право на підключення такої системи до центральної бази даних (крім оператора, який є технічним адміністратором Порталу Дія); технічні характеристики електронної медичної інформаційної системи; відомості про обсяг функціональних можливостей електронної медичної інформаційної системи для роботи в електронній системі охорони здоров'я; виписка з Єдиного державного реєстру юридичних осіб, фізичних осіб – підприємців та громадських формувань про такого оператора. Для

встановлення відповідності електронної медичної інформаційної системи технічним вимогам адміністратор проводить протягом 30 календарних днів з дня подання заявки оператором тестування електронної медичної інформаційної системи відповідно до тестової програми, що розробляється адміністратором та затверджується НСЗ України. За результатами тестування адміністратор оформляє висновок та надсилає його оператору протягом трьох робочих днів. У разі встановлення невідповідності електронної медичної інформаційної системи технічним вимогам висновок повинен містити опис таких невідповідностей та пропозиції щодо їх усунення. Оператор має право повторно подати електронну заявку адміністратору після усунення невідповідностей. У разі встановлення відповідності електронної медичної інформаційної системи технічним вимогам адміністратор укладає з оператором договір про підключення до центральної бази даних для визначеного обсягу функціональних можливостей для роботи в електронній системі охорони здоров'я. Адміністратор оприлюднює на веб-сайті системи протягом п'яти робочих днів з дати укладення договору інформацію про підключені до центральної бази даних електронні медичні інформаційні системи та їх функціональні можливості в електронній системі охорони здоров'я, операторів, з якими адміністратор уклав договір [94].

У разі переходу права власності на електронну медичну інформаційну систему, підключену до центральної бази даних, права на підключення такої системи до центральної бази даних або заміни технічного адміністратора Порталу Дія новий оператор має право протягом 10 робочих днів з дня переходу відповідних прав або заміни технічного адміністратора Порталу Дія звернутися до адміністратора щодо укладення нового договору. До заявки додаються такі ж документи, які необхідні для підключення електронної медичної інформаційної системи. Повторне тестування електронної медичної інформаційної системи у такому випадку не проводиться. У разі незвернення нового оператора у встановлений строк електронна медична інформаційна система відключається від центральної бази даних [94].

Рішення про зупинення доступу електронної медичної інформаційної системи до центральної бази даних або відключення такої системи від центральної бази даних приймає адміністратор у разі наявності хоча б однієї з таких підстав: 1) добровільного подання оператором заяви про відключення електронної медичної інформаційної системи від центральної бази даних; 2) порушення оператором вимог щодо забезпечення захисту інформації, у тому числі щодо забезпечення цілісності, доступності, конфіденційності та розмежування доступу до даних, внесених до електронної системи охорони здоров'я; 3) встановлення Державною службою спеціального зв'язку та захисту інформації України порушення оператором вимог законодавства щодо криптографічного та технічного захисту інформації; 4) встановлення за результатами тестування невідповідності електронної медичної інформаційної системи технічним вимогам; 5) відсутності в оператора права власності на електронну медичну інформаційну систему, права на підключення електронної медичної інформаційної системи до центральної бази даних або заміни технічного адміністратора Порталу Дія; 6) відсутності більше ніж 24 години у користувачів електронної медичної інформаційної системи доступу до центральної бази даних внаслідок технічних проблем такої системи; 7) порушення оператором умов договору, укладеного з адміністратором; 8) незвернення нового оператора до адміністратора про укладення договору протягом 10 робочих днів. У разі зупинення доступу електронної медичної інформаційної системи до центральної бази даних такий доступ відновлюється адміністраторам після усунення виявлених порушень [94].

Адміністратором центральної бази даних електронної системи охорони здоров'я є державне підприємство «Електронне здоров'я» [134], яке відповідає за: 1) адміністрування та технічну підтримку центральної бази даних з метою забезпечення безперебійної роботи центральної бази даних; 2) прийняття рішення про підключення, відключення та зупинення доступу електронної медичної інформаційної системи до центральної бази даних, укладення та припинення відповідних договорів з операторами; 3) надання технічної підтримки операторам

з питань підключення, відключення, взаємодії електронної медичної інформаційної системи з центральною базою даних, підтверджує впровадження нових функціональних можливостей системи; 4) надання інформаційних та консультаційних послуг щодо електронної системи охорони здоров'я; 5) розроблення та підтримання в актуальному стані технічної документації центральної бази даних. Адміністратор не здійснює обробку персональних даних пацієнтів [94].

Керівник суб'єкта господарювання у сфері охорони здоров'я та фізична особа – підприємець, яка одержала ліцензію на провадження господарської діяльності з медичної практики мають право: 1) реєструвати у центральній базі даних суб'єкта господарювання у сфері охорони здоров'я та уповноважених осіб такого суб'єкта господарювання, вносити зміни до відповідних відомостей у Реєстрі суб'єктів господарювання у сфері охорони здоров'я; 2) вчиняти дії для укладення, зміни та припинення договорів за програмою медичних гарантій; 3) формувати та подавати НСЗ України електронні звіти через електронну систему охорони здоров'я; 4) здійснювати дії для припинення доступу до центральної бази даних уповноважених осіб суб'єкта господарювання у сфері охорони здоров'я та медичних працівників; 5) переглядати інформацію, що внесена працівниками до електронної системи охорони здоров'я з урахуванням вимог Закону України «Про захист персональних даних»; 6) передавати та переглядати оперативну інформацію в режимі он-лайн та інформацію про наявні ресурси мережі екстреної медичної допомоги в частині функціонування електронної медичної інформаційно-аналітичної системи з оптимізації роботи оперативно-диспетчерських служб центрів екстреної медичної допомоги та медицини катастроф [94].

Прикладами електронних медичних інформаційних систем, володільцями яких є суб'єкти забезпечення захисту персональних даних у сфері охорони здоров'я приватної форми власності, є Helsi [135], Medcard24 [136], Moniheal [137], Health24 [138], Askep [139] тощо.

Загалом усі електронні медичні інформаційні системи збирають приблизно однакові дані, проте в угодах про це зазначено по-різному. І не завжди чітко і вичерпно. Сервіс Helsi зазначає, що збирає як загальні дані про особу, так і чутливі дані про стан здоров'я. Medcard24 збирає загальні дані, проте не конкретизує, які саме, а відсилає до Закону України «Про захист персональних даних». Водночас, чітко прописано, що сервіс збирає дані, що містять лікарську таємницю: факт звернення до лікаря, медичні послуги, препарати, які необхідні чи можуть такими бути для пацієнта тощо. А ось з сервісом Health24 складніше. В угоді чітко вказано на загальні дані, які збираються. Проте жодного слова про медичні дані. Хоча сервіс призначений як для лікарів, так і для пацієнтів, на ньому є можливість записатися на прийом до лікаря, тож факт запису і звернення сервіс обробляє. А це лікарська таємниця. Сервіс Askep також має проблеми. У розділі про дані, які збирає сервіс, зазначено: «Аскеп збирає дані, щоб ефективно керувати своїми продуктами та надавати вам найкращі можливості для роботи з ними. Деякі дані ви надаєте напряму, наприклад, коли створюєте обліковий запис в системі Аскеп, адмініструєте обліковий запис, надсилаєте на eHealth інформацію про заклад, лікаря, пацієнта, декларації». Це аж ніяк не можна вважати інформуванням користувачів про зміст і склад даних, які збираються. Медсервіси повинні доопрацювати свої угоди, аби пацієнт, який реєструється в сервісі, чітко розумів що саме про нього буде знати сервіс. Медичні сервіси є посередниками між пацієнтом і системою охорони здоров'я. Вони обмінюються даними між лікарями, клініками, органами охорони здоров'я з одного боку і пацієнтами з іншого. Закон України «Про захист персональних даних» передбачає обов'язок у момент збору повідомляти суб'єкту даних, кому передаються його дані [140].

Необхідно відмітити, що кожен медсервіс повинен в угодах з користувачем зазначити інформацію щодо передання персональних даних. На практиці, такі зазначення дійсно є, проте вони не завжди є чіткими та вичерпними. Так, Helsi дає вичерпний список суб'єктів, яким може передавати дані користувача: володільцям, які ведуть медичні реєстри або інші реєстри, куди має бути передана

відповідна інформація, медзакладам та лікарям, тим, кому сам користувач дозволив доступ до даних. Також вказано, що медзаклади-користувачі Helsi, можуть передавати дані контролюючим органам, згідно з законодавством. Такий самий перелік надає і сервіс Health24. Сервіс Medcard24 не містить переліку. В умовах обробки персональних даних зазначено, що сервіс має право передавати персональні дані, а користувач має право отримувати інформацію про третіх осіб, яким вони передаються. Сервіс навіть не окреслює можливі категорії осіб, кому може передати дані. У Типовому порядку обробки персональних даних Уповноваженого Верховної Ради України з прав людини зазначено, що володілець даних, яким Medcard24 і є, визначає саме перелік третіх осіб, яким може передати їх. Тож такий перелік має бути в угоді. Угода з Moniheal передбачає, що система може «розкривати деякі ваші персональні дані» не лише органам, які мають право законно вимагати дані (органи слідства, прокуратури, суди), а й на вимогу «посадових осіб будь-якого державного органу, або якщо ми вважаємо, що розкриття необхідне або доцільне для запобігання заподіянню шкоди здоров'ю або фінансових збитків». Це суперечить практиці ЄСПЛ. Згідно з рішенням у справі «Gardel v. France» («Гардел проти Франції») від 17 грудня 2009 року [141], доступ до персональних даних у реєстрах можуть отримувати тільки ті публічні службовці, які несуть офіційний обов'язок зберігати конфіденційність інформації. Ніяк не «будь-які». До того ж такий доступ повинен здійснюватися лише з конкретною законною метою (слідство, захист населення, державна безпека тощо). Також Moniheal залишає за собою право передати «будь-які наявні у нас ваші персональні дані у разі повного або часткового продажу або передачі Товариства чи його активів». Відтак, обіцяють «докласти розумних зусиль», щоб правонаступник використовував дані за тими ж правилами. Якщо дані пацієнтів оброблятиме правонаступник без згоди суб'єкта даних і не у визначений спосіб, це вважатиметься порушенням [140].

Електронні медичні інформаційні системи, володільцями яких є суб'єкти охорони здоров'я приватної форми власності, як правило, зберігають дані пацієнтів на хмарних сервісах. Закон України «Про захист інформації в

інформаційно-телекомунікаційних системах» зобов'язує здійснювати обробку даних з обмеженим доступом (це і медичні дані) виключно в системі із застосуванням комплексної системи захисту інформації з підтвердженою відповідністю. Ця відповідність, своєю чергою, повинна підтверджуватися позитивним висновком державної експертизи. Відповідальність перед пацієнтами несуть володільці електронних медичних інформаційних систем, адже з ними пацієнт укладає угоду. Вони повинні бути впевнені у спроможності хмарних сховищ. Наприклад, сервіс Health24 зберігає дані пацієнтів в організації ТОВ «ДЕ НОВО» і опублікував атестат відповідності організації на своєму сайті. Також в «ДЕ НОВО» зберігає дані медичний сервіс Medcard24. Helsi зберігає дані в базі персональних даних «Хелсі», відповідно цей медсервіс сам повинен відповідати встановленим вимогам і мати документи відповідності. На сайті компанії відсутній атестат, проте в реальності він є. На тендері Prozzoro сервіс опублікував файл атестату 2020 року. Так само свою базу даних має сервіс Infomed, на сайті якого розміщений й атестат відповідності. Закон України «Про захист персональних даних» встановлює право людини знати про місцезнаходження персональних даних. Сервіс Askep, приміром, цієї вимоги не дотримується. У правилах конфіденційності зазначено, що дані зберігаються в хмарному сервісі, а організація, яка забезпечує хостинг, гарантує безпеку. Проте найменування компанії і юридичної адреси немає [140].

Слід також зазначити, що можливість спільної обробки медичних даних допускаються і в приватному секторі, де кілька суб'єктів господарювання у сфері охорони здоров'я можуть спільно вести бази персональних даних. Жодним положенням Закону України «Про захист персональних даних» цього не заборонено, а наведені вище приклади з публічного сектору це лише підтверджують. Однак у такому разі суб'єкти господарювання у сфері охорони здоров'я повинні подбати про те, щоб належним чином розмежувати свої повноваження щодо обробки персональних даних, співволодільцями яких вони виступають. Найлогічнішим видається оформити такі відносини договором. Варто звернути увагу на те, що поняття «співволоділець» відсутнє в українському

законодавстві, однак воно існує на практиці, що підтверджується відповідними прикладами. Про особливості діяльності та розмежування повноважень співволодільців йдеться у ст. 47 Регламенту Європейського парламенту і Ради (ЄС) 2016/679 від 27 квітня 2016 року [53]. Тому видається доцільним врегулювати такі ситуації і в Законі України «Про захист персональних даних» [133, с. 39-40].

Згідно ст. 2 Закону України «Про захист персональних даних» розпорядник персональних даних – це фізична чи юридична особа, якій володільцем персональних даних або законом надано право обробляти ці дані від імені володільця [46]. У ст. 4 Регламенту Європейського парламенту і Ради (ЄС) 2016/679 від 27 квітня 2016 року розпорядник (оператор) трактується як фізична чи юридична особа, орган публічної влади, агентство чи інший орган, який обробляє персональні дані від імені володільця (контролера) [53]. Розпорядником персональних даних можуть бути підприємства, установи і організації усіх форм власності, органи державної влади чи органи місцевого самоврядування, фізичні особи – підприємці, які обробляють персональні дані відповідно до закону [46]. При цьому, зауважимо, що розпорядником персональних даних, володільцем яких є орган публічної влади, крім цих органів, може бути лише підприємство державної або комунальної форми власності [46]. Володілець персональних даних може доручити обробку персональних даних розпоряднику персональних даних відповідно до договору, укладеного в письмовій формі [46]. Розпорядник персональних даних може обробляти персональні дані лише з метою і в обсязі, визначених у договорі [46].

Доцільно звернути увагу на те, що на відміну від Закону України «Про захист персональних даних» Регламент Європейського парламенту і Ради (ЄС) 2016/679 від 27 квітня 2016 року детальніше регламентує особливості співробітництва між володільцем та розпорядником персональних даних. Так, відповідно до ст. 28 Регламент Європейського парламенту і Ради (ЄС) 2016/679 від 27 квітня 2016 року у разі здійснення обробки персональних даних від імені володільця (контролера), володілець (контролер) повинен залучити лише таких

розпорядників (операторів), які надають достатні гарантії стосовно вжиття необхідних технічних і організаційних заходів та захисту прав суб'єкта персональних даних. Розпорядник (оператор) не повинен залучати будь-якого додаткового розпорядника (оператора) без отримання попереднього спеціального чи загального письмового дозволу володільця (контролера). У випадку загального письмового дозволу, розпорядник (оператор) повинен повідомити володільця (контролера) про будь-які цілеспрямовані зміни щодо залучення додаткового чи заміни інших розпорядників (операторів), таким чином надаючи володільцю (контролеру) можливість заперечити проти таких змін. Відносини між володільцем (контролером) і розпорядником (оператором) регулюються договором (може бути оформлений в письмовій чи електронній формі) або нормативно-правовим актом відповідно до законодавства ЄС. У разі залучення розпорядником (оператором) додаткового розпорядника (оператора – суброзпорядника) до здійснення обробки персональних даних від імені володільця (контролера), умови щодо захисту персональних даних є такими самими, які встановлено між володільцем (контролером) і розпорядником (оператором). Якщо такий додатковий розпорядник (оператор) не виконує обов'язки із захисту персональних даних, первинний розпорядник (оператор) залишається таким, що повністю відповідає перед володільцем (контролером) за виконання обов'язків такого додаткового розпорядника (оператора). При цьому якщо розпорядник (оператор) змінює мету та порядок обробки отриманих від володільця (контролера) персональних даних, то саме розпорядник (оператор) буде володільцем (контролером) персональних даних і відповідно нести відповідальність за обробку таких даних [53].

З огляду на викладені положення європейського законодавства, вважаємо, що правовий статус розпорядника персональних даних та особливості відносин між ним та володільцем персональних даних потребують деталізації у Законі України «Про захист персональних даних» відповідно до ст. 28 Регламенту Європейського парламенту і Ради (ЄС) 2016/679 від 27 квітня 2016 року.

У сфері охорони здоров’я розпорядниками персональних даних можуть бути органи публічної влади та їх посадові особи, співробітники закладів охорони здоров’я публічної форми власності, суб’єкти господарювання приватної форми власності, діяльність яких пов’язана з медичним обслуговуванням, а також медичні працівники, співробітники медичного закладу, працівники, відповідальні за захист персональних даних у лікаря-підприємця.

Відповідно до постанови КМ України від 25 квітня 2018 року № 411 [94] розпорядником реєстрів центральної бази даних електронної системи охорони здоров’я є НСЗ України. Щодо практики захисту персональних даних на місцях, то у закладах охорони здоров’я, за загальним правилом, відсутня самостійна посада розпорядника. Зазвичай, функції розпорядника покладаються на працівника відділу кадрів, бухгалтерії або медичного працівника, які можуть використовувати доступні їм відомості лише відповідно до професійних, службових і трудових обов’язків. Заклади охорони здоров’я повинні отримувати від працівників письмові зобов’язання про нерозголошення інформації, медичних персональних даних, що стали їм відомі у процесі виконання обов’язків. Обов’язок збереження такої таємниці повинен виконуватися навіть після припинення трудових відносин працівника із медичним закладом або установою [28, с. 498; 142, с. 29]. Слід також звернути увагу на те, що законодавче розуміння розпорядника персональних даних потребує перегляду в частині заміни слова «законом» на «законодавством», адже саме законодавством прямо визначається розпорядник персональних даних [133, с. 42].

До суб’єктів забезпечення захисту персональних даних у сфері охорони здоров’я необхідно віднести третіх осіб, які також можуть здійснювати обробку медичних даних, але з іншою метою. Згідно ст. 2 Закону України «Про захист персональних даних» третя особа – це будь-яка особа, за винятком суб’єкта персональних даних, володільця чи розпорядника персональних даних та Уповноваженого Верховної Ради України з прав людини, якій володільцем чи розпорядником персональних даних здійснюється передача персональних даних [46]. У ст. 4 Регламенту Європейського парламенту і Ради (ЄС) 2016/679 від 27

квітня 2016 року третя особа трактується як фізична чи юридична особа, орган публічної влади, агентство чи орган, який не є суб'єктом персональних даних, контролером, оператором та особами, які, під безпосереднім керівництвом контролера або оператора, уповноважені обробляти персональні дані [53]. Варто відмітити, що у як в українському, так і європейському законодавстві вживається поняття «одержувач», яке є значно ширшим за термін «третя особа». Згідно ст. 2 Закону України «Про захист персональних даних» одержувач – це фізична чи юридична особа, якій надаються персональні дані, у тому числі третя особа [46]. Відповідно до ст. 4 Регламенту Європейського парламенту і Ради (ЄС) 2016/679 від 27 квітня 2016 року одержувач означає фізичну чи юридичну особу, орган публічної влади, агентство чи інший орган, якому розкривають персональні дані, незалежно від того, чи є вони третьою стороною [53].

Ключова відмінність у тому, що третя особа – це окремий від володільця персональних даних суб'єкт. Передача персональних даних третій особі потребує наявності однієї з правових підстав, передбачених ст. 11 Закону України «Про захист персональних даних». Одержувачем можуть бути як треті особи, так і, наприклад, працівники володільця, структурні підрозділи, яким володілець може надати право доступу до персональних даних, які він обробляє. Однак за певних умов і передача персональних даних одним працівником володільця іншому може розглядатися як передача (поширення) персональних даних третій особі. Наприклад, якщо володілець чітко розмежував серед своїх працівників рівні доступу до персональних даних у базі даних, і працівник, що має такий доступ, передає персональні дані працівникові, який такого доступу не має, така дія розглядатиметься як передача персональних даних третій особі. При цьому така дія буде незаконна [133, с. 43].

Третя особа у відносинах щодо персональних даних з моменту отримання таких даних стає новим володільцем чи розпорядником таких даних, за умови наявності інших умов для кваліфікації цієї особи як володільця чи розпорядника та застосування законодавства про захист персональних даних. Тобто, третя особа, яка отримала від первісного володільця чи розпорядника персональні дані,

вступає в нові правовідносини з суб'єктом таких даних в якості нового володільця чи розпорядника. Тому можна виділити такі ознаки третіх осіб у відносинах щодо персональних даних: 1) треті особи не є стороною відносних правовідносин між суб'єктом даних та їх володільцем (розпорядником); 2) треті особи мають охоронюваний законом інтерес щодо персональних даних; 3) треті особи знаходяться в правовідносинах з володільцем (розпорядником) щодо передачі даних; 4) об'єктом таких відносин виступають персональні дані одного і того ж суб'єкта персональних даних; 5) із моменту отримання персональних даних третя особа набуває статусу їх володільця чи розпорядника [17, с. 143].

Отже, третіми особами у сфері захисту медичних даних можуть бути як органи публічної влади, так і суб'єкти господарювання приватної форми власності, діяльність яких пов'язана з медичним обслуговуванням. Третя особа отримує персональні дані про пацієнта від володільця або розпорядника таких даних. Однак мета обробки персональних даних пацієнта не співпадає з метою обробки таких даних володільцем чи розпорядником, які їх надають, що зумовлено сферою діяльності таких суб'єктів і потребою оперування відомостями про певну особу (наприклад, для правоохоронних органів для ідентифікації особи в межах своєї діяльності).

Особливе місце серед суб'єктів забезпечення захисту персональних даних у сфері охорони здоров'я відведено інституту Уповноваженого Верховної Ради України з прав людини. Наділення Уповноваженого Верховної Ради України з прав людини контролем за додержанням законодавства про захист персональних даних [46] вказує на важливе значення цього інституту у захисті основоположних прав і свобод людини і громадянина, зокрема права на невтручання в особисте життя, у зв'язку з обробкою персональних даних [143, с. 213].

Уповноважений Верховної Ради України з прав людини здійснює свою діяльність незалежно від інших державних органів та посадових осіб [2]. Уповноважений Верховної Ради України з прав людини – це призначений вищими органами державної влади контрольно-наглядовий, правозахисний, незалежний, політично-нейтральний, одноособовий чи колегіальний орган

державної влади (посадова особа), уповноважений конституцією чи законом за власною ініціативою або зверненням громадян контролювати діяльність органів і посадових осіб щодо дотримання ними прав і свобод людини та громадянина. Як правило, він діє неформально на власний розсуд та рекомендує корегуючі дії, спрямовані на забезпечення прав і свобод людини та громадянина [144, с. 35]. Важливим критерієм правового статусу омбудсмана є його незалежність від будь-яких державних та інших органів. Відповідно до чинного законодавства, що визначає правовий статус Уповноваженого Верховної Ради України з прав людини, омбудсман здійснює свої функції у межах своєї компетенції незалежно від органів державної влади і управління, органів місцевого самоврядування, громадських та політичних організацій. Український омбудсман під час здійснення своїх функцій підпорядковується лише законові, міжнародним стандартам у сфері прав людини та керується внутрішніми переконаннями [145, с. 175].

Відповідно до ст. 9 Закону України «Про захист персональних даних» володілець персональних даних повідомляє Уповноваженого Верховної Ради України з прав людини про обробку персональних даних, яка становить особливий ризик для прав і свобод суб'єктів персональних даних, упродовж тридцяти робочих днів з дня початку такої обробки. Види обробки персональних даних, яка становить особливий ризик для прав і свобод суб'єктів персональних даних, та категорії суб'єктів, на яких поширюється вимога щодо повідомлення, визначаються Уповноваженим Верховної Ради України з прав людини. Повідомлення про обробку персональних даних подається за формою та в порядку, визначеними Уповноваженим Верховної Ради України з прав людини. Володілець персональних даних зобов'язаний повідомляти Уповноваженого Верховної Ради України з прав людини про кожну зміну відомостей, що підлягають повідомленню, упродовж десяти робочих днів з дня настання такої зміни. Інформація, що повідомляється відповідно до цієї статті, підлягає оприлюдненню на офіційному веб-сайті Уповноваженого Верховної Ради України

з прав людини в порядку, визначеному Уповноваженим Верховної Ради України з прав людини [46].

Крім цього, Уповноважений Верховної Ради України з прав людини у сфері захисту персональних даних затверджує нормативно-правові акти у сфері захисту персональних даних; надавє рекомендації щодо практичного застосування законодавства про захист персональних даних, роз'яснює права і обов'язки відповідних осіб за зверненням суб'єктів персональних даних, володільців або розпорядників персональних даних, структурних підрозділів або відповідальних осіб з організації роботи із захисту персональних даних, інших осіб; взаємодіє із структурними підрозділами або відповідальними особами, які відповідно до Закону України «Про захист персональних даних» організовують роботу, пов'язану із захистом персональних даних при їх обробці, оприлюднює інформацію про такі структурні підрозділи та відповідальних осіб; звертається з пропозиціями до Верховної Ради України, Президента України, КМ України, інших державних органів, органів місцевого самоврядування, їх посадових осіб щодо прийняття або внесення змін до нормативно-правових актів з питань захисту персональних даних; надає за зверненням професійних, самоврядних та інших громадських об'єднань чи юридичних осіб висновки щодо проєктів кодексів поведінки у сфері захисту персональних даних та змін до них; інформує про законодавство з питань захисту персональних даних, проблеми його практичного застосування, права і обов'язки суб'єктів відносин, пов'язаних із персональними даними; здійснює моніторинг нових практик, тенденцій та технологій захисту персональних даних; організовує та забезпечує взаємодію з іноземними суб'єктами відносин, пов'язаних із персональними даними, у тому числі у зв'язку з виконанням Конвенції про захист осіб у зв'язку з автоматизованою обробкою персональних даних та Додаткового протоколу до неї, інших міжнародних договорів України у сфері захисту персональних даних; бере участь у роботі міжнародних організацій з питань захисту персональних даних [46].

Наведені положення Закону України «Про захист персональних даних» дають підстави стверджувати, що Уповноважений Верховної Ради України з прав людини є суб'єктом забезпечення захисту персональних даних у сфері охорони здоров'я, діяльність якого спрямована на забезпечення законності під час обробки та захисті персональних даних пацієнта.

Підсумовуючи викладене, констатуємо, що суб'єкти забезпечення захисту персональних даних у сфері охорони здоров'я – це фізичні та юридичні особи, діяльність яких пов'язана із забезпеченням захисту персональних даних у сфері охорони здоров'я. До суб'єктів забезпечення захисту персональних даних у сфері охорони здоров'я необхідно віднести: 1) володільці персональних даних у сфері охорони здоров'я; 2) розпорядники персональних даних у сфері охорони здоров'я; 3) треті особи персональних даних у сфері охорони здоров'я; 4) Уповноважений Верховної Ради України з прав людини. Саме володільці, розпорядники персональних даних та треті особи зобов'язані забезпечити захист персональних даних у сфері охорони здоров'я від неправомірного збирання, зберігання, використання, знищення, поширення та доступу до медичних даних. Натомість Уповноважений Верховної Ради України з прав людини зобов'язаний забезпечити додержання законодавства про захист персональних даних володільцями, розпорядниками та третіми особами під час здійснення діяльності, пов'язаної з персональними даними у сфері охорони здоров'я.

Володільцями персональних даних у сфері охорони здоров'я можуть бути органи публічної влади (МОЗ України та НСЗ України (як виключення КМ України) та суб'єкти господарювання приватної форми власності, діяльність яких пов'язана з медичним обслуговуванням. Розпорядниками персональних даних у сфері охорони здоров'я можуть бути органи публічної влади та їх посадові особи, співробітники закладів охорони здоров'я публічної форми власності, суб'єкти господарювання приватної форми власності, діяльність яких пов'язана з медичним обслуговуванням, а також медичні працівники, співробітники медичного закладу, працівники, відповідальні за захист персональних даних у лікаря-підприємця. Третіми особами персональних даних у сфері охорони

здоров’я можуть бути органи публічної влади та заклади охорони здоров’я будь-якої форми власності. Належне виконання обов’язків, пов’язаних із захистом персональних даних у сфері охорони здоров’я, такими суб’єктами забезпечить ефективний режим захисту медичних даних особи.

2.3. Правові засоби захисту персональних даних у сфері охорони здоров’я

Особисті немайнові права на персональні дані, які має кожна фізична особа, є невід’ємними і непорушними [46]. Недодержання встановленого законодавством про захист персональних даних порядку захисту персональних даних може призвести до незаконного доступу до медичних даних або порушення прав пацієнта. У цьому контексті особливої актуальності набувають питання про правові засоби захисту персональних даних у сфері охорони здоров’я – дієвих правових інструментів, передбачених законодавством, які спрямовані на недопущення протиправного втручання в право на персональні дані пацієнта чи обмежень у його здійсненні.

Першочерговими правовими засобами захисту персональних даних у сфері охорони здоров’я є превентивні заходи, метою яких є запобігання порушенням законодавства про захист персональних даних. Такі заходи повинні вживати суб’єкти забезпечення захисту персональних даних у сфері охорони здоров’я.

У ст. 24 Закону України «Про захист персональних даних» встановлено, що володільці, розпорядники персональних даних та треті особи зобов’язані забезпечити захист цих даних від випадкових втрати або знищення, від незаконної обробки, у тому числі незаконного знищення чи доступу до персональних даних [46].

Превентивні заходи захисту персональних даних у сфері охорони здоров’я, які зобов’язані вживати володільці та розпорядники персональних даних,

передбачені Типовим порядком обробки персональних даних, затвердженим наказом Уповноваженого Верховної Ради України з прав людини від 8 січня 2014 року № 1/02-14 [87].

Володілець, розпорядник персональних даних вживають заходів щодо забезпечення захисту персональних даних на всіх етапах їх обробки, у тому числі за допомогою організаційних та технічних заходів. Володілець, розпорядник персональних даних самостійно визначають перелік і склад заходів, спрямованих на безпеку обробки персональних даних, з урахуванням вимог законодавства у сферах захисту персональних даних, інформаційної безпеки [87].

Організаційні заходи охоплюють: визначення порядку доступу до персональних даних працівників володільця/розпорядника; визначення порядку ведення обліку операцій, пов'язаних з обробкою персональних даних суб'єкта та доступом до них; розробку плану дій на випадок несанкціонованого доступу до персональних даних, пошкодження технічного обладнання, виникнення надзвичайних ситуацій; регулярне навчання співробітників, які працюють з персональними даними [87].

Володілець/розпорядник веде облік працівників, які мають доступ до персональних даних суб'єктів. Володілець/розпорядник визначає рівень доступу зазначених працівників до персональних даних суб'єктів. Кожен із цих працівників користується доступом лише до тих персональних даних (їх частини) суб'єктів, які необхідні йому у зв'язку з виконанням своїх професійних чи службових або трудових обов'язків. Працівники, які мають доступ до персональних даних, дають письмове зобов'язання про нерозголошення персональних даних, які їм було довірено або які стали їм відомі у зв'язку з виконанням професійних чи службових або трудових обов'язків. Датою надання права доступу до персональних даних вважається дата надання зобов'язання відповідним працівником. Датою позбавлення права доступу до персональних даних вважається дата звільнення працівника, дата переведення на посаду, виконання обов'язків на якій не пов'язане з обробкою персональних даних. У разі звільнення працівника, який мав доступ до персональних даних, або переведення

його на іншу посаду, що не передбачає роботу з персональними даними суб'єктів, вживаються заходи щодо унеможливлення доступу такої особи до персональних даних, а документи та інші носії, що містять персональні дані суб'єктів, передаються іншому працівнику [87].

Володілець/розпорядник веде облік операцій, пов'язаних з обробкою персональних даних суб'єкта та доступом до них. З цією метою володільцем/розпорядником зберігається інформація про: дату, час та джерело збирання персональних даних суб'єкта; зміну персональних даних; перегляд персональних даних; будь-яку передачу (копіювання) персональних даних суб'єкта; дату та час видалення або знищення персональних даних; працівника, який здійснив одну із указаних операцій; мету та підстави зміни, перегляду, передачі та видалення або знищення персональних даних [87].

Володілець/розпорядник персональних даних самостійно визначає процедуру збереження інформації про операції, пов'язані з обробкою персональних даних суб'єкта та доступом до них. У випадку обробки персональних даних суб'єктів за допомогою автоматизованої системи така система автоматично фіксує вказану інформацію. Ця інформація зберігається володільцем/розпорядником упродовж одного року з моменту закінчення року, в якому було здійснено зазначені операції, якщо інше не передбачено законодавством України. Персональні дані залежно від способу їх зберігання (паперові, електронні носії) мають оброблятися у такий спосіб, щоб унеможливити доступ до них сторонніх осіб [87].

З метою забезпечення безпеки обробки персональних даних вживаються спеціальні технічні заходи захисту, у тому числі щодо виключення несанкціонованого доступу до персональних даних, що обробляються та роботі технічного та програмного комплексу, за допомогою якого здійснюється обробка персональних даних. У володільцях чи розпорядниках персональних даних, що здійснюють обробку персональних даних, яка підлягає повідомленню відповідно до Закону України «Про захист персональних даних», створюється (визначається) структурний підрозділ або відповідальна особа, що організовує роботу, пов'язану із захистом персональних даних при їх обробці. Інформація про зазначений

структурний підрозділ або відповідальну особу повідомляється Уповноваженому Верховної Ради України з прав людини, який забезпечує її оприлюднення. Структурний підрозділ або відповідальна особа, що організовує роботу, пов'язану із захистом персональних даних при їх обробці: 1) інформує та консультує володільця або розпорядника персональних даних з питань додержання законодавства про захист персональних даних; 2) взаємодіє з Уповноваженим Верховної Ради України з прав людини та визначеними ним посадовими особами його секретаріату з питань запобігання та усунення порушень законодавства про захист персональних даних [87, 46].

З метою виконання вказаних завдань відповідальна особа/структурний підрозділ: забезпечує реалізацію прав суб'єктів персональних даних; користується доступом до будь-яких даних, які обробляються володільцем/розпорядником та до всіх приміщень володільця/розпорядника, де здійснюється така обробка; у разі виявлення порушень законодавства про захист персональних даних та/або цього Порядку повідомляє про це керівника володільця/розпорядника з метою вжиття необхідних заходів; аналізує загрози безпеці персональних даних. Вимоги відповідальної особи до заходів щодо забезпечення безпеки обробки персональних даних є обов'язковими для всіх працівників, які здійснюють обробку персональних даних. Факти порушень процесу обробки та захисту персональних даних повинні бути документально зафіксовані відповідальною особою або структурним підрозділом, що організовує роботу, пов'язану із захистом персональних даних при їх обробці [87].

Повноваженнями застосування превентивних заходів захисту персональних даних у сфері охорони здоров'я наділений також Уповноважений Верховної Ради України з прав людини, до яких, насамперед, необхідно віднести такі:

1) отримувати пропозиції, скарги та інші звернення фізичних і юридичних осіб з питань захисту персональних даних та приймати рішення за результатами їх розгляду;

2) проводити на підставі звернень або за власною ініціативою виїзні та безвиїзні, планові, позапланові перевірки володільців або розпорядників

персональних даних в порядку, визначеному Уповноваженим, із забезпеченням відповідно до закону доступу до приміщень, де здійснюється обробка персональних даних;

3) отримувати на свою вимогу та мати доступ до будь-якої інформації (документів) володільців або розпорядників персональних даних, які необхідні для здійснення контролю за забезпеченням захисту персональних даних, у тому числі доступ до персональних даних, відповідних баз даних чи картотек, інформації з обмеженим доступом;

4) за підсумками перевірки, розгляду звернення видавати обов'язкові для виконання вимоги (приписи) про запобігання або усунення порушень законодавства про захист персональних даних, у тому числі щодо зміни, видалення або знищення персональних даних, забезпечення доступу до них, надання чи заборони їх надання третій особі, зупинення або припинення обробки персональних даних;

5) надавати рекомендації щодо практичного застосування законодавства про захист персональних даних, роз'яснювати права і обов'язки відповідних осіб за зверненням суб'єктів персональних даних, володільців або розпорядників персональних даних, структурних підрозділів або відповідальних осіб з організації роботи із захисту персональних даних, інших осіб;

6) взаємодіяти із структурними підрозділами або відповідальними особами, які відповідно до цього Закону організовують роботу, пов'язану із захистом персональних даних при їх обробці; оприлюднювати інформацію про такі структурні підрозділи та відповідальних осіб тощо [46].

Запобігання та виявлення порушень законодавства про захист персональних даних Уповноваженим Верховної Ради України з прав людини здійснюється на підставі звернень фізичних і юридичних осіб або за власною ініціативою шляхом проведення планових, позапланових, виїзних та безвиїзних перевірок. Планові та позапланові перевірки можуть бути виїзними та безвиїзними [87].

За результатами здійснення планової або позапланової перевірки Уповноважений Верховної Ради України з прав людини та/або уповноважена

посадова особи складає у двох примірниках акт перевірки додержання вимог законодавства про захист персональних даних, який повинен містити один із таких висновків: про відсутність у діяльності суб'єкта перевірки порушень вимог законодавства про захист персональних даних; про виявлені у діяльності суб'єкта перевірки порушення вимог законодавства про захист персональних даних, їх детальний опис із посиланням на норми чинного законодавства, які порушено. На підставі акта перевірки, під час якої виявлено порушення вимог законодавства про захист персональних даних, складається припис про усунення порушень вимог законодавства у сфері захисту персональних даних, виявлених під час перевірки, в якому зазначаються, серед іншого, підстава для видачі припису; заходи необхідні для усунення порушень, виявлених під час перевірки; строк виконання припису; строк інформування суб'єктом перевірки Уповноваженого Верховної Ради України з прав людини про усунення виявленого порушення. Суб'єкт перевірки повинен протягом визначеного у приписі строку (не менше ніж 30 календарних днів) вжити заходів щодо усунення порушень, зазначених у приписі, та письмово поінформувати Уповноваженого Верховної Ради України з прав людини про усунення порушень разом із наданням копій документів, що це підтверджують. Контроль за своєчасністю та повнотою виконання вимог, зазначених у приписі, здійснюється шляхом вивчення вказаних копій документів та, у разі необхідності, шляхом проведення позапланової перевірки [87].

Наступними правовими засобами захисту персональних даних у сфері охорони здоров'я є припиняючі заходи, метою яких є усунення та припинення порушення законодавства про захист персональних даних. Припиняючі заходи застосовуються Уповноваженим Верховної Ради України з прав людини до володільця або розпорядника персональних даних за наявності факту порушення законодавства про захист персональних даних.

До заходів припинення порушення законодавства про захист персональних даних необхідно віднести такі: безпосереднє усунення володільцем або розпорядником персональних даних порушень законодавства про захист персональних даних; отримання Уповноваженим Верховної Ради України з прав

людини скарг фізичних і юридичних осіб з питань захисту персональних даних та приймати рішення за результатами їх розгляду; здійснення Уповноваженим Верховної Ради України з прав людини позапланових перевірок володільців або розпорядників персональних даних із забезпеченням відповідно до закону доступу до приміщень, де здійснюється обробка персональних даних; видання Уповноваженим Верховної Ради України з прав людини вимоги (припису) про усунення порушень законодавства про захист персональних даних та підстав, які зумовлювали таке порушення. Метою внесення припису є припинення порушення законодавства про захист персональних даних та по мірі можливості його виправлення, а також усунення обставин, що сприяли його виникненню, чи інших, що можуть призвести до його виникнення в майбутньому. З цією метою припис може містити, серед іншого, вказівки щодо: зміни, видалення або знищення персональних даних, забезпечення доступу до них, надання чи заборони їх надання третій особі, зупинення або припинення обробки персональних даних. Вказані вимоги є зрозумілими і окремого роз'яснення не потребують. Їх метою є припинити порушення Закону (наприклад, видалити дані, що обробляються незаконно), відновити порушені права (наприклад, надати суб'єкту доступ до його персональних даних чи змінити його персональні дані, що не відповідають дійсності) або запобігти потенційним порушенням в майбутньому (наприклад, припинити обробку (зокрема, збір, зберігання та використання) персональних даних, що не є необхідними для досягнення задекларованої легітимної мети їх обробки, запровадити додаткові заходи захисту персональних даних) [109, с. 127-128; 146, с. 139].

У разі невиконання припису протягом вказаного у ньому строку Уповноважений Верховної Ради України з прав людини або уповноважена посадова особа складає протокол про адміністративне правопорушення за формою та у порядку, передбаченому КУпАП та Порядком оформлення матеріалів про адміністративні правопорушення. У разі виявлення під час перевірки суб'єкта перевірки ознак кримінального правопорушення (ст. 182 «Порушення недоторканності приватного життя» КК України) Уповноважений

Верховної Ради України з прав людини направляє необхідні матеріали до правоохоронних органів [87].

КУпАП передбачено адміністративну відповідальність за порушення законодавства у сфері захисту персональних даних (ст. 188^{39}) та невиконання законних вимог Уповноваженого Верховної Ради України з прав людини (ст. 188^{40}).

Так, у ст. 188^{39} КУпАП передбачено, що 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 - тягнуть за собою накладення штрафу на громадян від ста до двохсот неоподатковуваних мінімумів доходів громадян і на посадових осіб, громадян - суб'єктів підприємницької діяльності - від двохсот до чотирьохсот неоподатковуваних мінімумів доходів громадян (ч. 1). 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 - тягнуть за собою накладення штрафу на громадян від двохсот до трьохсот неоподатковуваних мінімумів доходів громадян і на посадових осіб, громадян - суб'єктів підприємницької діяльності - від трьохсот до однієї тисячі неоподатковуваних мінімумів доходів громадян (ч. 2). Повторне протягом року вчинення порушення з числа передбачених частинами першою або другою цієї статті, за яке особу вже було піддано адміністративному стягненню, - тягне за собою накладення штрафу на громадян від трьохсот до п'ятисот неоподатковуваних мінімумів доходів громадян і на посадових осіб, громадян - суб'єктів підприємницької діяльності - від п'ятисот до двох тисяч неоподатковуваних мінімумів доходів громадян (ч. 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, - тягне за собою накладення штрафу на

громадян від ста до п’ятисот неоподатковуваних мінімумів доходів громадян і на посадових осіб, громадян - суб’єктів підприємницької діяльності - від трьохсот до однієї тисячі неоподатковуваних мінімумів доходів громадян (ч. 4). Повторне протягом року вчинення порушення, передбаченого частиною четвертою цієї статті, за яке особу вже було піддано адміністративному стягненню, - тягне за собою накладення штрафу від однієї тисячі до двох тисяч неоподатковуваних мінімумів доходів громадян (ч. 5) [72].

Загалом же чч. 1 та 2 ст. 188^{39} КУпАП доволі однозначні та чіткі й не потребують додаткових роз’яснень. Також слід зазначити, що вказаними положеннями передбачається відповідальність за порушення лише незначних аспектів законодавства про захист персональних даних. Здебільшого йдеться про порушення володільцями своїх зобов’язань перед Уповноваженим Верховної Ради України з прав людини. Разом з тим жодне з вказаних положень не передбачає відповідальності за порушення правил обробки / захисту персональних даних. Однак саме відносини, пов’язані з обробкою та захистом персональних даних, і є ключовий предмет правового регулювання Закону України «Про захист персональних даних» [133, с. 133].

Водночас ч. 4 ст. 188^{39} КУпАП сформульована доволі розпливчасто та заплутано, тому її практичне застосування пов’язане з суттєвими труднощами. З об’єктивної сторони вказане положення включає два елементи, пов’язані причинно-наслідковим зв’язком: 1) недодержання встановленого законодавством про захист персональних даних порядку захисту персональних даних; 2) незаконний доступ до них або порушення прав суб’єкта персональних даних. В законодавстві нема не лише означення понять «захист персональних даних» та «порядок захисту персональних даних», а й будь-яких вимог щодо того, яким критеріям повинен відповідати такий захист. Єдине, що передбачено Законом в цій частині, – це обов’язок забезпечити «захист даних» (ст. 24 Закону України «Про захист персональних даних»). Можна зробити припущення, що йдеться, з одного боку, про загальний обов’язок володільця вживати організаційних та технічних заходів з метою запобігання випадковій втраті або знищенню,

незаконній обробці, зокрема незаконному знищенню чи доступові до персональних даних, а з іншого – про обов'язок кожного працівника не допускати розголошення персональних даних, які стали йому відомі у зв'язку з виконанням професійних, чи службових, чи трудових обов'язків. З огляду на практику, яка сформувалася за результатами розгляду судами протоколів про адміністративні порушення [147-159], можна стверджувати, що поняття «встановленого законодавством про захист персональних даних порядку захисту персональних даних» тлумачиться доволі широко та охоплює будь-які дії, які становлять порушення Закону України «Про захист персональних даних». Загалом же тлумаченню цього поняття взагалі не приділяється уваги в рішеннях судів, зазвичай вони автоматично займають таку позицію. Тому видається доцільним запровадити як у КУпАП, так і в Законі України «Про захист персональних даних» певні, хоча б базові вимоги щодо якості та рівня такого захисту (достатність/адекватність/ пропорційність тощо), обов'язку вжити заходів для визначення необхідного рівня захисту (проводити діагностику систем захисту, визначення ризиків, пов'язаних з обробкою тощо) та інше [146, с. 141-142; 133, с. 133-135].

Далі, згідно з КупАП, для того щоб становити порушення ст. 188^{39}, такі дії повинні бути в причиново-наслідковому зв'язку з незаконним доступом до персональних даних або порушенням прав суб'єкта персональних даних. З незаконним доступом усе більш-менш зрозуміло, наприклад порушення порядку захисту, що призвело до незаконного доступу третіх осіб. Разом з тим варто ще раз наголосити на важливому понятійному аспекті [133, с. 135]. Закон України «Про захист персональних даних» розрізняє поняття доступу третіх осіб та поширення/передачу третім особам (ст. 14). Порядок доступу викладено у ст. 16 Закону України «Про захист персональних даних» і він базується на процедурі «запит-відповідь». У випадку, якщо персональні дані було всупереч Закону України «Про захист персональних даних» оприлюднено чи поширено (тобто попередньо не було запиту), це вже не охоплюється поняттям доступу. Це суттєвий термінологічний недолік Закону України «Про захист персональних

даних». У всіх міжнародних документах поняття доступу використовується виключно в контексті відповідного права суб'єкта персональних даних. Коли ж мова йде про отримання персональних даних третіми особами, це характеризується як розкриття (disclosure – в національному контексті), передача (transfer – в міжнародному контексті), поширення (dissemination). Насправді будь-яке незаконне поширення/оприлюднення/передача персональних даним третіми особами повинне характеризуватися як правопорушення та тягнути за собою передбачену законом відповідальність [146, с. 142-143].

З іншою частиною структури ч. 4 ст. ст. 188^{39} КУпАП ситуація дещо складніша. Формулювання «захист прав суб'єкта персональних даних» автоматично відсилає до ст. 8 Закону України «Про захист персональних даних» («Права суб'єкта персональних даних»). У вказаному положенні йдеться, серед іншого, про право отримувати інформацію про те, які дані, як та ким обробляються; заперечувати проти обробки; відкликати згоду на обробку персональних даних; звертатися зі скаргами на незаконну обробку; та право на захист від незаконної обробки, пошкодження, поширення неправдивих даних та прийняття автоматизованого рішення. Однак на практиці важко уявити порушення «порядку захисту персональних даних», що призвело б до порушення права «отримувати інформацію про умови надання доступу до персональних даних, зокрема інформацію про третіх осіб, яким передаються його персональні дані», права «знати про джерела збирання, місцезнаходження своїх персональних даних, мету їх обробки» чи, наприклад, права «на захист від автоматизованого рішення, яке має для нього правові наслідки» (пп. 2, 3 та 13 ч. 2 ст. 8 Закону України «Про захист персональних даних») та ін. Вказані комбінації виглядають позбавленими будь-якого змісту. Єдине змістовне поєднання (і то лише частково), яке випливає з положень вказаної статті це недодержання «порядку захисту персональних даних», що призвело до порушення прав суб'єкта персональних даних, а саме його права «на захист своїх персональних даних від незаконної обробки та випадкової втрати, знищення, пошкодження у зв'язку з умисним приховуванням, ненаданням чи несвоєчасним їх наданням, а також на захист від

надання відомостей, що є недостовірними чи ганьблять честь, гідність та ділову репутацію фізичної особи» (ст. 8 Закону України «Про захист персональних даних»). У сферу дії вказаного положення КУпАП очевидно потрапляють дії, пов'язані з незаконною передачею, розкриттям, втратою, знищенням та зміною персональних даних, якщо вони були спричинені недодержанням «встановленого законодавством про захист персональних даних порядку захисту персональних даних». На практиці ж у сферу дії цієї статті потрапляє здебільшого незаконна передача персональних даних (чи незаконний доступ з боку третіх осіб) [133, с. 135-136]. Щодо захисту персональних даних у сфері охорони здоров'я здебільшого осіб притягують до відповідальності на підставі ч. 4 ст. 188^{39} КУПАП за незаконну передачу персональних даних третім особам у разі поширення медичним закладом інформації щодо стану психічного здоров'я [160].

Необхідно відмітити, що самі по собі порушення окремих найвагоміших положень Закону України «Про захист персональних даних» можуть (і повинні) кваліфікуватись як окремі правопорушення у сфері законодавства про захист персональних даних (неповідомлення суб'єкта про збір персональних даних; незаконна обробка (і зокрема поширення) персональних даних, яка не пов'язана з порушенням порядку захисту; обробка персональних даних на підставі згоди з порушенням основних вимог, що ставляться до неї (поінформованість, добровільність, наявність документів, що підтверджують її надання); відмова в наданні доступу суб'єктові до його персональних даних, надання неповних відомостей чи надання відповіді з порушенням визначених Законом строків; ненадання відомостей щодо порядку обробки персональних даних; ненадання відомостей про порядок доступу до персональних даних; брак обліку операцій, пов'язаних з обробкою персональних даних; відмова змінити/видалити персональні дані, що не відповідають дійсності, непризначення відповідальної особи; нечітке визначення її обов'язків, порушення умов щодо призначення розпорядника тощо). Виявлення таких порушень зазвичай завершується винесенням припису Уповноваженого Верховної Ради України з прав людини, мета якого – їх усунення. У приписі можуть бути висунуті будь-які вимоги,

необхідні для вдосконалення системи захисту персональних даних володільця/розпорядника Невиконання такого припису тягне за собою відповідальність, передбачену ч. 2 ст. 188^{39} КУПАП [133, с. 138-139].

Однак, слід зауважити, що володілець від самого початку незацікавлений у налагодженні належної системи захисту персональних даних, оскільки хоч би яке серйозне порушення законодавства про захист персональних даних скоїв володілець, його можна притягнути до адміністративної відповідальності лише у разі, якщо це призвело до незаконного поширення персональних даних суб'єкта або порушення порядку доступу до них, визначеного ст. 16 Закону України «Про захист персональних даних». Теоретично володільця можна притягнути до відповідальності також у разі незаконного знищення, зміни чи втрати даних, однак жодної практики з цього приводу не виявлено. Інакше ж володільцеві загрожує лише винесення припису. Отже, володільцеві/розпорядникові набагато зручніше дочекатися приходу з перевіркою наглядового органу (наприклад, за скаргою суб'єкта) та виконати винесений припис. Така ситуація підсилюється і тим, що, з огляду на обмежені ресурси Секретаріату Уповноваженого Верховної Ради України з прав людини, ймовірність проведення такої перевірки, коли нема скарги, вкрай незначна [133, с. 139].

Згідно ст. 188^{40} КУпАП невиконання законних вимог Уповноваженого Верховної Ради України з прав людини або представників Уповноваженого Верховної Ради України з прав людини - тягне за собою накладення штрафу на посадових осіб, громадян - суб'єктів підприємницької діяльності від ста до двохсот неоподатковуваних мінімумів доходів громадян [72]. В якості невиконання законних вимог розцінюються наступні дії працівників володільця: ненадання документів/інформації; невчасне надання документів/інформації; відмова в наданні документів/інформації; недопущення до проведення перевірки; ненадання доступу до приміщень; ненадання доступу до інформації/документів, що є в електронному вигляді [146, с. 139].

У ст. 255 КУпАП встановлено, що протоколи про адміністративні правопорушення, передбачені ст. ст. 188^{39} та 188^{40} КУпАП, мають право складати

уповноважені особи секретаріату Уповноваженого Верховної Ради України з прав людини або представники Уповноваженого Верховної Ради України з прав людини [72]. Порядок оформлення матеріалів про адміністративні правопорушення визначено наказом Уповноваженого Верховної Ради України з прав людини від 16 лютого 2015 року № 3/02-15 [93]. Згідно ст. 221 КУпАП справи про такі адміністративні правопорушення розглядають судді районних, районних у місті, міських чи міськрайонних судів [72]. У ст. ст. 276, 277, 38 КУпАП передбачено, що справи про ці адміністративні правопорушення розглядаються за місцем їх вчинення у п'ятнадцятиденний строк з дня одержання судом протоколу про адміністративне правопорушення та інших матеріалів справи, а стягнення може бути накладено не пізніш як через три місяці з дня вчинення правопорушення [72].

Аналіз судових рішень у справах, де особу визнано винуватою у скоєнні адміністративного правопорушення, передбаченого ст. 188^{39} КУпАП, показує, що суди не накладали стягнень і закривали провадження у зв'язку із закінченням строку їх накладення [154, 161]. Це зумовлено тим, що в абсолютній більшості випадків, встановлений КУпАП строк (три місяці з дня вчинення правопорушення) недостатній для вчасного оформлення адміністративного матеріалу, направлення його до суду та розгляду справи судом. Основна перешкода для вчасного накладення стягнення – природа порушень законодавства про захист персональних даних. На відміну від порушень, які фіксують інші органи в момент їх виявлення та відразу передають до суду (порушення правил дорожнього руху, порушення митних правил тощо), порушення законодавства про захист персональних даних фіксують зазвичай у ході проведення перевірки за скаргами суб'єктів персональних даних, тобто коли порушення вже могло відбутися достатньо тривалий час тому. Як наслідок, з моменту скоєння правопорушення та його виявлення суб'єктом до направлення справи до суду проходить досить значний час [133, с. 140].

Варто також вказати на необхідність належного обґрунтування скарги або позову, що здебільшого неможливо без звернення до володільця. Далі, після того

як суб’єкт направляє скаргу до Уповноваженого Верховної Ради України з прав людини, її розгляд також займає значний час. У цьому зв’язку слід звернути увагу на те, що Секретаріат Уповноваженого Верховної Ради України з прав людини, працівники якого і займаються питаннями захисту персональних даних, працюють у Києві, а порушення трапляються в різних регіонах. Своєю чергою, регіональні представники Уповноваженого займаються всім колом питань і не завжди мають можливість та достатню кваліфікацію для проведення перевірки за скаргами про порушення законодавства про захист персональних даних. Фіксація факту порушення законодавства про захист персональних даних потребуватиме проведення перевірки (виїзної – у форматі перевірки чи безвиїзної – через направлення запитів), яка, також потребуватиме значних затрат часу. І всі ці стадії можуть супроводжуватися значними затримками: надання відповідей в останній момент, надання нечітких і неповних відповідей, ненадання відповіді, перешкоджання в проведенні перевірки, за що штраф істотно менший, ніж за порушення законодавства про захист персональних даних (ст. 188^{40} КУпАП «Невиконання законних вимог Уповноваженого Верховної Ради України»). Тому, навіть за умови швидкого проходження попередньої стадії, суддя може не встигнути розглянути матеріали про адміністративне правопорушення, не кажучи вже про те, що 1) матеріали можуть бути повернуті для увідповіднення їх процесуальним вимогам, 2) особа, на яку накладають стягнення, може затягувати розгляд справи, зловживаючи своїми процесуальними правами, а 3) суддя може бути перевантаженим роботою [133, с. 141].

У зв’язку з цим доцільно вдосконалити чинні положення законодавства України щодо відповідальності за порушення про захист персональних даних. Зокрема, необхідно продовжити визначені законодавством строки накладення адміністративного стягнення за порушення законодавства про захист персональних даних і гарантувати ефективну діяльність контрольного органу як кількісно, так і через представництво в регіонах [133, с. 141].

З цього приводу Ю.С. Самойленко слушно відмічає, що окремі положення законодавства унеможливлюють в окремих випадках притягнення особи до

адміністративної відповідальності за порушення законодавства щодо захисту персональних даних. Зокрема, дана категорія справ розглядається за місцем їх вчинення, яке іноді важко встановити адже внесення, обробка і поширення персональних даних з порушенням законодавства може здійснюватись володільцем дистанційно (через використання ЕОМ та засобом інтернету), тому потрібно конкретизувати, що місцем розгляду справи є юридична адреса володільця персональних даних, хоча постраждала особа шляхом звернення до суду може клопотати про розгляд справи за місцем її проживання на що суд або задовольняє є клопотання або мотивовано відмовляє в його задоволені [109, с. 133-134]. Крім цього, на її думку слід продовжити строк притягнення до адміністративної відповідальності та накладення стягнення. Адже за цей час особа повинна встигнути направити скаргу, Уповноважений Верховної Ради України з прав людини розглянути її, зібрати матеріали, оформити правопорушення (зокрема скласти протокол), ознайомити з матеріалами правопорушника, направити матеріали до суду, а суд розглянути справу. Зазвичай вже суб'єкт направляє скаргу із запізненням (часто навіть після закінчення трьох місячного строку). Відтак доцільно продовжити строки притягнення до відповідальності та накладення стягнення за порушення законодавства про захист персональних даних до одного року. Зазначене є актуальним навіть якщо право виносити постанови у справах про порушення законодавства про захист персональних даних буде передано Уповноваженому Верховної Ради України з прав людини [162, с. 226; 109, с. 134].

Окремо слід наголосити на необхідності вдосконалення положень щодо суб'єктного складу осіб, які можуть нести відповідальність за порушення законодавства про захист персональних даних. А що не завжди можливо встановити конкретну особу, відповідальну за порушення законодавства про захист персональних даних (навіть якщо з матеріалів справи очевидно, що поширення персональних даних скоїв хтось із працівників організації – володільця відповідних персональних даних [163]), то в такому разі повинна існувати можливість притягнення до відповідальності конкретної юридичної

особи [133, с. 142]. Особливо це стосується закладів охорони здоров’я, оскільки у разі порушення ними законодавства про захист персональних даних їх не можливо бути притягнути до адміністративної відповідальності.

КК України передбачено кримінальну відповідальність за порушення недоторканності приватного життя (ст. 182). Згідно ст. 182 КК України незаконне збирання, зберігання, використання, знищення, поширення конфіденційної інформації про особу або незаконна зміна такої інформації, крім випадків, передбачених іншими статтями цього Кодексу, - караються штрафом від п’ятисот до однієї тисячі неоподатковуваних мінімумів доходів громадян або виправними роботами на строк до двох років, або пробаційним наглядом на строк до трьох років, або обмеженням волі на той самий строк (ч. 1). Ті самі дії, вчинені повторно, або якщо вони заподіяли істотну шкоду охоронюваним законом правам, свободам та інтересам особи, - караються пробаційним наглядом на строк від трьох до п’яти років або обмеженням волі на строк від трьох до п'яти років, або позбавленням волі на той самий строк (ч. 2) [73]. Загальним об’єктом неправомірного посягання на персональні дані виступають особисті права та свободи людини і громадянина. Родовим об’єктом складу такого кримінального правопорушення є право особи на недоторканність життя, безпосереднім об’єктом – персональні дані, що становлять відомості про особу [109, с. 138].

У юридичній літературі слушно відмічається, що ст. 182 КК України характеризується недостатньою вичерпністю опису протиправних діянь. Зокрема, у ч. 1 цієї статті наведено перелік операцій обробки конфіденційних даних, незаконне здійснення яких має наслідком кримінальну відповідальність (нині це збирання, зберігання, використання, поширення, зміна та знищення конфіденційної інформації). Однак з невідомих причин до переліку не було внесено такі операції: накопичення, що передбачає об’єднання, систематизацію та внесення персональних даних до відповідних інформаційних баз; адаптування, тобто переведення даних в іншу форму (зокрема цифрову) для забезпечення їх обробки на конкретних технічних засобах або під управлінням конкретних програмних продуктів; знеособлення – дії, в результаті яких унеможливлюється

встановлення особи суб'єкта персональних даних без застосування додаткової інформації (додаткових засобів). Як наслідок, незаконне проведення цих операцій з погляду букви закону, не може вважатися злочином та слугувати підставою для кримінальної відповідальності. В умовах очевидності їх суспільної небезпеки таке становище неприйнятне. У зв'язку з цим у ст. 182 КК України мають бути конкретизовані всі види обробки конфіденційної інформації, визначені Законом України «Про захист персональних даних» (ст. 2). З одного боку, це сприятиме розширенню меж правової охорони конфіденційності приватного життя, а з іншого – дасть змогу уникнути невизначеностей і різночитань під час кваліфікації злочинів [12, с. 164-165].

Необхідно зауважити, що саме від виду персональних даних як предмета неправомірного посягання залежить міра покарання за вчинення відповідного злочинного діяння, а також суб'єкт вчинення цього посягання, тому в кримінальному законодавстві виділяють різні склади злочину. Наприклад, ст. 145 КК України передбачена відповідальність за умисне розголошення лікарської таємниці особою, якій вона стала відома у зв'язку з виконанням професійних чи службових обов'язків. Предметом складу цього злочину виступає лікарська таємниця – певним чином задокументована інформація про хворобу, медичне обстеження, огляд та його результати, тобто інформація про стан здоров'я пацієнта, що і є персональними даними. Стаття 163 КК України передбачає відповідальність за порушення таємниці листування, телефонних розмов, телеграфних та інших повідомлень, що передаються засобами зв'язку або через комп'ютер. У цьому випадку предметом злочину є відомості, що передані чи передаються громадянами шляхом листування або телефонних розмов, а також повідомлення громадян, які передаються або були передані телеграфом чи за допомогою інших засобів зв'язку, а також через комп'ютер і становлять таємницю громадянина [109, с. 138-139]. До видів злочинів, об'єктом посягання яких є персональні дані, можемо віднести: розголошення таємниці усиновлення (удочеріння) всупереч волі усиновителя (удочерителя) (ст. 168 КК України), незаконне використання спеціальних технічних засобів негласного отримання

інформації (ст. 359 КК України), порушення правил експлуатації електронно-обчислювальних систем (ст. 363 КК України) [109, с. 139].

Дискусійний характер мають і деякі положення кримінально-процесуального законодавства. Зокрема, відповідно до ст. 477 Кримінального процесуального кодексу України провадження в справах про порушення недоторканості приватного життя здійснюється лише у формі приватного обвинувачення, тобто виключно на підставі заяви потерпілого [77]. На перший погляд, такий підхід може здатись обґрунтованим, оскільки і з назви ст. 182 КК України, і з доктринального уявлення про безпосередній об'єкт передбачених цією статтею порушень випливає їх спрямованість проти приватних інтересів окремої особи [164, с. 111]. Отож, з погляду законодавця, саме вона й повинна вирішувати питання про кримінально-правовий захист своїх прав та кримінальне переслідування порушника. Однак при детальному розгляді ситуація не видається настільки однозначною. Адже незаконні операції з персональними даними, особливо на первинних етапах їх обробки (збирання, систематизація, зберігання), здебільшого мають закритий характер. Вони перебігають приховано, а ймовірність їх виявлення суб'єктом персональних даних (читай потерпілою особою) дуже мала. Часто потерпіла особа констатує порушення своїх прав не за фактом протиправного діяння, а за його наслідками, тобто вже після того, як воно справило реальний негативний вплив на її життя. У решті випадків незаконні операції з персональними даними залишаються непоміченими. Та це зовсім не означає, що вони не становлять суспільної небезпеки [12, с. 171].

Крім того, як показує практика, незаконні операції з персональними даними найчастіше здійснюють в рамках функціонування великих інформаційних баз (баз персональних даних). У ході їх реалізації відбувається системна обробка інформації про велику кількість громадян, що свідчить про масовий характер порушень недоторканності приватного життя. Таким чином, порушення, передбачені ст. 182 КК України, хоч і посягають на суто приватні інтереси, але в багатьох випадках це інтереси не окремого індивіда, а широкого кола осіб. У зв'язку з цим та враховуючи те, що основна маса правопорушень проти

недоторканності приватного життя, зокрема у сфері обробки персональних даних, виявляються під час реалізації заходів публічного контролю, а також беручи до уваги необхідність системної протидії незаконній обробці персональних даних на всіх її стадіях та етапах, доцільно повернутися до практики розгляду відповідних кримінальних проваджень у загальному порядку, який передбачає можливість відкриття провадження не лише за заявою потерпілого, а й у разі отримання інформації про злочин з будь-яких інших джерел [12, с. 172].

Водночас слід зазначити, що практики застосування ст. 182 КК України в Єдиному державному реєстрі судових рішень практично немає. Серед поодиноких рішень, ухвалених за цією статтею, можна назвати вироки у справах, предметом яких було незаконна передача конфіденційної інформації (персональних даних) володільцем третім особам [165] та незаконний збір та зберігання персональних даних [166, 167; 133, с. 132].

За даними Уповноваженого Верховної Ради України з прав людини стан додержання законодавства про захист персональних даних виглядає наступним чином.

Протягом 2018 року на виконання повноважень контролю за додержанням законодавства про захист персональних даних Уповноваженим Верховної Ради України з прав людини було проведено такі заходи: розглянуто 806 повідомлень про порушення права на приватність; здійснено 41 перевірку щодо додержання законодавства про захист персональних даних, з яких 31 планова, 6 позапланових та 4 моніторингові візити; надано 488 роз'яснень законодавства про захист персональних даних; складено 14 протоколів про адміністративне правопорушення, з яких один протокол за ч. 2 ст. 188^{39} КУпАП, 11 протоколів за ч. 4 ст. 188^{39} КУпАП та 2 протоколи за ст. 188^{40} КУпАП; у межах інформаційно-просвітницької роботи проведено 10 навчальних заходів (лекцій, семінарів і тренінгів) та надано більш як сто телефонних консультацій суб'єктам відносин, пов'язаних із обробкою персональних даних. За результатами перевірок видано 45 приписів про усунення порушень вимог законодавства про захист персональних даних, виявлених під час перевірки [168, с. 81].

Протягом 2019 року Уповноваженим Верховної Ради України з прав людини розглянуто 1061 повідомлень, проведено 36 перевірок, складено та передано до суду 10 протоколів про адміністративне правопорушення за ч. 4 ст. 188^{39} КУпАП [169, с. 193-194]. Впродовж року Уповноваженим Верховної Ради України з прав людини проведено перевірки 36 володільців/розпорядників персональних даних, з них 27 – планових, 5 – позапланових та здійснено 4 моніторингові візити. Під час здійснення перевірок виявлено такі системні порушення володільцями персональних даних прав суб'єктів персональних даних: права на захист персональних даних від незаконної обробки та випадкової втрати у зв'язку із неналежним оформленням зобов'язань про нерозголошення персональних даних і незаконним розповсюдженням інформації про особу на запити третіх осіб; права на відкликання згоди на обробку персональних даних, на заперечення проти обробки персональних даних, на внесення застереження щодо обмеження обробки персональних даних у зв'язку із неправомірно визначеною підставою обробки персональних даних; права на отримання інформації щодо обробки персональних даних, в тому числі про умови надання доступу до персональних даних, зокрема інформацію про третіх осіб, яким передаються його персональні дані. Серед порушень також виявлено відсутність у володільців персональних даних внутрішніх документів, які регулюють порядок обробки та захисту персональних даних; зберігання в особових справах надмірної кількості копій документів про особу, що є ризиком їх незаконного використання, а отже – можливого порушення права особи на захист своїх персональних даних [169, с. 200].

У 2019 році Уповноваженим Верховної Ради України з прав людини в процесі здійснення повноважень виявлено, що в сфері фармаконагляду без належних правових підстав та відповідного нормативно-правового регулювання відбувається надмірна обробка персональних даних про стан здоров'я, пов'язаних із виявленням, збором, оцінкою, вивченням та запобіганням виникненню побічних реакцій, несприятливих подій після імунізації/туберкулінодіагностики та будь-яких інших питань, пов'язаних з безпекою та ефективністю застосування

лікарських засобів, вакцин, туберкуліну тощо. У зв'язку із зазначеним Уповноваженим Верховної Ради України з прав людини направлено на адресу МОЗ лист, в якому наголошується на необхідності вирішення цієї проблеми, а також в якості одного зі шляхів її вирішення запропоновано внести зміни до Порядку здійснення фармаконагляду, затвердженого наказом МОЗ України від 27 грудня 2006 року № 898, з метою приведення його у відповідність до Закону України «Про захист персональних» в частині здійснення фармаконагляду в знеособленому вигляді [169, с. 197-198].

З метою з'ясування стану захищеності права особи на приватність під час впровадження в Україні медичної реформи Уповноваженим Верховної Ради України з прав людини здійснено низку перевірок суб'єктів, які обробляють персональні дані в електронній системі охорони здоров'я, серед яких Національна служба здоров'я України, державне підприємство «Електронне здоров'я», власники електронних медичних інформаційних систем – ТОВ «Хелсі ЮА», ТОВ «Медстар солюшенс», ТОВ «Здоров'я 24», ТОВ «Сіет Холдінг» та медичні заклади, які надають первинну медичну допомогу, зокрема комунальні некомерційні підприємства «Центр первинної медико-санітарної допомоги Печерського району», «Центр первинної медико-санітарної допомоги «Русанівка» Дніпровського району м. Києва», 201 «Центр первинної медико-санітарної допомоги Жашківського району». Уповноваженим Верховної Ради України з прав людини видано 3 приписи про усунення порушення законодавства у сфері захисту персональних даних та надано рекомендації щодо застосування законодавства у сфері захисту персональних даних [169, с. 200-201].

Протягом 2020 року до Уповноваженого Верховної Ради України з прав людини надійшло 2031 повідомлення про порушення прав людини на захист персональних даних, що порівняно з 2019 роком (1061) майже удвічі більше. Збільшення повідомлень пов'язано з економічною кризою, спричиненою всесвітньою пандемією COVID-19. З метою здійснення парламентського контролю за додержанням права на захист персональних даних проведено 67 перевірок володільців та/або розпорядників персональних даних, відкрито 62

провадження, складено та передано до суду 9 протоколів про адміністративне правопорушення за ч. 4 ст. 188^{39} КУпАП [170, с. 21-22].

У 2020 році Уповноваженим Верховної Ради України з прав людини з метою контролю додержання права на приватність під час впровадження медичної реформи, зокрема, впровадження Електронної системи охорони здоров'я здійснено перевірки організації захисту персональних даних медичними закладами та додержання законодавства у сфері захисту персональних даних під час функціонування Електронної системи охорони здоров'я. За результатами здійснених контрольних заходів впровадження Електронної системи охорони здоров'я (які тривали з кінця 2019 року по липень 2020 року) виявлено системні порушення прав людини, зокрема встановлено: неправомірне витребування згоди на обробку персональних даних пацієнтів; невідповідне визначення володільця та розпорядника персональних даних пацієнтів, що позбавляє особу можливості оскаржити дії суб'єкта, який збирає та поширює персональні дані; недодержання принципу ненадмірності тощо. З метою недопущення порушення права на приватність під час обробки медичними закладами чутливих персональних даних у березні 2020 року Міністру охорони здоров'я України внесено подання Уповноваженого Верховної Ради України з прав людини, яким рекомендовано розробити та затвердити типовий договір між надавачем медичних послуг та оператором електронної медичної інформаційної системи, а також доопрацювати технічні вимоги до електронної медичної інформаційної системи. За результатами реагування Уповноваженого Верховної Ради України з прав людини відповідні норми враховано у Концепції розвитку електронної охорони здоров'я, затвердженій розпорядженням Кабінету Міністрів України від 28 грудня 2020 року № 1671-р [170, с. 30-31].

У 2021 році з метою перевірки стану додержання прав громадян на захист персональних даних під час здійснення їх обробки володільцями та/або розпорядниками персональних даних Уповноваженим Верховної Ради України з прав людини проведено 62 перевірки, винесено 54 приписи про усунення виявлених порушень [171, с. 24].

Протягом 2023 року до Уповноваженого Верховної Ради України з прав людини надійшло 1205 звернень (1336 повідомлень) щодо ймовірного порушення права на захист персональних даних, 652 повідомлення про незаконну обробку персональних даних, 190 повідомлень про порушення права на доступ до інформації про себе, з питань надання рекомендацій звернулося 274 заявники, з питань неналежної організації обробки персональних даних звернулися 220 заявників за відновленням порушених прав громадян. Упродовж 2023 року у сфері захисту персональних даних Уповноваженим Верховної Ради України з прав людини складено 38 протоколів про адміністративні правопорушення, із них: 29 – за статтею 188^{40} КУпАП, 9 – за статтею 188^{39} КУпАП [172, с. 212, 213, 215, 217].

Аналіз статистичної інформації щодо діяльності Уповноваженого Верховної Ради України з прав людини показує на присутність фактів порушення законодавства про захист персональних даних відповідними суб'єктами.

Дієвими правовими засобами захисту персональних даних у сфері охорони здоров'я є відновлючі заходи, метою яких є відновлення порушеного права, усунення перешкод в його реалізації, усунення реальної загрози порушення суб'єктивних прав протиправними діями.

У ст. 8 Закону України «Про захист персональних даних» встановлено, що суб'єкт персональних даних має право: пред'являти вмотивовану вимогу володільцю персональних даних із запереченням проти обробки своїх персональних даних; пред'являти вмотивовану вимогу щодо зміни або знищення своїх персональних даних будь-яким володільцем та розпорядником персональних даних, якщо ці дані обробляються незаконно чи є недостовірними; звертатися із скаргами на обробку своїх персональних даних до Уповноваженого Верховної Ради України з прав людини або до суду [46]. У ч. 1 ст. 18 Закону України «Про захист персональних даних» передбачено оскарження рішення про відстрочення або відмову в доступі до персональних даних до Уповноваженого Верховної Ради України з прав людини або суду [46].

Отже, з метою захисту своїх прав щодо медичних даних пацієнт має право:

1) звернутися до володільця чи розпорядника, дії або бездіяльність якого призвели, до порушення його права на захист персональних даних, із вмотивованою вимогою: про запереченням проти обробки персональних даних; про зміну персональних даних; про знищення персональних даних; про припинення будь-яких інших порушень законодавства про захист персональних даних.

2) звернутися до Уповноваженого Верховної Ради України з прав людини із скаргою щодо оскарження діяльності володільця, розпорядника, третіх осіб щодо обробки персональних даних стосовно: рішення про відстрочення або відмову в доступі до персональних даних; рішення про відмову в задоволені вмотивованої вимоги суб'єкта персональних даних щодо заперечення проти обробки персональних даних, а також їх зміни та/або знищення; будь-якого іншого рішення, дії чи бездіяльності, якими порушується законодавство про захист персональних даних.

3) звернутися до суду з позовом щодо: зобов'язання володільця та/або розпорядника персональних даних надати доступ до персональних даних; зобов'язання володільця та/або розпорядника персональних даних припинити обробку персональних даних, змінити персональні дані, знищити персональні дані; захисту своїх персональних даних від незаконної обробки та випадкової втрати, знищення, пошкодження у зв'язку з умисним приховуванням, ненаданням чи несвоєчасним їх наданням, а також на захист від надання відомостей, що є недостовірними чи ганьблять честь, гідність та ділову репутацію фізичної особи; відшкодування майнової і моральної шкоди, завданої правопорушеннями у сфері захисту персональних даних.

При цьому, слід враховувати, що в залежності від обставин справи позови можуть розглядатися як в порядку адміністративного (наприклад, володільцем та/або розпорядником персональних даних є НСЗ України) так і цивільного судочинства (наприклад, відшкодування майнової і моральної шкоди, завданої правопорушеннями у сфері захисту персональних даних).

Необхідно також зазначити, що ч. 3 ст. 55 Конституції України гарантує кожному після використання всіх національних засобів правового захисту звертатися за захистом своїх прав і свобод до відповідних міжнародних судових установ [55]. Тому за умови використання всіх національних засобів юридичного захисту пацієнт може звернутися до ЄСПЛ, рішення якого є обов'язковими для виконання Україною [173]. Судова практика ЄСПЛ визнає право на персональні дані таким, що охоплюється змістом ст. 8 Конвенції про захист прав людини і основоположних свобод від 4 листопада 1950 року, а саме правом на повагу до приватного і сімейного життя [124]. Згідно ч. 2 ст. 8 Конвенції про захист прав людини і основоположних свобод від 4 листопада 1950 року органи державної влади не можуть втручатись у здійснення цього права, за винятком випадків, коли втручання здійснюється згідно із законом і є необхідним у демократичному суспільстві в інтересах національної та громадської безпеки чи економічного добробуту країни, для запобігання заворушенням чи злочинам, для захисту здоров'я чи моралі або для захисту прав і свобод інших осіб [124]. ЄСПЛ, встановивши факт порушення Конвенції про захист прав людини і основоположних свобод, може застосувати один із таких способів захисту прав суб'єкта персональних даних: – присудження потерпілій стороні справедливої сатисфакції, яка охоплює як компенсацію моральної шкоди, так і відшкодування майнової шкоди. При цьому компенсація моральної шкоди може бути присуджена в грошовій формі або визнано, що висновок про порушення Конвенції, з усіма наслідками, які він потягне за собою у майбутньому, може вважатися достатньою справедливою сатисфакцією; – відновлення настільки, наскільки це можливо, попереднього юридичного стану, який суб'єкт персональних даних мав до порушення Конвенції про захист прав людини і основоположних свобод (restitutio in integrum); – інші заходи, передбачені у рішенні ЄСПЛ [17, с. 205].

Таким чином, правові засоби захисту персональних даних у сфері охорони здоров'я – це заходи компетентних суб'єктів, які спрямовані на запобігання, припинення правопорушення у сфері захисту медичних даних, відновлення порушеного права чи компенсацію заподіяної правопорушенням шкоди. Такими

заходами є превентивні, припиняючі та відновлючі. Превентивні заходи спрямовані на запобігання порушенням законодавства про захист персональних даних у сфері охорони здоров'я. Ці заходи зобов'язані застосовувати володільці, розпорядники та треті особи. Припиняючі заходи спрямовані на усунення та припинення порушення законодавства про захист персональних даних. Ці заходи уповноважені застосовувати володільці, розпорядники, треті особи та Уповноважений Верховної Ради України з прав людини. Відновлювальні заходи спрямовані на відновлення порушеного права, усунення перешкод в його реалізації та загрози порушення суб'єктивних прав протиправними діями. Ці заходи уповноважені застосовувати володільці, розпорядники, треті особи, Уповноважений Верховної Ради України з прав людини, суд.

Висновки до розділу 2

1. Обробка персональних даних у сфері охорони здоров'я здійснюється за умови надання пацієнтом однозначної згоди на обробку таких даних або на підставі закону. Обробка персональних даних у сфері охорони здоров'я без згоди пацієнта здійснюється: 1) коли медичні відомості необхідні в цілях охорони здоров'я (встановлення медичного діагнозу, забезпечення піклування чи лікування або надання медичних послуг, моніторинг відповідності встановленим умовам надання таких послуг функціонування електронної системи охорони здоров'я; контроль якості надання медичних послуг; обмін інформацією про фінансування медичних послуг та послуг у сфері охорони здоров'я); 2) для захисту життєво важливих інтересів суб'єкта персональних даних. Обробляти персональні дані без згоди пацієнта можна до часу, коли отримання згоди стане можливим. Обмеження щодо обробки персональних даних у сфері охорони здоров'я може здійснюватися у випадках, передбачених законом, наскільки це

необхідно у демократичному суспільстві в інтересах національної безпеки, економічного добробуту або захисту прав і свобод суб'єктів персональних даних чи інших осіб.

2. Суб'єкти забезпечення захисту персональних даних у сфері охорони здоров'я – це фізичні та юридичні особи, які зобов'язані забезпечити захист персональних даних у сфері охорони здоров'я від неправомірного збирання, зберігання, використання, знищення, поширення та доступу до медичних даних. Суб'єктами забезпечення захисту персональних даних у сфері охорони здоров'я є: 1) володільці персональних даних у сфері охорони здоров'я; 2) розпорядники персональних даних у сфері охорони здоров'я; 3) треті особи персональних даних у сфері охорони здоров'я; 4) Уповноважений Верховної Ради України з прав людини.

3. При визначенні володільця персональних даних у сфері охорони здоров'я необхідно виходити з реальних повноважень того чи іншого суб'єкта. Залежно від наявних повноважень, володільців персональних даних у сфері охорони здоров'я може бути декілька. Якщо володільців персональних даних у сфері охорони здоров'я двоє чи більше, то їх слід вважати співволодільцями персональних даних у сфері охорони здоров'я. У такому разі кожен з них нестиме відповідальність лише тією мірою, якою він відповідальний за здійснення повноважень володільця.

4. Розпорядником персональних даних у сфері охорони здоров'я можуть бути підприємства, установи і організації усіх форм власності, органи публічної влади, фізичні особи – підприємці, які обробляють персональні дані відповідно до закону. Розпорядником персональних даних у сфері охорони здоров'я, володільцем яких є орган публічної влади, крім цих органів, може бути лише підприємство державної або комунальної форми власності. Володілець персональних даних у сфері охорони здоров'я може доручити обробку персональних даних розпоряднику персональних даних відповідно до договору, укладеного в письмовій формі. Розпорядник персональних даних у сфері охорони здоров'я може обробляти персональні дані лише з метою і в обсязі, визначених у договорі.

5. Третя особа у відносинах щодо персональних даних у сфері охорони здоров'я з моменту отримання таких даних стає новим володільцем чи розпорядником таких даних, за умови наявності інших умов для кваліфікації цієї особи як володільця чи розпорядника та застосування законодавства про захист персональних даних. Третя особа, яка отримала від первісного володільця чи розпорядника персональні дані у сфері охорони здоров'я, вступає в нові правовідносини з суб'єктом таких даних в якості нового володільця чи розпорядника. Мета обробки персональних даних пацієнта не співпадає з метою обробки таких даних володільцем чи розпорядником, які їх надають, що зумовлено сферою діяльності таких суб'єктів і потребою оперування відомостями про певну особу.

6. Володільцями персональних даних у сфері охорони здоров'я можуть бути органи публічної влади (МОЗ України та НСЗ України (як виключення КМ України) та суб'єкти господарювання приватної форми власності, діяльність яких пов'язана з медичним обслуговуванням. Розпорядниками персональних даних у сфері охорони здоров'я можуть бути органи публічної влади та їх посадові особи, співробітники закладів охорони здоров'я публічної форми власності, суб'єкти господарювання приватної форми власності, діяльність яких пов'язана з медичним обслуговуванням, а також медичні працівники, співробітники медичного закладу, працівники, відповідальні за захист персональних даних у лікаря-підприємця. Третіми особами персональних даних у сфері охорони здоров'я можуть бути органи публічної влади та заклади охорони здоров'я будь-якої форми власності. Уповноважений Верховної Ради України з прав людини зобов'язаний забезпечити додержання законодавства про захист персональних даних володільцями, розпорядниками та третіми особами під час здійснення діяльності, пов'язаної з персональними даними у сфері охорони здоров'я.

7. Правові засоби захисту персональних даних у сфері охорони здоров'я – це заходи компетентних суб'єктів, які спрямовані на запобігання, припинення правопорушення у сфері захисту медичних даних, відновлення порушеного права

чи компенсацію заподіяної правопорушенням шкоди. Такими заходами є превентивні, припиняючі та відновлючі.

8. Превентивні заходи спрямовані на запобігання порушенням законодавства про захист персональних даних у сфері охорони здоров'я. Ці заходи зобов'язані застосовувати володільці, розпорядники та треті особи. Превентивні заходи щодо забезпечення захисту персональних даних у сфері охорони здоров'я вживаються на всіх етапах їх обробки, у тому числі за допомогою організаційних та технічних заходів. Повноваженнями застосування превентивних заходів захисту персональних даних у сфері охорони здоров'я наділений також Уповноважений Верховної Ради України з прав людини на підставі звернень фізичних і юридичних осіб або за власною ініціативою шляхом проведення планових, позапланових, виїзних та безвиїзних перевірок.

9. Припиняючі заходи спрямовані на усунення та припинення порушення законодавства про захист персональних даних. Ці заходи уповноважені застосовувати володільці, розпорядники, треті особи (безпосереднє усунення володільцем або розпорядником персональних даних порушень законодавства про захист персональних даних; отримання Уповноваженим Верховної Ради України з прав людини скарг фізичних і юридичних осіб з питань захисту персональних даних та приймати рішення за результатами їх розгляд тощо) та Уповноважений Верховної Ради України з прав людини (складає протокол про адміністративне правопорушення за порушення законодавства у сфері захисту персональних даних та невиконання законних вимог Уповноваженого Верховної Ради України з прав людини; у разі виявлення під час перевірки суб'єкта перевірки ознак кримінального правопорушення направляє необхідні матеріали до правоохоронних органів).

10. Відновлювальні заходи спрямовані на відновлення порушеного права, усунення перешкод в його реалізації та загрози порушення суб'єктивних прав протиправними діями. Ці заходи уповноважені застосовувати володільці, розпорядники, треті особи, Уповноважений Верховної Ради України з прав людини, суд. З метою захисту своїх прав щодо медичних даних пацієнт має право:

1) звернутися до володільця чи розпорядника, дії або бездіяльність якого призвели, до порушення його права на захист персональних даних, із вмотивованою вимогою: про запереченням проти обробки персональних даних; про зміну персональних даних; про знищення персональних даних; про припинення будь-яких інших порушень законодавства про захист персональних даних.

2) звернутися до Уповноваженого Верховної Ради України з прав людини із скаргою щодо оскарження діяльності володільця, розпорядника, третіх осіб щодо обробки персональних даних стосовно: рішення про відстрочення або відмову в доступі до персональних даних; рішення про відмову в задоволені вмотивованої вимоги суб'єкта персональних даних щодо заперечення проти обробки персональних даних, а також їх зміни та/або знищення; будь-якого іншого рішення, дії чи бездіяльності, якими порушується законодавство про захист персональних даних.

3) звернутися до суду з позовом щодо: зобов'язання володільця та/або розпорядника персональних даних надати доступ до персональних даних; зобов'язання володільця та/або розпорядника персональних даних припинити обробку персональних даних, змінити персональні дані, знищити персональні дані; захисту своїх персональних даних від незаконної обробки та випадкової втрати, знищення, пошкодження у зв'язку з умисним приховуванням, ненаданням чи несвоєчасним їх наданням, а також на захист від надання відомостей, що є недостовірними чи ганьблять честь, гідність та ділову репутацію фізичної особи; відшкодування майнової і моральної шкоди, завданої правопорушеннями у сфері захисту персональних даних.

За умови використання всіх національних засобів юридичного захисту пацієнт може звернутися до ЄСПЛ, рішення якого є обов'язковими для виконання Україною.

РОЗДІЛ 3
УДОСКОНАЛЕННЯ ПРАВОВОГО РЕГУЛЮВАННЯ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ У СФЕРІ ОХОРОНИ ЗДОРОВ'Я

3.1. Міжнародні та європейські стандарти захисту персональних даних у сфері охорони здоров'я

Сучасний етап розвитку правового регулювання захисту персональних даних у сфері охорони здоров'я в Україні характеризується інтенсивним пошуком ефективних правових інструментів, які б відповідали новітнім тенденціям безпеки персональної інформації пацієнтів. У цьому контексті актуальним є вивчення міжнародних та європейських стандартів захисту персональних даних у сфері охорони здоров'я для удосконалення вітчизняного законодавства про захист персональних даних та охорону здоров'я.

Вихідні положення правового регулювання захисту персональних даних у сфері охорони здоров'я визначені у міжнародно-правових актах стосовно захисту прав людини, зокрема у Загальній декларації прав людини від 10 грудня 1948 року [174], Конвенції про захист прав людини і основоположних свобод від 4 листопада 1950 року [124], Міжнародному пакті про громадянські і політичні права від 16 грудня 1966 року [175], Конвенції про права осіб з інвалідністю від 13 грудня 2006 року [176].

Згідно ст. 12 Загальної декларації прав людини від 10 грудня 1948 року ніхто не може зазнавати безпідставного втручання у його особисте життя і кожна людина має право на захист закону від такого втручання [174]. У ст. 8 Конвенції про захист прав людини і основоположних свобод від 4 листопада 1950 року передбачено право на невтручання до приватного життя, за винятком випадків, коли втручання здійснюється згідно із законом [124]. Згідно ст. 17 Міжнародного пакту про громадянські і політичні права від 16 грудня 1966 року ніхто не повинен зазнавати свавільного чи незаконного втручання в його особисте життя і кожна людина має право на захист закону від такого втручання [175]. Відповідно

до ст. 22 Конвенції про права осіб з інвалідністю від 13 грудня 2006 року жодна особа з інвалідністю не повинна наражатися на довільне чи незаконне посягання на недоторканість її приватного життя. Особи з інвалідністю мають право на захист закону від такого посягання. Держави-учасниці Конвенції про права осіб з інвалідністю охороняють конфіденційність відомостей про особу, стан здоров'я та реабілітацію осіб з інвалідністю нарівні з іншими [176].

Важливу роль у формуванні правового регулювання захисту персональних даних у сфері охорони здоров'я відіграли міжнародні документи Всесвітньої медичної асоціації. Ця міжнародна організація була утворена 17 вересня 1947 року на Першій Генеральній Асамблеї в Парижі і являє собою своєрідний парламент для лікарів, який представляє інтереси та права лікарів різних країн світу, формує та впроваджує міжнародні норми медичної діяльності, обов'язкові для усіх [177].

Серед міжнародних документів Всесвітньої медичної асоціації, які вплинули на правове регулювання захисту персональних даних у сфері охорони здоров'я, слід виокремити такі: Женевська декларація 1948 року (передбачено обов'язок для лікарів берегти таємницю, яку їм довірили, навіть після смерті пацієнта) [178], Міжнародний кодекс медичної етики (передбачено обов'язок для лікарів поважати пацієнта і дотримуватися конфіденційності пацієнта) [179], Дванадцять принципів організації охорони здоров'я для будь-якої національної системи охорони здоров'я (передбачено, що всі особи, які беруть участь у лікуванні пацієнта на будь-якій стадії лікування, або особи, які контролюють це лікування, повинні усвідомити і дотримувати конфіденційний характер взаємовідносин лікаря і пацієнта) [180], Лісабонська декларація стосовно прав пацієнта (закріплено право пацієнта на конфіденційність медичної і особистої інформації) [181], Положення про використання комп'ютерів в медицині (встановлено норми з приводу захисту інформації про пацієнта в умовах розвитку технічного прогресу і інформаційної комп'ютерної мережі) [182, с. 16], Положення про медичне обстеження, «телемедицину» та медичну етику (перший нормативний акт міжнародного характеру, який не тільки визначає право пацієнта, але й

встановлює вимогу його гарантування через встановлення правової відповідальності в разі порушення принципу конфіденційності) [182, с. 16], Тимчасове положення про СНІД (передбачено обов'язки для лікарів щодо збереження конфіденційності інформації про пацієнта) [183], Декларація про проєкт «Геном людини» (передбачено, що медична таємниця та інформація не повинна передаватись третім особам без згоди) [184], Положення про захист прав та конфіденційність пацієнта (передбачено механізми конфіденційності щодо пріоритетності етичних зобов'язань медичних працівників над договірними зобов'язаннями, пов'язаними з прийомом на роботу) [185].

До міжнародних актів, які мають значення для становлення інституту захисту персональних даних у сфері охорони здоров'я, доцільно також віднести Декларацію про політику в галузі забезпечення прав пацієнта в Європі (визначено перелік та умови конфіденційної інформації, а саме: вся інформація про стан здоров'я пацієнта, діагноз, прогноз та лікування його захворювання, а також будь-яка інша інформація особистого характеру повинна зберігатися в секреті, навіть після смерті пацієнта; конфіденційну інформацію можна розкрити тільки у разі, коли є згода пацієнта або на підставі закону; всі дані, які можуть розкриті особу пацієнта повинні бути захищені; пацієнти мають право доступу до всіх матеріалів щодо їх діагнозу та лікуванню, крім даних третіх осіб; заборонено будь-яке посягання на особисте та сімейне життя пацієнта за виключенням випадків, коли пацієнт не заперечує проти цього і необхідність посягання обумовлена цілями діагностики та лікування) [186] та Конвенцію про захист прав і гідності людини щодо застосування біології та медицини (у ст. 5 передбачено, що будь-яке втручання у сферу здоров'я може здійснюватися тільки після добровільної та свідомої згоди на нього відповідної особи. Такій особі заздалегідь надається відповідна інформація про мету і характер втручання, а також про його наслідки та ризики. Відповідна особа у будь-який час може безперешкодно відкликати свою згоду; у ст. 6 передбачено умови захисту осіб, які неспроможні дати згоду; у ст. 10 передбачено, що кожна особа має право на повагу до її особистого життя, коли йдеться про інформацію про здоров'я цієї особи. Кожна особа має право на

ознайомлення із будь-якою зібраною про її здоров'я інформацією. У виняткових випадках в інтересах пацієнта здійснення цих прав може обмежуватися законом) [187].

З приходом інформаційного суспільства та впровадженням комп'ютерів у різних сферах економічного та суспільного життя, Організація Економічної Співпраці і Розвитку стала першою міжурядовою організацією, яка у 1980 році ухвалила Керівні принципи про захист приватності та транскордонні потоки персональних даних. Положення, що їх містять, характеризуються своєю ясністю та гнучкістю для застосування та своїми формулюваннями, достатньо широкими для пристосування до технологічного прогресу. Принципи орієнтують усіх інформаційних агентів на їх дотримання під час комп'ютеризованої обробки даних про індивідів (від локальних комп'ютерів до мереж національного та міжнародного рівня) усіх типів персональних даних, що оброблятимуться (від адміністрування даних службою кадрів до складання профілю споживача), та усіх категорій даних (від допоміжних операційних до основних, від пересічних до вразливих). Ці принципи були впроваджені у величезній кількості національних регуляційних або саморегуляційних інструментах та до цього часу широко використовуються як у публічному, так і приватному секторах [188, с. 6, 37-40].

Поряд з цим, необхідно зазначити, що закріплення ключових міжнародних і, насамперед, європейських стандартів щодо захисту персональних даних у сфері охорони здоров'я відбулося в межах діяльності РЄ та ЄС.

У 1981 році РЄ була прийнята Конвенція про захист осіб у зв'язку з автоматизованою обробкою персональних даних (далі – Конвенція № 108) [63], яка стала першим у світі міжнародним правовим актом, який закріпив основоположні, уніфіковані принципи створення національного законодавства держав світу у сфері захисту персональних даних [189, с. 20-34]. Слід звернути увагу на те, що Конвенція № 108 не є «європейською», що відрізняє її від інших конвенцій РЄ. У цьому розумінні, стаття 23 несе в собі важливий елемент, оскільки дозволяє вступ до Конвенції держав, які не є членами РЄ. Це зроблено для того, щоб закласти фундамент для досягнення міжнародного консенсусу в

питаннях захисту персональних даних, особливо з третіми, неєвропейськими країнами [188, с. 13]. У Конвенції № 108 встановлено вимоги до медичних даних, а саме передбачено заборону на обробку даних стосовно стану здоров'я або статевого життя суб'єкта таких даних якщо внутрішнє законодавство не забезпечує відповідних гарантій, а також передачі даних до третіх країн, що не забезпечують відповідного рівня захисту [63].

З метою узгодження стандартів захисту персональних даних у Європі в 2001 році був прийнятий Додатковий протокол до Конвенції про захист осіб у зв'язку з автоматизованою обробкою персональних даних щодо органів нагляду та транскордонних потоків даних [64]. Крім того, у вересні 2009 року також був ініційований процес оновлення Конвенції № 108 і хоча положення модернізованої Конвенції № 108 в основному були доопрацьовані у 2014 році, її завершення було відкладено до прийняття Загального регламенту про захист даних ЄС 2016 року [53]. Основною причиною стало бажання забезпечити послідовність та узгодженість оновленої Конвенції № 108, яку зазвичай називають Конвенція № 108+, з правовою базою ЄС. У 2018 році текст Конвенції № 108 було оновлено Протоколом (CETS № 223) про внесення змін до Конвенції № 108, який наразі відкритий для підписання. Метою оновлення положень Конвенції № 108 було вирішення проблем, пов'язаних із приватністю, що виникають внаслідок використання новітніх інформаційно-комунікаційних технологій, та посилення механізму Конвенції № 108 для забезпечення її ефективного впровадження. У контексті захисту персональних даних у сфері охорони здоров'я Конвенція № 108+ встановлює особливий порядок обробки персональних даних, що стосуються здоров'я або статевого життя. Примітно, що оновлена Конвенція № 108+ повністю не копіює формулювання Загального регламенту про захист даних 2016 року, проте відображає подібні концепції і підходи щодо гарантування права на захист персональних даних. Втім, наразі єдиним юридично обов'язковим міжнародно-правовим актом глобального значення у сфері захисту персональних даних залишається Конвенція № 108. Незважаючи на динамічність процесу розвитку та модернізації положень Конвенції № 108, її оновлена редакція хоча і

гарантує право на захист персональних даних, проте ще не набрала чинності, відтак процес визнання та закріплення права на захист персональних даних у міжнародному праві не є завершеним [27, с. 31-34].

Європейське Економічне Співтовариство в перший раз згадує про захист даних у доповіді 1973 року, що була продовжена дебатами у Європейському Парламенті в 1974-75 роках. Про необхідність узгодження політики країн Європейських Співтовариств в цьому питанні йдеться у Резолюції, що була ухвалена Радою ЄС у липні 1974 року. У червні 1979 року Парламент ухвалив підготовлену експертами Комітету з правових питань Резолюцію «Про захист прав індивідів стосовно технічного розвитку і обробки даних», в якій робиться акцент на створені спільного ринку в обробці даних. У Резолюції, зокрема, зазначено, що національні положення в галузі захисту приватності мають безпосередній вплив на такий спільний ринок, а саме, здатні «деформувати умови конкуренції». У Рекомендації від 29 липня 1981 року № 81/679/ЕЕС, яка присвячена затвердженню РЄ Конвенції № 108, вказується про її прийнятність для створення однакового рівня захисту інформаційної приватності в Європі. Фактором, що активізував розробку документа, стала не вирішена повною мірою проблема транскордонної передачі даних як всередині Європи, так і при передачі даних за межі континенту. Випадок, який отримав значний резонанс, стався у 1991 році, коли Французьке агентство з питань захисту персональних даних заборонило компанії Фіат електронну передачу інформації про французьких працівників компанії до її головного офісу в Італії, доки Фіат не погодиться бути пов’язаною вимогами законодавства Франції про захист даних. Європейська Комісія подала проєкт директиви у вересні 1990 року після низки запитів Європейського Парламенту щодо необхідності вжиття заходів у цій галузі. З численними зауваженнями Європейського Парламенту проєкт подали на друге читання у жовтні 1992 року. У лютому 1994 року держави-члени дійшли політичної угоди стосовно основних положень директиви; і лише через рік Рада Міністрів ухвалила «спільну позицію», що була підтверджена Парламентом у червні 1995 року. Директива № 95/46/ЄС про захист фізичних осіб при обробці

персональних даних і про вільне переміщення таких даних набула чинності 24 жовтня 1995 року [188, с. 17-18].

Директива № 95/46/ЄС встановила загальні умови обробки персональних даних в державах-членах ЄС, порядок передачі даних до третіх країн, умови відповідальності та санкцій, а також вперше у міжнародному праві визначила організаційні питання, що пов'язані з правами та обов'язками наглядового органу [26, с. 34-35]. У Розділі ІІІ Директиви № 95/46/ЄС було регламентовано особливості обробки «вразливих даних». Відповідно до ст. 8 заборонялася обробка персональних даних стосовно здоров'я чи статевого життя особи. Обробка медичних даних здійснювалася за умови надання пацієнтом однозначної згоди на обробку таких даних. Обробка персональних даних у сфері охорони здоров'я без згоди пацієнта можлива була у разі захисту життєво важливих інтересів особи, якщо суб'єкт даних не може дати свою згоду через свою недієздатність чи неправоздатність, якщо обробка даних необхідна з метою профілактичної медицини, медичної діагностики, надання медичних послуг чи лікування або для служб охорони здоров'я, і якщо медичні дані обробляються медичним працівником або іншою особою, які зобов'язані дотримуватися медичної таємниці [190].

Аналізуючи положення Директиви № 95/46/ЄС можна дійти висновку, що правовий захист персональних даних здійснюється на основі: принципу персоноцентризму (слугує перш за все для захисту прав людини), принципу екстериторіальності (контролери даних незалежно від національності чи місця проживання фізичних осіб повинні поважати їх права), а також принципу субсидіарності (обробка персональних даних у ЄС повинна відбуватись згідно із законодавством однієї з держав-членів; повноваження контролера даних, створеного у державі-члені ЄС, повинні визначатися національним законодавством; держави-члени за власним бажанням визначають ризики для прав суб'єктів даних у своєму законодавстві) [191, с. 59]. Таким чином, у рамках ЄС первинне правове регулювання захисту персональних даних розглядалося у його тісному взаємозв'язку з правом на приватність [27, с. 29].

Фундаментальне значення у сфері захисту персональних даних ЄС відіграла Хартія про основоположні права, у ст. 8 якої було встановлено, що кожна людина має право на захист персональних даних щодо неї. Такі дані мають використовуватися належним чином для визначених цілей та на підставі згоди такої людини або інших обґрунтованих підставах, встановлених законом. Кожна людина має право на доступ до даних, зібраних щодо неї, та право на виправлення в них помилок. Дотримання цих правил підлягає контролю з боку незалежного державного органу [192]. Відтак саме Хартія ЄС, з одного боку, вперше закріпила у статті 8 право на захист персональних даних як самостійне право, відокремлене від права на захист приватного життя, а, з іншого боку, гарантувала його захист як основоположного права у ЄС. Піднесення захисту персональних даних до категорії основоположних прав на рівні ЄС мало вирішальне значення задля посилення ефективності захисту, який фактично надається фізичним особам через право ЄС в процесах, пов'язаних з обробкою персональних даних [27, с. 29-30].

Наступний крок еволюції у сфері захисту персональних даних був зроблений після прийняття Лісабонського договору. Новий Договір про функціонування ЄС передбачав загальне положення про захист даних, що містилось у ст. 16. Насправді, ця стаття виходить далеко за рамки простого перефразування ст. 286 Маахстрийського договору. В даній статті також мова про те, що «кожна людина має право на захист особистих даних, що стосуються її самої» (стаття 16 (1)). Крім того, в ній вказується використання «звичайної законодавчої процедури» при встановленні правил захисту персональних даних, які, зокрема, розглядаються державами-членами «при здійсненні діяльності, яка підпадає під сферу дії законодавства Союзу», і правила, що стосуються вільного переміщення таких даних» (ст. 16 (2)) [26, с. 36-37].

У світлі новітніх інформаційно-технологічних розробок Європейська Комісія розробила низку актів, що оновлюють систему захисту персональних даних в ЄС. Правовим актом, що оновив і деталізував засади захисту персональних даних, які були раніше викладені у Директиві 95/46/ЄС, є прийнятий 27 квітня 2016 року Регламент ЄС 2016/679 про захист фізичних осіб під час обробки персональних

даних та їх вільного обігу, та про скасування Директиви 95/46/ЄС (Загальний регламент про захист даних) [53].

Серед основних особливостей Загального регламенту про захист даних та його відмінностей від раніше чинної Директиви 95/46/ЄС можна виділити такі:

1) Загальний регламент про захист даних є актом прямої дії, має загальнообов'язковий характер та підлягає безпосередньому застосуванню без імплементації у національне законодавство держав-членів ЄС. Водночас Директива 95/46/ЄС є актом, що надавала державам-членам ЄС свободу розсуду в обранні форм і засобів досягнення результату, визначеного директивою;

2) матеріальна сфера дії Загального регламенту про захист даних поширюється на повну чи часткову автоматизовану обробку даних та обробку даних із використанням неавтоматизованих засобів, за виключенням обробки даних інституціями ЄС. Водночас матеріальна сфера застосування має низку обґрунтованих винятків та не застосовується до обробки персональних даних: в ході діяльності, що виходить за межі дії права ЄС; в ході діяльності, що виходить за межі глави 2 розділу V Договору про ЄС, що регламентує положення про спільну зовнішню та безпекову політику; обробки даних фізичними особами для задоволення особистих або побутових потреб; під час обробки компетентними органами в ході кримінального переслідування, виконання кримінальних покарань, у тому числі для захисту від загроз громадській безпеці або запобігання таким загрозам;

3) територіальна дія Загального регламенту про захист даних застосовується до обробки даних на основі визначення: території діяльності установи контролера або оператора, незалежно від фактичного місця обробки, 2) території поза межами ЄС, якщо обробка пов'язана із постачанням товарів чи наданням послуг суб'єктам даних на території ЄС або моніторингом поведінки суб'єктів даних, якщо така поведінка відбувається у межах ЄС (так званий критерій таргетингу), 3) території поза межами ЄС, якщо обробка здійснюється контролером через застосування державою членом права ЄС, що базується на міжнародному публічному праві,

зокрема це стосується діяльності консульств чи круїзних суден під державним прапором країнчленів ЄС;

4) Загальний регламент про захист даних визначає суб'єктів даних на яких поширюється, а саме, що його дія поширюється на всіх громадян держав-членів ЄС, а також резидентів ЄС, незалежно від їхнього громадянства чи місця проживання [27, с. 130-131].

Загальний регламент про захист даних 2016 року, на відміну від Директиви 95/46/ЄС, є актом прямої дії, що гарантує право на захист персональних даних на рівні основоположних прав людини та регламентує основні принципи захисту цього права. Водночас Загальний регламент про захист даних деталізував принцип законності (ст. 6), підставу обробки персональних даних за згодою суб'єкта даних (ст. 7, пункти 32, 33, 42 і 43 Преамбули), зміст прав суб'єкта персональних даних (право доступу до персональних даних, якими володіє суб'єкт даних про фізичну особу (ст. 15), право на виправлення (ст. 16). право на забуття – фізична особа може вимагати видалення персональних даних, якщо вона не бажає їх подальшої обробки, а суб'єкт даних не має обґрунтованих причин зберігати їх (ст. 17), право на обмеження обробки (ст. 18), право на мобільність даних (ст. 20), право на заперечення (ст. 21), посилив захист дітей (ст. 8), запровадив обов'язок оператора повідомляти контролера без необґрунтованої затримки після того, як йому стало відомо про порушення захисту персональних даних (ст. 33), містить положення про кібербезпеку (ст. ст. 5, 33, 34), встановив штрафні санкції за порушення правил обробки даних та матеріальну чи нематеріальну шкоду, заподіяну з вини контролера або оператора даних (ст. ст. 77-84) [53]. Окрім того, даний правовий акт значно збільшує категорію відомостей, що становлять персональні дані, передбачивши, серед іншого, захист даних про місцеперебування, онлайн- ідентифікаторів (IP-адреса, «cookies»), генетичних та біометричних даних. Важливим є й той факт, що Загальний регламент про захист даних 2016 року має екстериторіальне застосування, адже спрямований на захист прав людини не тільки на території ЄС, але і поза його межами [27, с. 30-31].

Крім цього, у Загальному регламенті про захист даних посилено передбачені Директивою 95/46/ЄС засоби захисту медичних даних щодо заборони обробки таких даних, в тому числі захисту генетичної інформації (п. 34, 53, ст. 9) [53]. У ст. 9 Загального регламенту про захист даних детально регламентовано обробку особливих категорій персональних даних («чутливих»), до яких відносяться медичні дані. За загальним правилом обробка медичних даних заборонена, за виключенням таких випадків: суб'єкт даних надав явну згоду на обробку даних; обробка є необхідною для цілей виконання обов'язків і здійснення спеціальних прав контролера або суб'єкта даних у сфері зайнятості та права соціального забезпечення і соціального захисту, якщо воно дозволено законодавством ЄС або держави-члена або колективною угодою згідно з законодавством держави-члена, що надає необхідні гарантії для фундаментальних прав та інтересів суб'єкта даних; обробка є необхідною для захисту життєво важливих інтересів суб'єкта даних або іншої фізичної особи, якщо суб'єкт даних фізично чи юридично неспроможний надати згоду; обробка здійснюється в ході відповідної законної діяльності з необхідними гарантіями установою, асоціацією чи будь-яким іншим некомерційним органом з політичною, філософською, релігійною ціллю або для цілі професійної спілки та за умови, що обробка стосується винятково членів чи колишніх членів органу або до осіб, що регулярно підтримують контакт з ними у зв'язку з його цілями, та що персональні дані не розкривають поза межами такого органу без згоди суб'єктів даних; обробка стосується персональних даних, що відкрито оприлюднені суб'єктом даних; обробка є необхідною для формування, здійснення або захисту правових претензій або якщо суди діють як судові органи; обробка є необхідною з причин суттєвого суспільного інтересу, на підставі законодавства ЄС або держави-члена, що має бути пропорційним цілі, якої прагнуть досягти, поважати сутність права на захист даних і передбачати належні та спеціальні заходи для захисту фундаментальних прав та інтересів суб'єкта даних; обробка є необхідною для цілей превентивної медицини чи гігієни праці, для оцінювання працездатності працівника, медичного діагнозу, надання послуг у сфері охорони здоров'я чи соціального забезпечення чи лікування або управління

системами та послугами в сфері охорони здоров'я чи соціального забезпечення чи лікування на підставі законодавства ЄС або держави-члена чи відповідно до контракту з медичним працівником і з урахуванням встановлених умов і гарантій; обробка є необхідною з причин суспільного інтересу в сфері охорони суспільного здоров'я, зокрема, захисту від серйозних транскордонних загроз здоров'ю чи забезпечення високих стандартів якості та безпеки в сфері охорони здоров'я і лікарських препаратів або медичного обладнання, на підставі законодавства ЄС або держави-члена, що передбачає належні та спеціальні заходи для захисту прав і свобод суб'єкта даних, зокрема, професійної таємниці; обробка є необхідною для досягнення цілей суспільного інтересу, цілей наукового чи історичного дослідження або статистичних цілей на підставі законодавства ЄС або держави-члена, що має бути пропорційним цілі, якої прагнуть досягти, поважати сутність права на захист даних і передбачати належні та спеціальні заходи для захисту фундаментальних прав та інтересів суб'єкта даних [53].

При цьому, Суд ЄС застосовує широке тлумачення «чутливих даних». Наприклад, коли хтось згадав на веб-сайті, що колега пошкодила ногу та працювала неповний робочий день за медичними показаннями, Суд ЄС у справі C-101/01 встановив, що це означало розголошення особистих даних щодо стану здоров'я [193, с. 267].

Захист персональних даних у сфері охорони здоров'я охоплює різні ступені кібербезпеки від використання медичного обладнання та індивідуальних гаджетів до хмарних сервісів, де зберігаються дані пацієнтів лікарень [194]. Ці питання визначені у Регламенті 2017/745 від 5 квітня 2017 року про медичні вироби, внесення змін до Директиви 2001/83/ЄС, Регламенту (ЄС) № 178/2002 і Регламенту (ЄС) № 1223/2009 та скасування директив Ради 90/385/ЄЕС і 93/42/ЄЕС [195]. Захист персональних даних у сфері електронних комунікацій регламентовано Директивою 97/66/ЄС від 15 грудня 1997 року стосовно обробки персональних даних і захисту права на невтручання в особисте життя в телекомунікаційному секторі [196], Директивою 2016/1148 від 6 липня 2016 року про заходи для високого спільного рівня безпеки мережевих та інформаційних

систем на території Союзу [197] та Директивою 2018/1972 від 11 грудня 2018 року про запровадження Європейського кодексу електронних комунікацій [198].

Питання застосування великих даних, алгоритмів та штучного інтелекту у сфері захисту персональних даних визначено Конвенцією № 108, Резолюцією Європейського Парламенту від 14 березня 2017 року про значення великих даних для основних прав: приватності, захисту персональних даних, недискримінації, безпеки та правозастосування (2016/2225 (INI)), Рекомендаціями щодо захисту фізичних осіб стосовно обробки персональних даних у світі Великих даних від 23 січня 2017 року, Резолюцією щодо Великих даних Уповноважених із захисту даних та приватності 2014 року, Висновками від 19 листопада 2015 року № 7/2015 «Прийняття викликів великих даних» та від 23 вересня 2016 року № 8/2016 «Когерентне забезпечення основних прав у еру Великих даних» [199, с. 379-383].

Великі дані та штучний інтелект викликають декілька питань щодо ідентифікації контролерів і операторів та їхньої відповідальності: коли така велика кількість даних збирається і обробляється, хто є їхнім власником? Хто є контролером, коли дані обробляються інтелектуальними машинами та програмним забезпеченням? Які конкретно обов'язки кожного суб'єкта в обробці даних? Та для яких цілей можуть використовуватися великі дані? Питання відповідальності в контексті штучного інтелекту стане ще більш складним, коли штучний інтелект прийматиме рішення на основі обробки даних, яку він розробив самостійно. Загальний регламент захисту персональних даних забезпечує правову базу для відповідальності контролерів чи операторів даних. Неправомірна обробка персональних даних передбачає відповідальність контролера та оператора даних. Штучний інтелект та автоматизоване прийняття рішень викликають питання про те, хто несе відповідальність за порушення, які зачіпають приватність суб'єктів даних, коли складність і кількість оброблюваних даних не можуть бути визначені з певністю. Якщо штучний інтелект та алгоритми розглядаються як продукти, виникає дилема між персональною відповідальністю, яка регулюється Загальним регламентом захисту персональних даних, та відповідальністю за продукт, яка ним не врегульована. Для цього необхідне

створення норм щодо відповідальності з метою заповнення прогалини між персональною відповідальністю та відповідальністю за продукт, наприклад робототехніку та штучний інтелект, в тому числі автоматизоване прийняття рішень [199, с. 384-385].

Оновлена Конвенція № 108 наділяє суб'єктів даних новими правами для здійснення більш ефективного контролю за своїми персональними даними в епоху великих даних. Це стосується, наприклад, щодо права не підлягати рішенням, що мають значний вплив на особу і прийняті виключно на основі автоматизованої обробки даних, без врахування його або її думки; права на вимогу отримувати відомості про причини обробки даних, якщо результати такої обробки застосовуються до нього або неї, а також права на заперечення. Інші положення Оновленої Конвенції № 108, зокрема щодо прозорості та додаткових зобов'язань, є додатковими елементами механізму захисту, встановленого Оновленою Конвенцією № 108 для подолання цифрових викликів [199, с. 386]. У Загальному регламенті про захист даних питання застосування великих даних, алгоритмів та штучного інтелекту регламентовано у ст. 21 (право на заперечення), ст. 22 (автоматизоване індивідуальне вироблення й ухвалення рішень, у тому числі, профайлінг) та ст. 23 (обмеження) [53].

Значну роль у забезпеченні дотримання стандартів захисту персональних даних у сфері охорони здоров'я мають документи рекомендаційного характеру Ради Європи, які хоча й не є обов'язковими, проте сприяють узгодженню керівних принципів захисту медичних даних. Наприклад, Рекомендація № R (81) 1 та Рекомендація № R (97); ДНК (Рекомендація № R (92); дані, отримані в результаті генетичних тестів (Рекомендація CM/Rec (2016); дані, пов'язані зі здоров'ям (Рекомендація CM/Rec (2019) [27, с. 72].

Вагоме значення в утвердженні захисту персональних даних у сфері охорони здоров'я відіграла судова практика ЄСПЛ щодо розгляду порушень ст. 8 Конвенції про захист прав людини і основоположних свобод, яка гарантує право на повагу до приватного життя. Доцільно відмітити, що крім виконання рішень ЄСПЛ державами-учасники Конвенціїї про захист прав людини і основоположних

свобод зобов'язані здійснювати загальні і індивідуальні заходи, які є необхідним у рамках внутрішньої правової системи, аби покласти край виявленому порушенню та виправити негативні наслідки такого порушення, про що свідчить рішення ЄСПЛ у справі Scozzari and Giunta v. Italy [200].

В одному з рішень у справі щодо захисту персональних даних у сфері охорони здоров'я ЄСПЛ зазначив, що захист персональних даних, у тому числі медичних відомостей, має фундаментальне значення для реалізації людиною свого права на повагу до приватного і сімейного життя. Дотримання конфіденційності відомостей про здоров'я є особливо важливим принципом правових систем усіх учасників Конвенції. Передача таких відомостей може серйозно вплинути на приватне та сімейне життя громадян, а також на їх соціальне становище та трудову зайнятість, оскільки робить їх об'єктом наруги та можливих утисків. З іншого боку, дотримання конфіденційності даних про здоров'я має ключове значення не тільки для захисту приватного життя пацієнта, а й для збереження його довіри до медичних працівників та системи охорони здоров'я загалом. За відсутності таких гарантій захисту особи, що потребують медичної допомоги, можуть утриматися від звернення за необхідним лікуванням, наражаючись тим самим на небезпеку власного здоров'я [118, с. 160-161; 201, с. 8-22].

За роки свого існування ЄСПЛ напрацював широкий пласт позицій з приводу захисту персональних даних. Уся практика ЄСПЛ у цій сфері наголошує на необхідності дотримання «трискладового тесту» правомірності втручання держави у сферу персональних даних: 1) згідно із законом; 2) відповідно до легітимної мети; 3) пропорційними засобами. У своїх рішеннях у справах «Leander v. Sweden» [202, с. 9-44], «Rotaru V. Romania» [203], «Catt v. United Kingdom» [204], «S. & Marper v. United Kingdom» [205], GSB v. Switzerland [206] ЄСПЛ сформулював ряд своїх ключових позицій: законній обробці персональних даних має передувати визначення конкретних легітимних цілей такої обробки; за відсутності підстав, передбачених законодавством країн, третя особа не вправі обробляти персональні дані особи; наявність легальної підстави здійснення

операцій із персональними даними та їх чітке регулювання спеціальним законодавством і регламентами, які відповідають верховенству праву та критерію якості закону, зокрема. допустимість періодичного оновлення персональних даних виключно у випадку їх закономірної зміни за заявою суб'єкта персональних даних; адекватність заходів обробки та захисту персональних даних та їх пропорційність до цілей такої обробки та захисту; тривалість обробки персональних даних не має перевищувати строк, який необхідний для досягнення цілей такої обробки; щодо категорії «чутливих даних» та висновку, що ризик шкідливості обробки даних загалом залежить не від вмісту, що несуть дані, а від контексту, в якому вони використані [207, с. 169-170]

Необхідно зазначити, що у сфері захисту персональних даних рішення ЄСПЛ проти України стосувалися саме проблеми захисту персональних даних про стан здоров'я та медичної інформації.

Так, у справі «Пантелеєнко проти України» ЄСПЛ встановив порушення ст. 8 Конвенції про захист прав людини і основоположних свобод через розголошення конфіденційної медичної інформації стосовно психічного здоров'я і психіатричного лікування заявника у рамках розгляду справи про наклеп та відсутність внутрішнього засобу правового захисту для оскарження та отримання компенсації за розкриття такої інформації [208]. Примітно, що у справі «Пантелеєнко проти України» порушення сталося не внаслідок відсутності певних законодавчих норм, а через неправильне застосування судом національного законодавства стосовно збирання, зберігання, використання та поширення інформації про стан психічного здоров'я особи, яке, до того ж не було вирішальним для судового процесу [27, с. 196]. Подібною є також справа «Заїченко проти України (№ 2), яка стосується питання законності дій органів внутрішніх справ щодо збирання відомостей про стан здоров'я заявника, що не було необхідними для розгляду на національному рівні справи про адміністративні правопорушення [209]. У цій справі ЄСПЛ також констатував порушення прав заявника через відсутність спеціальних положень національного законодавства, що регламентували б порядок проведення примусового

обстеження (і, зокрема, збору інформації про психічний стан здоров'я) в рамках розгляду справи про скоєння адміністративного правопорушення [27, с. 197].

У справі «М.К. проти України» було встановлено порушення права заявниці на повагу до її приватного життя через те, що вона не була належним чином поінформована про результат тестування на ВІЛ, яке було проведене під час її регулярного огляду у військовому госпіталі [210]. Як наслідок, інформація про ВІЛ позитивний статус військовослужбовиці була розголошена її матері та за місцем її служби. Хоч ця справа стосувалася законодавства, яке було змінено невдовзі після обставин, що мали місце у справі, але це рішення вкотре наголошує на важливості захисту чутливих даних, а також необхідність отримання чіткої згоди на обробку таких даних. Примітно, що у цій справі ЄСПЛ посилався на свої попередні висновки у справі Surikov v. Ukraine, що стосувалася свавільного збору та зберігання роботодавцем відомостей про психічне здоров'я заявника, які мали характер чутливих даних, були застарілими та невідповідними, а також подальше їх використання для розгляду питання про підвищення заявника та розповсюдження колегам заявника в процесі прийняття рішення роботодавцем і в ході публічного слухання. У цьому рішенні ЄСПЛ наголосив, що спосіб, у який законодавство України було розтлумачене і застосоване національними судами, дозволяло зберігати дані про стан психічного здоров'я заявника впродовж тривалого періоду, а також використання цих даних для цілей, не пов'язаних з початковою метою їх збору [27, с. 197].

Зважаючи на те, що рішення ЄСПЛ є обов'язковими та розглядаються як джерело права, відповідно, при розгляді подібних справ висновки ЄСПЛ повинні використовуватися як усталена правова позиція для усіх національних судів. Відтак рішення ЄСПЛ у справах щодо захисту персональних даних у сфері охорони здоров'я сприяють формуванню єдиного підходу до правозастосування та належного впровадження на практиці європейських стандартів захисту персональних даних і відповідних гарантій, які повинні бути включені в національне законодавство задля запобігання свавільному втручанню в основоположні права людини, включаючи право на захист персональних даних, і

забезпечення справедливого балансу між конкуруючими правами людини. Відповідно, одним з суттєвих аспектів виконання відповідних міжнародних зобов'язань є оновлення та модернізація вітчизняного законодавства у сфері захисту даних відповідно до сучасних європейських стандартів та його орієнтованість на підходи, висвітлені у практиці ЄСПЛ [27, с. 198-199].

Таким чином, у міжнародному та європейському правопорядку право на захист персональних даних є основоположним правом на рівні з правом на приватне життя. Міжнародні та європейські стандарти захисту персональних даних у сфері охорони здоров'я спрямовані на забезпечення захисту прав пацієнтів при обробці їх персональних даних. Міжнародне та європейське правове регулювання захисту персональних даних у сфері охорони здоров'я складається із низки правових актів різного характеру.

Аналіз міжнародних стандартів захисту персональних даних у сфері охорони здоров'я дає підстави класифікувати міжнародні стандарти правового регулювання захисту персональних даних у сфері охорони здоров'я на міжнародні акти загального характеру, які регулюють захист персональних даних у сфері охорони здоров'я опосередковано (Загальна декларація прав людини, Конвенція про захист прав людини і основоположних свобод, Міжнародний пакт про громадянські і політичні права, Конвенція про права осіб з інвалідністю) та міжнародні документи, які безпосередньо стосуються захисту персональних даних у сфері охорони здоров'я (Женевська декларація, Міжнародний кодекс медичної етики, Дванадцять принципів організації охорони здоров'я, Лісабонська декларація стосовно прав пацієнта, Положення про використання комп'ютерів в медицині, Положення про медичне обстеження, «телемедицину» та медичну етику, Тимчасове положення про СНІД, Декларація про проєкт «Геном людини», Положення про захист прав та конфіденційність пацієнта, Конвенція про захист прав і гідності людини щодо застосування біології та медицини, Керівні принципи про захист приватності та транскордонні потоки персональних даних, Декларація про політику в галузі забезпечення прав пацієнта в Європі, Конвенція про захист осіб у зв'язку з автоматизованою обробкою персональних даних).

Європейські стандарти правового регулювання захисту персональних даних у сфері охорони здоров'я характеризуються значним масивом нормативних актів регіонального рівня (наприклад, Конвенція про захист осіб у зв'язку з автоматизованою обробкою персональних даних), первинного (установчі договори ЄС) та вторинного (регламенти, директиви, резолюції, рекомендації, висновки) права ЄС.

3.2. Напрями вдосконалення правового регулювання захисту персональних даних у сфері охорони здоров'я

Захист персональних даних є одним із основних напрямів забезпечення інформаційної безпеки України [211]. Правові відносини, пов'язані із захистом персональних даних, характеризуються наступними проблемами: неузгодженість законодавства України про захист персональних даних з європейськими стандартами; відсутність ефективних засобів захисту права на приватність, запобігання і протидії порушенням законодавства про захист персональних даних під час обробки персональних даних; відсутність дієвого інституційного механізму незалежного контролю за додержанням права на захист персональних даних; існування надмірних баз персональних даних, володільцями або розпорядниками яких є органи державної влади, органи місцевого самоврядування, підприємства державної або комунальної форми власності, що належать до сфери управління таких органів; існування практики порушення права на невтручання в особисте і сімейне життя осіб, які перебувають у місцях несвободи [212]. Одним із завдань, спрямованих на вирішення цих проблем, є забезпечення дотримання права на приватність у медичній сфері [212].

У Рішенні ЄСПЛ у справі «M. S. v. Sweden» було визнано фундаментальну важливість захисту персональних даних, у тому числі медичного характеру, у реалізації права на повагу до особистого життя [213]. Дотримання конфіденційності даних про стан здоров'я є життєво важливим принципом правових систем усіх держав-членів Конвенції про захист прав людини і основоположних свобод. Як визначено Рішенням, вкрай важливо не лише поважати почуття приватності пацієнта, але й зберегти його довіру до медичної професії та медичних послуг загалом. При цьому національне законодавство має передбачати належні гарантії для запобігання будь-якому розголошенню персональних даних. Вказане Рішення обґрунтовує потребу у постійному розвитку законодавства про захист персональних медичних даних як гарантії забезпечення права на недоторканість приватного життя людини і громадянина [28, с. 498].

До сучасних проблем, які обмежують належний розвиток сфери захисту персональних медичних даних, відносять: невідповідність нормативно-правової бази сучасному стану інформатизації сфери охорони здоров'я; ігнорування ліцензійних засобів обробки та зберігання медичних даних, що гальмує процес інтеграції вітчизняних медичних інформаційних систем до європейського інформаційного простору; надмірна кількість персональних даних пацієнтів, що зберігаються в єдиній базі даних; відсутність контролю з боку державних органів за діяльністю приватних операторів медичних інформаційних систем; недостатній рівень комп'ютерної грамотності медичних працівників та відсутність ІТ-фахівців у закладах надання медичної допомоги; ігнорування стандартів не лише правового і організаційного, а й технічного захисту інформації тощо [214, с. 28-29; 215; 28, с. 498].

Нинішній Закон України «Про захист персональних даних» в переважній більшості містить загальні норми дії без чіткого розмежування конкретних сфер суспільних відносин, що призводить до неузгодженості та протиріччя стосовно захисту персональних даних у сфері охорони здоров'я. Тому з метою належного правового регулювання суспільних відносин у сфері захисту персональних даних

необхідно у Законі України «Про захист персональних даних» передбачити як загальні питання захисту персональних даних, так і регулювання суспільних відносин, пов'язаних з захистом персональних даних в конкретних сферах, у тому числі охорони здоров'я. При цьому правові особливості захисту персональних даних у сфері охорони здоров'я доцільно упорядкувати як у законодавстві про захист персональних даних, так і в законодавстві України про охорону здоров'я.

Одним із питань, яке потребує законодавчого вирішення, є унормування термінологічного визначення понять у відносинах щодо захисту персональних даних у сфері охорони здоров'я, а саме: «персональні дані», «персональні дані у сфері охорони здоров'я», «захист персональних даних», «згода суб'єкта персональних даних», «володілець персональних даних», «розпорядник персональних даних», «третя особа», «безпека персональних даних», «обробка персональних даних», «база персональних даних», «знеособлення персональних даних», «псевдонімізація», «профілювання», «стан здоров'я», «генетичні дані», «таємниця про стан здоров'я», «лікарська таємниця», «медична інформація», «медичне обслуговування», «медична послуга» тощо. Наведені категорії є системоутворюючими для захисту персональних даних у сфері охорони здоров'я і вони потребують чіткого та однозначного законодавчого трактування. При цьому вони мають відповідати європейським стандартам.

Наприклад, концепція вітчизняного медичного законодавства неповною мірою враховує настанови європейських інституцій щодо захисту приватності життя пацієнтів. Перш за все йдеться про Закон України «Основи законодавства України про охорону здоров'я», в якому відсутній одноманітний підхід до змістовного наповнення поняття «стан здоров'я». Зокрема, воно характеризується як: 1) «медична інформація», тобто інформація для пацієнта (ч. 3 ст. 39), яку становлять відомості про стан його здоров'я, мету проведення запланованих досліджень і лікувальних заходів, прогноз можливого розвитку захворювання, у тому числі наявність ризику для життя і здоров'я. Слід вказати на відсутність обов'язку повідомляти пацієнта про результати лікувальних заходів; 2) «таємниця про стан здоров'я» (ст. 39^1), яка, крім відомостей про стан здоров'я пацієнта,

містить факт звернення за медичною допомогою, діагноз, відомості, одержані у його медичному обстеженні; 3) «лікарська таємниця» (ст. 40), тобто інформація про хворобу, медичне обстеження, огляд та їх результати, інтимну та сімейну сторони життя громадянина. Аналізуючи ці положення, зазначимо, що усі види такої інформації становлять медичну інформацію, причому інформація про пацієнта може бути ширшою, ніж інформація для пацієнта, оскільки ч. 4 ст. 39 Закону України «Основи законодавства України про охорону здоров'я» перебачає право лікаря надавати неповну інформацію, обмежити можливість ознайомлення з окремими медичними документами, якщо інформація про хворобу пацієнта може погіршити стан його здоров'я або стан здоров'я інших осіб, які мають піклуватися про пацієнта, зашкодити процесові лікування [36]. Необхідно зауважити, що в загальному вигляді складники медичної інформації представлені в Законі України «Основи законодавства України про охорону здоров'я», частково – в спеціальних законах; інформація про пацієнта в спеціальних законах взагалі не позначена, а зміст лікарської таємниці конкретизується в законах «Про психіатричну допомогу» [121] та «Про захист населення від інфекційних хвороб» [122; 118, с. 164]. Однак інший підхід до обмеження інформаційних прав пацієнта міститься в пункті 2.3 Декларації про політику в галузі забезпечення прав пацієнта в Європі: інформація може бути прихована від пацієнта лише в тих випадках, коли є переконливі підстави вважати, що надання медичної інформації не тільки не принесе користі, а й серйозно зашкодить його здоров'ю [186]. Виникає питання і про доцільність збереження у вітчизняному законодавстві наведеної «тріади» позначень, по суті, того ж самого поняття. Однозначна відповідь міститься в Рекомендації № R (97) 5 Комітету Міністрів РЄ, відповідно до якої термін «медичні дані» стосується всіх особистих даних про стан здоров'я фізичної особи. Це також охоплює дані, які чітко та тісно пов'язані з даними про стан здоров'я, а також генетичними даними. Більш лаконічне визначення цього феномена міститься в Рекомендації Ради ОЕСР щодо управління персоналом – медичною є будь-яка інформація, що стосується цієї особи, яка ідентифікована або може бути ідентифікована [118, с. 161-162].

Важливе значення для захисту персональних даних у сфері охорони здоров'я має належне правове регулювання особливостей захисту даних пацієнта, а саме: чітке розуміння принципів обробки персональних даних, підстав та вимог до обробки медичних даних, прав пацієнта як суб'єкта персональних даних (зокрема, право на інформацію, право на доступ до персональних даних, право на виправлення персональних даних, право на забуття персональних даних, право на обмеження обробки персональних даних, право на мобільність персональних даних, право на заперечення проти обробки персональних даних, право на захист від автоматизованого прийняття рішення, право на захист своїх прав та відшкодування шкоди), порядку та умов надання згоди пацієнта на обробку його персональних даних, обов'язків володільця (контролера) персональних даних та розпорядника (оператора) персональних даних, порядку передачі медичних даних на територію іноземної держави або міжнародній організації, порядку та умов доступу до медичних даних третіх осіб, вимог до суб'єктів інформаційного забезпечення системи охорони здоров'я. Слід вказати і на не відповідність внутрішніх нормативних документів суб'єктів господарювання у сфері медичного обслуговування положенням законодавства про захист персональних даних, оскільки такі акти не у повному обсязі регламентують особливості захисту персональних даних у сфері охорони здоров'я [216, 217, 218]. Доцільно також передбачити, що персональні дані у сфері охорони здоров'я повинні обробляти виключно медичні працівники або особи чи органи, які працюють від імені медичних працівників, з дотриманням встановлених правил конфіденційності. На нашу думку, питання, пов'язані із захистом медичних даних доцільно врегулювати в новому Законі України «Про захист персональних даних», передбачивши у ньому окремий розділ «Захист персональних даних у сфері охорони здоров'я».

Необхідно відмітити, що принципи обробки персональних даних, наведені в Законі України «Про захист персональних даних» (законність (ч. 5 ст. 6), визначеність мети (ч. 1 ст. 6), відкритість і прозорість (ч. 1 ст. 6), точність і достовірність (ч. 2 ст. 6), відповідність, адекватність і ненадмірність (ч. 3 ст. 6),

ефективність захисту персональних даних (ч. 1 ст. 24)) [46] та ст. 5 Загального регламенту захисту персональних даних [53] стосуються будь-якої сфери, в тому числі охорони здоров'я. Водночас слід зазначити, що персональні дані у сфері охорони здоров'я відносяться до «чутливих даних», тому, на нашу думку, у законодавстві про охорону здоров'я доцільно передбачити спеціальний принцип обробки персональних даних у сфері охорони здоров'я. Основним нормативно-правовим актом у сфері охорони здоров'я є Закон України «Основи законодавства України про охорону здоров'я», у ст. 4 якого передбачено основні принципи охорони здоров'я [36]. Серед цих принципів відсутній спеціальний принцип обробки персональних даних у сфері охорони здоров'я. У зв'язку з цим важливо доповнити ст. 4 Закону України «Основи законодавства України про охорону здоров'я» таким принципом як захищеність інформації про медичне обслуговування особи та відомостей щодо її стану здоров'я. Дотримання цього принципу, в сукупності з іншими принципами обробки персональних даних, усіма суб'єктами відносин щодо медичного обслуговування, сприятиме ефективному захисту персональних даних у сфері охорони здоров'я [219, с. 41].

Особливої уваги потребує належне правове регулювання захисту персональних у сфері охорони здоров‘я в умовах воєнного стану в Україні, оскільки під час дії такого правового режиму може обмежуватися право на приватність.

Після російського повномасштабного вторгнення в Україну у 2022 році було прийнято Закон України «Про державну реєстрацію геномної інформації людини» [220]. Згідно ст. 1 цього Закону геномна інформація людини – це відомості про генетичні ознаки людини, тобто персональні дані у сфері охорони здоров'я, а саме генетичні дані (зразки ДНК). Поняття геномної інформації визначене доволі широко, адже включає фактично будь-які відомості про генетичні ознаки людини. У розумінні законодавства про захист персональних даних геномна інформація належить до чутливих персональних даних, тобто відомостей, які підлягають особливому порядку обробки та відповідним гарантіям захисту. Варто звернути увагу, що ст. 6 Конвенції № 108 закріплює вимогу, що персональні дані не

можуть піддаватися автоматизованій обробці, якщо внутрішнє законодавство не забезпечує відповідних гарантій. Тому, перш за все, прийняття Закон України «Про державну реєстрацію геномної інформації людини» є важливим для виконання вимог міжнародних зобов'язань. Головним чином геномна інформація використовується в кримінальному провадженні для розкриття злочинів, розшуку безвісти зниклих, ідентифікації загиблих, а також ідентифікації осіб, які не здатні через стан здоров'я, вік або інші обставини повідомити інформацію про себе. Враховуючи масові порушення прав людини з якими Україна стикнулася з початком повномасштабного вторгнення, прийняття згаданого закону може позитивно відзначитися на ефективному розслідування воєнних злочинів та пошуку зниклих безвісти. Примітно, що цим Законом також передбачено можливість обміну геномною інформацією з іншими країнами та міжнародними організаціями під час кримінального провадження, що може принести позитивні результати в контексті розслідування воєнних злочинів, вчинених на території України [27, с. 190-191].

Однак деякі положення Закону України «Про державну реєстрацію геномної інформації людини» мають певні ризики щодо забезпечення прав суб'єкта даних. Так, попри те, що геномна інформація є чутливими персональними даними, право на її використання належить широкому колу суб'єктів. Водночас цим Законом передбачені доволі тривалі строки зберігання геномної інформації (впродовж 50 років), що несе істотні ризики, зокрема у разі потенційної загрози витоку такої інформації. З урахуванням законодавства у сфері захисту персональних даних саме володілець (контролер) даних повинен вживати всіх організаційних та технічних заходів для забезпечення безпеки даних, що обробляються. Втім, у прийнятому Законі відсутні чіткі гарантії та запобіжники щодо попередження ризику втрати геномної інформації чи її витоку, а також не закріплений обов'язок володільця (контролера) повідомити особу про такі порушення безпеки персональних даних. Фактично питання запобігання ризику розкриття інформації для інших цілей чи її розголошення, у тому числі шляхом несанкціонованого доступу, в законі чітко врегульовано лише щодо обміну геномною інформацією з

іншими країнами чи міжнародними організаціями під час кримінального провадження. Крім того, не конкретизовані й питання можливості вилучення геномної інформації у зв'язку зі смертю особи, яка її надала, що необхідно для того, щоб мінімізувати ризики доступу до чутливих персональних даних родичів такої особи. Так само відсутні положення щодо права на видалення і відкликання згоди на обробку геномної інформації особою, яка їх надала, адже у ст. 8 Закону України «Про державну реєстрацію геномної інформації людини» визначено перелік категорій осіб, які під час дії воєнного стану обов'язково надають біологічні матеріали для державної реєстрації, зокрема, до таких осіб відносять військовослужбовців, поліцейських, осіб рядового та начальницького складу служби цивільного захисту, а також членів добровольчих формувань територіальних громад. До того ж за порушення законодавства у сфері державної реєстрації геномної інформації, яка належить до персональних даних у сфері охорони здоров'я, фактично передбачена загальна адміністративна та кримінальна відповідальність за порушення законодавства у сфері персональних даних. Інший аспект ризиків, пов'язаних з обробкою таких даних, виявляється у тому, що у законі не прописаний чітко механізм контролю за дотриманням законності при обробці геномної інформації, хоча і міститься загальне положення, що контроль за додержанням прав людини здійснює Уповноважений. Відтак, попри те, що прийняття вказаного закону є позитивним кроком в контексті виконання Україною своїх міжнародних зобов'язань у відповідь на ризики, що виникають у зв'язку з введенням воєнного стану, в аспекті обробки геномної інформації вкотре постає основна проблема захисту персональних даних у сфері охорони здоров'я в Україні [27, с. 191-192].

На відносини у сфері медичного обслуговування також суттєво впливають цифровізація та інформатизація. В цих умовах здійснюється накопичення великих обсягів інформації, зокрема і персональних даних у сфері охорони здоров'я. Як наслідок зростає кількість кібератак. У 2023 році кількість зареєстрованих в Україні кіберінцидентів зросла на 62,5% порівняно з попереднім, 2022 роком

[221; 172, с. 213]. Через потенційні загрози постає проблема безпеки та конфіденційності персональних даних у сфері охорони здоров'я.

В цих трансформаційних процесах значну увагу привертає застосування технологій штучного інтелекту, що вимагає встановлення відповідного правового регулювання у сфері захисту персональних даних, у тому числі охорони здоров'я.

Більшість технологій штучного інтелекту мають згубний вплив на право на приватність. Штучний інтелект за своєю природою потребує даних, вони в основному ґрунтуються на алгоритмах, які автоматично аналізують величезні набори даних для створення відповідей. Крім того, навіть якщо такі методи, як диференціальна конфіденційність, використовуються для захисту конфіденційності окремих осіб, технології штучного інтелекту можуть генерувати інформацію з таких даних, які потім використовуються для прогнозування і діяти відповідно до особистих характеристик конкретної особи, при цьому утримуючись від ідентифікації фізичної особи. Швидкий розвиток технологій і глобалізація зумовили виникнення нових проблем для забезпечення захисту персональних даних у сфері охорони здоров'я. Багато технологій штучного інтелекту засновані на тому, що задіюють великі масиви даних, в які входить також і особиста інформація, та найбільш конфіденційна, як наприклад лікарська таємниця. Технології штучного інтелекту можуть використовуватися для збору і аналізу величезної кількості особистої інформації для різних цілей [222, с. 394].

Серед викликів та загроз захисту персональних даних у сфері охорони здоров'я із застосування технологій штучного інтелекту М.В. Бєлова та Д.М. Бєлов виділяють такі [223, с. 20]:

«1) ризик несанкціонованого доступу до персональних даних у сфері охорони здоров'я. Використання штучного інтелекту може призвести до збільшення обсягу персональних даних, що обробляються, та зберігаються. Це створює загрозу можливого несанкціонованого доступу до цих даних, що може призвести до порушення приватності та потенційних зловживань;

2) ризик алгоритмічної дискримінації. Штучний інтелект використовує алгоритми для прийняття рішень на основі обробки персональних даних. Однак,

такі алгоритми можуть бути підвержені дискримінації, якщо вони ґрунтуються на неправильних або необ'єктивних даних. Це може призвести до нерівності, порушення прав та дискримінації осіб на основі їх особистих характеристик. Ризик алгоритмічної дискримінації виникає, коли системи штучного інтелекту, засновані на алгоритмах та машинному навчанні, приймають рішення, які можуть призводити до некоректного, несправедливого або дискримінаційного оброблення індивідів або груп людей на підставі їхніх персональних характеристик. Одним з основних джерел ризику алгоритмічної дискримінації є якість та характеристики вихідних даних, на основі яких системи штучного інтелекту навчаються. Якщо вихідні дані містять приховані відображення дискримінації або нерепрезентативність, то алгоритми можуть усвідомити ці недоліки і відображати їх у своїх рішеннях. Крім того, алгоритми можуть надмірно підкреслювати існуючі соціокультурні нерівності, оскільки вони використовуються для прогнозування майбутніх подій на підставі історичних даних. Це може спричиняти зацикленість на стереотипах, виключенні певних груп або надмірне обтяження незахищених груп;

3) недостатня прозорість і пояснюваність алгоритмів. Штучний інтелект може використовувати складні алгоритми, які важко пояснити та зрозуміти. Це створює проблему в обсязі розуміння, як самі алгоритми приймають рішення на основі персональних даних, що може ускладнити контроль та нагляд за їхньою діяльністю».

Таким чином, внаслідок розширення сфери застосування технологій штучного інтелекту виникає низка загроз та викликів захисту персональних даних у сфері охорони здоров'я. Сьогодні складно уявити яким чином будуть врегульовані відносини щодо захисту персональних даних у сфері охорони здоров'я із застосування технологій штучного інтелекту. Це потребує розробки та прийняття відповідних законодавчих актів, які мають бути пов'язані із використанням штучного інтелекту у сферах захисту персональних даних та охорони здоров'я [224, с. 319]. В Україні станом на сьогодні прийнята лише Концепція розвитку штучного інтелекту в Україні [225], а в ЄС діє Регламент про

штучний інтелект [226]. У зв'язку з цим контроль за додержанням законодавства про захист персональних даних, особливо «чутливих даних», до яких відносяться і дані про здоров'я, Уповноваженого Верховної Ради України з прав людини потребує нових підходів щодо захисту персональних даних у сфері охорони здоров'я, які мають бути спрямовані на швидке та ефективне реагування на несанкціонований доступ до медичних даних пацієнтів [143, с. 214].

Щодо контролю за додержанням законодавства про захист персональних даних, до яких відносяться і дані про здоров'я, Уповноваженим Верховної Ради України з прав людини, то слід зазначити, що діяльність цього органу не є ефективною (представники Уповноваженого Верховної Ради України з прав людини фіксують факт вчинення адміністративного правопорушення у протоколі, проте самостійно до адміністративної відповідальності притягати не можуть; приписи Уповноваженого Верховної Ради України з прав людини мають рекомендаційний характер, і для притягнення до адміністративної відповідальності за невиконання законних вимог Уповноваженого Верховної Ради України з прав людини його представники повинні складати окремий протокол про адміністративне правопорушення, який передають на розгляд суду) та не відповідає принципу незалежності від інших органів публічної влади. Згідно європейських стандартів контроль за додержанням законодавства про захист персональних даних має здійснювати незалежний від інших органів публічної влади контролюючий орган [53, 63, 64].

Наразі у ВР України перебуває на розгляді проєкт Закону України від 18 жовтня 2021 року № 6177 «Про Національну комісію з питань захисту персональних даних та доступу до публічної інформації» [227], який передбачає створення такого органу як Національна комісія з питань захисту персональних даних та доступу до публічної інформації – центрального органу виконавчої влади зі спеціальним статусом, що забезпечує формування та реалізує державну політику в сфері захисту персональних даних та доступу до публічної інформації, а також здійснює державний контроль за дотриманням законодавства про захист персональних даних та/або доступ до публічної інформації. Необхідно відмітити,

що цей орган має поєднувати одночасно повноваження із захисту персональних даних та контролю у сфері доступу до публічної інформації у одному органі, що, на нашу думку, не сприятиме ефективності його діяльності, оскільки ці сфери мають відмінності і це може призвести до конфліктності. Це саме стосується і повноважень щодо формування та реалізації державної політики в сфері захисту персональних даних та доступу до публічної інформації. При цьому головним органом у системі центральних органів виконавчої влади, що забезпечує формування та реалізацію державної політики у інформаційній сфері, є Міністерство культури та інформаційної політики України [228]. На нашу думку контроль за додержанням законодавства про захист персональних даних повинен здійснювати незалежний від інших органів публічної влади орган і виключно у сфері захисту персональних даних. Це буде відповідати європейським стандартам та сприятиме ефективності контролю за додержанням законодавства про захист персональних даних.

Суттєвого вдосконалення потребує інститут юридичної відповідальності за порушення законодавства про захист персональних даних, у тому числі у сфері охорони здоров'я.

Правопорушення у сфері захисту персональних даних характеризується високим рівнем латентності, що дає змогу говорити про значні масштаби їх соціально-економічної небезпеки. Велика кількість правопорушень та брак стрімкого прогресу в боротьбі з деліктністю у сфері захисту персональних даних зумовлюються багатьма чинниками, як-то: постійні зміни правил автоматизованої обробки персональних даних, слабка резистентність програмно-технічного забезпечення до несанкціонованих втручань, низький рівень правосвідомості суб'єктів інформаційних відносин, недостатня щільність внутрішнього та зовнішнього контролю за додержанням законності тощо. Однак головна причина невтішного стану справ полягає в недоліках організаційно-правового забезпечення. Фактично на всіх його ділянках мають місце системні збої, зумовлені вадами нормативно-правової регламентації, відсутністю системного підходу в адмініструванні, численними організаційними, методичними й

кадровими проблемами, а також багатьма іншими чинниками, які вкрай негативно відображаються на загальному стані захисту персональних даних [12, с. 182-183].

Упорядкуванню та законодавчому вирішенню підлягають наступні питання: 1) деліктизація порушень прав суб'єктів персональних даних, а також порушень правил обробки таких даних шляхом встановлення за них адміністративної відповідальності; 2) кардинальне оновлення змісту ст. 212^3 КУпАП, яка, з одного боку, має охоплювати всі випадки порушення права на інформацію (а не лише порушення вимог окремих законів), а з іншого – передбачати відповідальність усіх осіб, які такі порушення вчиняють; 3) перегляд санкцій, передбачених за делікти у сфері захисту персональних даних на предмет взаємної узгодженості, системного зв'язку, дотримання правил юридичної техніки, адекватності (співмірності) суспільній небезпеці правопорушень, відповідності соціально-економічним умовам сьогодення; 4) удосконалення процесуальних засад відповідальності за правопорушення у сфері обробки та захисту персональних даних; 5) розширити перелік способів захисту порушених прав у сфері інформації, визначений ст. 200 Цивільного кодексу України; оптимізувати зміст ст. 301 Цивільного кодексу України «Право на особисте життя та його таємницю», звільнивши її від декларативних положень, закріпивши в ній заборону на обробку конфіденційної інформації без згоди суб'єкта, переглянувши її на предмет відповідності вимогам юридичної техніки. Врегулювати на рівні Цивільного кодексу України відносини з приводу: поширення конфіденційної інформації сторонами цивільно-правових зобов'язань, обробки персональних даних, які оприлюднив їх суб'єкт (за його згодою) та перебувають в загальному доступі, використання персональних даних у наукових дослідженнях та під час створення об'єктів інтелектуальної власності, спадкування права на захист таємниці приватного життя, знищення матеріальних носіїв, які використовуються для незаконного зберігання персональних даних [12, с. 159-182].

Враховуючи євроінтеграційні прагнення України важливим є приведення у відповідність законодавства України до законодавства ЄС про захист персональних даних у сфері охорони здоров'я [229, с. 119].

Згідно Угоди про асоціацію між Україною, з однієї сторони, та ЄС, Європейським співтовариством з атомної енергії і їхніми державами-членами, з іншої сторони, Україна взяла на себе зобов'язання щодо забезпечення належного рівня захисту персональних даних відповідно до найвищих європейських та міжнародних стандартів, зокрема відповідних документів РЄ [230].

Основним документом у сфері захисту персональних даних у країнах ЄС є Загальний регламент захисту персональних даних від 27 квітня 2016 року № 2016/679 [53]. Цим регламентом стосовно захисту персональних даних у сфері охорони здоров'я введено поняття спеціальної категорії персональних даних, а саме «чутливих даних» (зумовлено тим, що під час обробки можуть створюватися значні ризики для основних прав і свобод і це потребує особливого захисту), до яких належать дані про стан здоров'я. У Загальному регламенті захисту персональних даних розкрито сутність персональних даних про стан здоров'я (дані, що пов'язані зі станом здоров'я суб'єкта даних та розкривають інформацію про минулий, поточний або майбутній стан фізичного або психічного здоров'я суб'єкта даних), наведено розуміння категорії «суспільне здоров'я» і її складників, встановлено нові стандарти захисту персональних даних про стан здоров'я, посилено обов'язки контролерів (суб'єкт, відповідальний за обробку персональних даних у сфері охорони здоров'я) та процесорів (суб'єкт, який допомагає у обробці персональних даних у сфері охорони здоров'я) щодо обробки персональних даних у сфері охорони здоров'я, встановлено умови надання згоди на обробку персональних даних, охарактеризовано особливості обробки спеціальних категорій персональних даних, до яких належать дані про стан здоров'я, визначено умови доступу до персональних даних, передбачено питання, пов'язані з безпекою персональних даних, а також відповідальність за порушення законодавства про захист персональних даних тощо. Таким чином, у ЄС на законодавчому рівні встановлено особливі вимоги щодо захисту персональних даних у сфері охорони здоров'я.

Відповідно до п. 11 Плану з виконання Угоди про асоціацію між Україною, з однієї сторони, та ЄС, Європейським співтовариством з атомної енергії і їхніми

державами-членами, з іншої сторони, затвердженого постановою КМ України від 25 жовтня 2017 року № 1106 [231], Україна має вдосконалити законодавство про захист персональних даних з метою приведення його у відповідність з Загальним регламентом захисту персональних даних ЄС від 27 квітня 2016 року № 2016/679, а саме: розробити та подати на розгляд КМ України законопроєкт щодо внесення відповідних змін до Закону України «Про захист персональних даних»; опрацювати законопроєкт з експертами ЄС; забезпечити супроводження розгляду ВР України законопроєкту; ресурсно забезпечити впровадження Закону України; посилити інституційну спроможність Уповноваженого Верховної Ради України з прав людини як незалежного інституту з нагляду за дотриманням законодавства про захист персональних даних. Однак відповідних змін у законодавстві про захист персональних даних, в тому числі у сфері охорони здоров'я, не відбулося [229, с. 120-121].

Визначивши в національному законодавстві стратегічні цілі інтеграції в ЄС і членство в цій організації, Україна повинна відповідати вимогам європейської системи цінностей та стандартів захисту прав і свобод людини і громадянина. У зв'язку з цим та враховуючи важливість захисту персональних даних у сфері охорони здоров'я необхідно вдосконалити законодавство про захист персональних даних, в тому числі у сфері охорони здоров'я, з метою приведення його у відповідність з Загальним регламентом захисту персональних даних ЄС від 27 квітня 2016 року № 2016/679 [229, с. 121].

Наразі у ВР України перебуває на розгляді проєкт Закону України від 25 жовтня 2022 року № 8153 «Про захист персональних даних» [232], необхідність прийняття якого обумовлена тим, що стан законодавства не в повній мірі забезпечує захист персональних даних в Україні в світлі розвитку міжнародних та європейських стандартів у цій сфері.

Завданням проєкту Закону є приведення нормативного регулювання України в сфері захисту персональних даних у відповідність до нових міжнародних стандартів в цій сфері, які передбачені Конвенцією 108+ та Загальним регламентом про захист персональних даних, а також врегулювати правові відносини,

пов’язані з обробкою персональних даних, які не врегульовані чинним законом. Крім того, законопроєкт має на меті підвищити рівень захисту конституційного права на повагу до приватного життя через посилення стандартів обробки персональних даних та надати більше прав суб’єкту персональних даних для забезпечення можливості здійснення повноцінного контролю суб’єктом за обробкою його персональних даних [233].

Законопроєкт передбачає: приведення термінології сфери захисту персональних даних у відповідність до нових міжнародних стандартів; деталізацію та більш зрозуміле формулювання принципів обробки персональних даних; більш чітке формулювання підстав обробки персональних даних; деталізовані та прозорі вимоги до згоди на обробку персональних даних, які дозволять уникнути зловживань та маніпуляцій; розширення прав суб’єктів персональних даних та механізм їх реалізації; чітке визначення обов’язків контролера і оператора персональних даних; порядок повідомлення про витік персональних даних; інститут відповідальної особи з питань захисту персональних даних, її функціональні обов’язки, вимоги та порядок призначення; врегулювання передачі персональних даних на територію іноземних держав та міжнародних організацій; фінансову відповідальність, адміністративно-господарські санкції, що застосовуються до контролера та/або оператора за порушення права на захист персональних даних, які дозволять забезпечити дієвість закону та виконання його вимог [233].

Законопроєктом визначено особливі вимоги до: обробки персональних даних (чутливі персональні дані), обробки персональних даних, пов’язаних з притягненням до кримінальної відповідальності, обробки біометричних даних суб’єктами владних повноважень та обробки персональних даних з метою прямого маркетингу, передвиборчої агітації та політичної реклами. Суттєво розширені права суб’єкта персональних даних у повній відповідності до вимог Загального регламенту про захист персональних даних та Конвенції 108, а саме визначено механізми для захисту: права на інформацію; права суб’єкта даних на доступ до персональних даних; права суб’єкта персональних даних на

виправлення персональних даних; права суб'єкта персональних даних на забуття; права на заперечення проти обробки персональних даних; права на мобільність персональних даних; права на обмеження обробки персональних даних; права на захист від автоматизованого прийняття рішення; права суб'єкта даних на захист своїх прав та відшкодування шкоди. Також встановлено порядок розгляду вимог суб'єкта персональних даних контролерами та операторами [233].

Відповідно до висновків Головного науково-експертного управління Апарату ВР України, Комітету ВР України з питань інтеграції України до ЄС та Комітету ВР України з питань прав людини, деокупації та реінтеграції тимчасово окупованих територій України, національних меншин і міжнаціональних відносин, проєкту «Підтримка впровадження європейських стандартів прав людини в Україні» деякі положення проєкту Закону України від 25 жовтня 2022 року № 8153 «Про захист персональних даних» рекомендовано переглянути, уточнити або внести до них правки, щоб гарантувати їх відповідність міжнародним та європейським стандартам [233, 234].

На нашу думку, про що вже було зазначено у цьому підрозділі дисертаційного дослідження, проєкт Закону України від 25 жовтня 2022 року № 8153 «Про захист персональних даних» або інший новий Закон України «Про захист персональних даних» повинен містити окремий розділ «Захист персональних даних у сфері охорони здоров'я», у якому необхідно передбачити чітке розуміння поняття «медичні дані», співвідношення законодавства про захист персональних даних та охорону здоров'я, цілі обробки медичних даних, підстави та вимоги до обробки медичних даних, порядок та умови надання згоди пацієнта на обробку його медичних даних, особливості функціонування електронної системи охорони здоров'я, права пацієнта як суб'єкта медичних даних, обов'язки суб'єктів господарювання у сфері медичного обслуговування як володільців (контролерів) та розпорядників (операторів) медичних даних, вимоги до порядку обробки медичних даних як внутрішнього документа суб'єктів господарювання у сфері медичного обслуговування, вимоги до суб'єктів інформаційного забезпечення системи охорони здоров'я, порядок та умови

доступу до медичних даних третіх осіб, особливості передачі медичних даних на територію іноземної держави або міжнародній організації, правила конфіденційності щодо медичних даних, особливості контролю за дотриманням законності при обробці медичної інформації, особливості зберігання медичних даних, гарантії безпеки медичних даних.

Підсумовуючи викладене, напрямами вдосконалення правового регулювання захисту персональних даних у сфері охорони здоров'я в Україні, є: 1) прийняття нового Закону України «Про захист персональних даних», який буде спрямований на регулювання суспільних відносин, пов'язаних із захистом персональних даних загалом, так і захисту персональних даних в конкретних сферах суспільних відносин, у тому числі у сфері охорони здоров'я; 2) упорядкування законодавства про охорону здоров'я із законодавством про захист персональних даних; 3) створення нового спеціального незалежного від інших органів публічної влади контролюючого органу за додержанням законодавства про захист персональних даних; 4) реформування інституту юридичної відповідальності за порушення законодавства про захист персональних даних; 5) належна регламентація відносин, пов'язаних із безпекою та конфіденційністю персональних даних у сфері охорони здоров'я; 6) приведення законодавства про захист персональних даних та охорону здоров'я у відповідність до міжнародних та європейських стандартів.

Запропоновані напрями мають сприяти створенню необхідних умов для ефективного функціонування відносин, пов'язаних із захистом персональних даних у сфері охорони здоров'я.

Висновки до розділу 3

1. У міжнародному та європейському правопорядку право на захист персональних даних є основоположним правом на рівні з правом на приватне

життя. Міжнародні стандарти правового регулювання захисту персональних даних у сфері охорони здоров'я визначені у міжнародних документах Організації Об'єднаних Націй, Всесвітньої медичної асоціації, Організації економічного співробітництва та розвитку та РЄ. Міжнародні стандарти правового регулювання захисту персональних даних у сфері охорони здоров'я доцільно класифікувати на міжнародні акти загального характеру, які регулюють захист персональних даних у сфері охорони здоров'я опосередковано, та міжнародні документи, які безпосередньо стосуються захисту персональних даних у сфері охорони здоров'я. Міжнародні стандарти сприяють формуванню ефективного національного законодавства про захист персональних даних та охорону здоров'я.

2. Європейські стандарти правового регулювання захисту персональних даних у сфері охорони здоров'я характеризуються значним масивом нормативних актів РЄ та ЄС, а також судовою практикою ЄСПЛ. Право РЄ щодо захисту персональних даних у сфері охорони здоров'я містить норми обов'язкового та рекомендаційного характеру. Право ЄС щодо захисту персональних даних у сфері охорони здоров'я ґрунтується на нормах первинного та вторинного законодавства. Вагоме значення в утвердженні захисту персональних даних у сфері охорони здоров'я має судова практика ЄСПЛ, рішення якого є обов'язковими для виконання, в тому числі щодо вжиття заходів для удосконалення законодавства. Європейські стандарти правового регулювання захисту персональних даних у сфері охорони здоров'я мають фундаментальне значення для України щодо виконання зобов'язання про приведення національного законодавства у відповідність до європейського законодавства. Тому забезпечення належного рівня захисту персональних даних у сфері охорони здоров'я відповідно до європейських та міжнародних стандартів є одним пріоритетних завдань України.

3. Сучасний стан законодавства характеризуються неузгодженістю та протиріччям і не в повній мірі забезпечує захист персональних даних у сфері охорони здоров'я в Україні. Напрямами вдосконалення правового регулювання захисту персональних даних у сфері охорони здоров'я в Україні, є: 1) прийняття

нового Закону України «Про захист персональних даних», який буде спрямований на регулювання суспільних відносин, пов'язаних із захистом персональних даних загалом, так і захисту персональних даних в конкретних сферах суспільних відносин, у тому числі у сфері охорони здоров'я; 2) упорядкування законодавства про охорону здоров'я із законодавством про захист персональних даних; 3) створення нового спеціального незалежного від інших органів публічної влади контролюючого органу за додержанням законодавства про захист персональних даних; 4) реформування інституту юридичної відповідальності за порушення законодавства про захист персональних даних; 5) належна регламентація відносин, пов'язаних із безпекою та конфіденційністю персональних даних у сфері охорони здоров'я; 6) приведення законодавства про захист персональних даних та охорону здоров'я у відповідність до міжнародних та європейських стандартів.

4. Новий Закон України «Про захист персональних даних» повинен містити окремий розділ «Захист персональних даних у сфері охорони здоров'я», у якому необхідно передбачити чітке розуміння поняття «медичні дані», співвідношення законодавства про захист персональних даних та охорону здоров'я, цілі обробки медичних даних, підстави та вимоги до обробки медичних даних, порядок та умови надання згоди пацієнта на обробку його медичних даних, особливості функціонування електронної системи охорони здоров'я, права пацієнта як суб'єкта медичних даних, обов'язки суб'єктів господарювання у сфері медичного обслуговування як володільців (контролерів) та розпорядників (операторів) медичних даних, вимоги до порядку обробки медичних даних як внутрішнього документа суб'єктів господарювання у сфері медичного обслуговування, вимоги до суб'єктів інформаційного забезпечення системи охорони здоров'я, порядок та умови доступу до медичних даних третіх осіб, особливості передачі медичних даних на територію іноземної держави або міжнародній організації, правила конфіденційності щодо медичних даних, особливості контролю за дотриманням законності при обробці медичної інформації, особливості зберігання медичних даних, гарантії безпеки медичних даних.

ВИСНОВКИ

У дисертації здійснено теоретичне узагальнення й вирішення наукового завдання, що полягає у визначенні сутності та особливостей правового регулювання захисту персональних даних у сфері охорони здоров'я. Сформульовано низку висновків та пропозицій, спрямованих на вирішення цього завдання. Основні з них такі:

1. Поняття «персональні дані» та сфера охорони здоров'я підпадають під правовий вплив різних галузей права. Персональні дані у сфері охорони здоров'я – це конфіденційна інформація про медичне обслуговування особи, яка дозволяє її ідентифікувати та дізнатися відомості щодо її стану здоров'я. Істотними ознаками персональних даних у сфері охорони здоров'я є такі: 1) конфіденційна інформація; 2) стосується фізичної особи; 3) містить інформацію про медичне обслуговування особи та відомості про її стан здоров'я; 4) фізична особа є ідентифікованою.

До конфіденційної інформації про медичне обслуговування особи відноситься: інформація про фізичну особу, зібрана під час реєстрації на надання медичних послуг або надання медичних послуг; номер, символьний знак або опис, що приписують фізичній особі для того, щоб ідентифікувати фізичну особу для цілей охорони здоров'я; інформація, отримана внаслідок дослідження або огляду частини тіла чи речовини, що міститься в тілі, у тому числі з генетичних даних або біологічних проб; будь-яка медична інформація (про медичні обстеження, про захворювання, про лікувальні заходи, про прогноз розвитку захворювання, про недієздатність, про ризик захворювання, про історію хвороби, про фізіологічний чи біомедичний стан здоров'я особи, про діагнози та будь-які документи, що стосуються здоров'я та обмеження повсякденного функціонування/життєдіяльності людини). Така інформація викладається у формалізованому вигляді, що забезпечує можливість обробки персональних даних у сфері охорони здоров'я в інформаційних системах.

2. Інститут захисту персональних даних у сфері охорони здоров'я доцільно розглядати як: право на невтручання в особисте життя, а саме право на конфіденційну інформацію про медичне обслуговування особи та відомості щодо її стану здоров'я; комплексний правовий інститут – сукупність правових норм різної галузевої належності, які регулюють суспільні відносини, пов'язані із захистом і обробкою персональних даних у сфері охорони здоров'я; напрям діяльності – комплекс заходів, спрямованих на забезпечення конфіденційності персональних даних у сфері охорони здоров'я. Захист персональних даних у сфері охорони здоров'я – це сукупність заходів, спрямованих на гарантування безпеки конфіденційної інформації про медичне обслуговування особи та відомостей щодо її стану здоров'я.

3. Періодизацію становлення інституту захисту персональних даних у сфері охорони здоров'я виокремлено за такими етапами розвитку: 1) 1991-2009 рр. – відсутність належного правового регулювання захисту персональних даних у сфері охорони здоров'я; 2) 2010-2014 рр. – запровадження інституту захисту персональних даних у сфері охорони здоров'я; 3) 2015 – дотепер – удосконалення інституту захисту персональних даних у сфері охорони здоров'я.

Наявність значної кількості різних нормативно-правових актів щодо захисту персональних даних у сфері охорони здоров'я дає підстави для класифікації їх за предметом правового регулювання на загальні та спеціальні акти. До загальних нормативних актів щодо захисту персональних даних у сфері охорони здоров'я відносяться нормативні акти, які регулюють як питання захисту персональних даних, так і інші суспільні відносини. До спеціальних нормативних актів щодо захисту персональних даних у сфері охорони здоров'я відносяться нормативні акти, які регулюють захист персональних даних у сфері охорони здоров'я.

4. Обробка персональних даних у сфері охорони здоров'я здійснюється за умови надання пацієнтом однозначної згоди на обробку таких даних або на підставі закону. Обробка персональних даних у сфері охорони здоров'я без згоди пацієнта здійснюється: 1) коли медичні відомості необхідні в цілях охорони здоров'я (встановлення медичного діагнозу, забезпечення піклування чи

лікування або надання медичних послуг, моніторинг відповідності встановленим умовам надання таких послуг функціонування електронної системи охорони здоров'я; контроль якості надання медичних послуг; обмін інформацією про фінансування медичних послуг та послуг у сфері охорони здоров'я); 2) для захисту життєво важливих інтересів суб'єкта персональних даних. Обробляти персональні дані без згоди пацієнта можна до часу, коли отримання згоди стане можливим. Обмеження щодо обробки персональних даних у сфері охорони здоров'я може здійснюватися у випадках, передбачених законом, наскільки це необхідно у демократичному суспільстві в інтересах національної безпеки, економічного добробуту або захисту прав і свобод суб'єктів персональних даних чи інших осіб.

5. Суб'єкти забезпечення захисту персональних даних у сфері охорони здоров'я – це фізичні та юридичні особи, які зобов'язані забезпечити захист персональних даних у сфері охорони здоров'я від неправомірного збирання, зберігання, використання, знищення, поширення та доступу до медичних даних. Суб'єктами забезпечення захисту персональних даних у сфері охорони здоров'я є: 1) володільці персональних даних у сфері охорони здоров'я – органи публічної влади (МОЗ України та НСЗ України) та суб'єкти господарювання приватної форми власності, діяльність яких пов'язана з медичним обслуговуванням; 2) розпорядники персональних даних у сфері охорони здоров'я – органи публічної влади та їх посадові особи, співробітники закладів охорони здоров'я публічної форми власності, суб'єкти господарювання приватної форми власності, діяльність яких пов'язана з медичним обслуговуванням, а також медичні працівники, співробітники медичного закладу, працівники, відповідальні за захист персональних даних у лікаря-підприємця; 3) треті особи персональних даних у сфері охорони здоров'я – органи публічної влади та суб'єкти господарювання будь-якої форми власності, діяльність яких пов'язана з медичним обслуговуванням; 4) Уповноважений Верховної Ради України з прав людини.

6. Правові засоби захисту персональних даних у сфері охорони здоров'я – це заходи компетентних суб'єктів, які спрямовані на запобігання, припинення

правопорушення у сфері захисту медичних даних, відновлення порушеного права чи компенсацію заподіяної правопорушенням шкоди. Такими заходами є превентивні, припиняючі та відновлючі. Превентивні заходи спрямовані на запобігання порушенням законодавства про захист персональних даних у сфері охорони здоров'я і вживаються володільцями, розпорядниками, третіми особи на всіх етапах їх обробки, у тому числі за допомогою організаційних та технічних заходів, а також Уповноваженим Верховної Ради України з прав людини на підставі звернень фізичних і юридичних осіб або за власною ініціативою шляхом проведення планових, позапланових, виїзних та безвиїзних перевірок. Припиняючі заходи спрямовані на усунення та припинення порушення законодавства про захист персональних даних і застосовуються володільцями, розпорядниками, третіми особи (безпосереднє усунення володільцем або розпорядником персональних даних порушень законодавства про захист персональних даних; отримання Уповноваженим Верховної Ради України з прав людини скарг фізичних і юридичних осіб з питань захисту персональних даних та приймати рішення за результатами їх розгляд тощо) та Уповноважений Верховної Ради України з прав людини (складає протокол про адміністративне правопорушення за порушення законодавства у сфері захисту персональних даних та невиконання законних вимог Уповноваженого Верховної Ради України з прав людини; у разі виявлення під час перевірки суб'єкта перевірки ознак кримінального правопорушення направляє необхідні матеріали до правоохоронних органів). Відновлювальні заходи спрямовані на відновлення порушеного права, усунення перешкод в його реалізації та загрози порушення суб'єктивних прав протиправними діями. Ці заходи уповноважені застосовувати володільці, розпорядники, треті особи, Уповноважений Верховної Ради України з прав людини та суд на підставі звернення особи про порушення її права на захист персональних даних у сфері охорони здоров'я.

7. У міжнародному та європейському правопорядку право на захист персональних даних є основоположним правом на рівні з правом на приватне життя. Міжнародні стандарти правового регулювання захисту персональних

даних у сфері охорони здоров'я доцільно класифікувати на міжнародні акти загального характеру, які регулюють захист персональних даних у сфері охорони здоров'я опосередковано, та міжнародні документи, які безпосередньо стосуються захисту персональних даних у сфері охорони здоров'я. Міжнародні стандарти сприяють формуванню ефективного національного законодавства про захист персональних даних та охорону здоров'я. Європейські стандарти правового регулювання захисту персональних даних у сфері охорони здоров'я характеризуються значним масивом нормативних актів РЄ та ЄС, а також судовою практикою ЄСПЛ. Європейські стандарти правового регулювання захисту персональних даних у сфері охорони здоров'я мають фундаментальне значення для України щодо виконання зобов'язання про приведення національного законодавства у відповідність до європейського законодавства. Тому забезпечення належного рівня захисту персональних даних у сфері охорони здоров'я відповідно до міжнародних та європейських стандартів є одним пріоритетних завдань України.

8. Сучасний стан законодавства характеризуються неузгодженістю та протиріччям і не в повній мірі забезпечує захист персональних даних у сфері охорони здоров'я в Україні. Напрямами вдосконалення правового регулювання захисту персональних даних у сфері охорони здоров'я в Україні, є: 1) прийняття нового Закону України «Про захист персональних даних», який буде спрямований на регулювання суспільних відносин, пов'язаних із захистом персональних даних загалом, так і захисту персональних даних в конкретних сферах суспільних відносин, у тому числі у сфері охорони здоров'я; 2) упорядкування законодавства про охорону здоров'я із законодавством про захист персональних даних; 3) створення нового спеціального незалежного від інших органів публічної влади контролюючого органу за додержанням законодавства про захист персональних даних; 4) реформування інституту юридичної відповідальності за порушення законодавства про захист персональних даних; 5) належна регламентація відносин, пов'язаних із безпекою та конфіденційністю персональних даних у сфері охорони здоров'я; 6) приведення законодавства про захист персональних

даних та охорону здоров’я у відповідність до міжнародних та європейських стандартів.

Новий Закон України «Про захист персональних даних» повинен містити окремий розділ «Захист персональних даних у сфері охорони здоров’я», у якому необхідно передбачити чітке розуміння поняття «медичні дані», співвідношення законодавства про захист персональних даних та охорону здоров’я, цілі обробки медичних даних, підстави та вимоги до обробки медичних даних, порядок та умови надання згоди пацієнта на обробку його медичних даних, особливості функціонування електронної системи охорони здоров’я, права пацієнта як суб’єкта медичних даних, обов’язки суб’єктів господарювання у сфері медичного обслуговування як володільців (контролерів) та розпорядників (операторів) медичних даних, вимоги до порядку обробки медичних даних як внутрішнього документа суб’єктів господарювання у сфері медичного обслуговування, вимоги до суб’єктів інформаційного забезпечення системи охорони здоров’я, порядок та умови доступу до медичних даних третіх осіб, особливості передачі медичних даних на територію іноземної держави або міжнародній організації, правила конфіденційності щодо медичних даних, особливості контролю за дотриманням законності при обробці медичної інформації, особливості зберігання медичних даних, гарантії безпеки медичних даних.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Про Основні засади розвитку інформаційного суспільства в Україні на 2007-2015 роки: Закон України від 9 січня 2007 року № 537-V. URL: https://zakon.rada.gov.ua/laws/show/537-16#top (дата звернення 01.03.2024).

2. Тунік А.В. Правові основи захисту персональних даних: дис. … канд. юрид. наук: 12.00.07. Київ, 2012. 229 с.

3. Різак М.В. Правове регулювання відносин обігу персональних даних: дис. … канд. юрид. наук: 12.00.07. Київ, 2012. 214 с.

4. Дяковський О.С. Правове забезпечення захисту персональних даних: автореф. дис. ... канд. юрид. наук. Дніпро, 2019. 17 с.

5. Брижко В.М. Організаційно-правові питання захисту персональних даних: автореф. дис. … канд. юрид. наук: 12.00.07. Ірпінь, 2004. 22 с.

6. Цвірюк Д.В. Адміністративно-правовий захист персональних даних в Україні: автореф. дис. ... канд. юрид. наук: 12.00.07. Харків, 2014. 20 с.

7. Мельник К.С. Правові та організаційні засади захисту персональних даних в умовах євроінтеграції України: автореф. дис. ... канд. юрид. наук: 12.00.07. Київ, 2016. 23 с.

8. Різак М.В. Адміністративно-правове забезпечення відносин обігу та обробки персональних даних в Україні: автореф. дис. … докт. юрид. наук: 12.00.07. Херсон, 2018. 39 с.

9. Щербина А.О. Адміністративно-правове регулювання використання персональних даних суб'єктами владних повноважень в Україні: автореф. дис. ... канд. юрид. наук. Запоріжжя, 2020. 22 с.

10. Самойленко Ю.С. Адміністративно-правове забезпечення захисту персональних даних в Україні: автореф. дис. … канд. юрид. наук: 12.00.07. Запоріжжя, 2023. 18 с.

11. Петрицький А.Л. Питання захисту персональних даних у сучасній правничій думці. *Право і суспільство.* 2014. № 6-1. Частина 2. С. 190–197.

12. Правовий захист персональних даних: монографія / Т.О. Гуржій, А.Л. Петрицький. Київ: Київ. нац. торг.-екон. ун-т, 2019. 216 с.

13. Брижко В.М. Організаційно-правові питання захисту персональних даних: дис. ... канд. юрид. наук: 12.00.07. Київ, 2004. 252 с.

14. Дмитренко О.А. Право фізичної особи на власні персональні дані в цивільному праві України: автореф. дис. … канд. юрид. наук: 12.00.03. Київ, 2010. 19 с.

15. Ясечко С.В. Цивільно-правова відповідальність за порушення права на інформацію: дис. ... канд. юрид. наук: 12.00.03. Харків, 2011. 224 с.

16. Романюк І.І. Охорона права на персональні дані в Україні (цивільно-правовий аспект): автореф. дис. ... канд. юрид. наук: 12.00.03. Київ, 2015. 21 с.

17. Бєлова Ю.Д. Цивільні правовідносини щодо персональних даних: дис. ... докт. філософії за спеціальністю 081 «Право». Хмельницький, 2021. 248 с.

18. Чернобай А.М. Правові засоби захисту персональних даних працівника: автореф. дис. … канд. юрид. наук: 12.00.05. Одеса, 2006. 21 с.

19. Гета Д.С. Захист персональних даних працівників у трудових відносинах: дис. … канд. юрид. наук: 12.00.05. Кривий Ріг, 2017. 202 с.

20. Авраменко А.В. Правове регулювання відносин щодо обігу та захисту персональних даних працівника в трудовому праві України. дис 12.00.05 Київ, 2019. 215 с.

21. Дем’яненко Ю.І. Кримінальна відповідальність за порушення недоторканості приватного життя: автореф. дис... канд. юрид. наук: 12.00.08. Харків, 2008. 20 с.

22. Король І.Б. Охорона недоторканості приватного життя: кримінально-правові та кримінологічні аспекти: автореф. дис... канд. юрид. наук: 12.00.08. Львів, 2015. 21 с.

23. Сосніна І.Б. Кримінальна відповідальність за порушення недоторканості приватного життя (ст. 182 КК України): автореф. дис... канд. юрид. наук: 12.00.08. Львів, 2017. 20 с.

24. Матвійчук В.К., Матвійчук В.В. Кримінально-правова характеристика діяння порушення недоторканності приватного життя (ст. 182 КК України): монографія / за заг. ред. В.К. Матвійчука. Київ: Видавництво Ліра-К, 2022. 232 с.

25. Пазюк А.В. Міжнародно-правовий захист права людини на приватність персоніфікованої інформації: дис. … канд. юрид. наук: 12.00.11. Київ, 2004. 207 с.

26. Шевчук О.О. Правове регулювання охорони персональних даних в Європейському Союзі: дис. … канд. юрид. наук: 12.00.11. Київ, 2018. 197 с.

27. Коваленко Ю.О. Захист персональних даних у практиці Європейського суду з прав людини та Суду Європейського Союзу: порівняльний аналіз: дис. ... докт. філософії за спеціальністю 293 «Міжнародне право». Київ, 2023. 261 с.

28. Токарєва К.С. Проблема захисту персональних даних у сфері охорони здоров'я в умовах інформатизації. *Юридичний науковий електронний журнал.* 2022. № 11. С. 496–499. DOI: https://doi.org/10.32782/2524-0374/2022-11/120.

29. Захист персональних даних у сфері охорони здоров'я в ЄС: законодавчий ландшафт. URL: https://www.apteka.ua/article/575210 (дата звернення 05.03.2024)

30. Демченко І.С. Е-здоров'я в Україні: правові питання та перспективи впровадження. *Медичне право.* 2017. № 2 (20). С. 23–33. DOI: https://doi.org/10.25040/medicallaw2017.02.023.

31. Ваші діагнози в їхніх руках: що електронні медсервіси роблять з даними і чим це загрожує. URL: https://cedem.org.ua/analytics/elektronni-medservisy/ (дата звернення 05.03.2024).

32. НКЦК при РНБО України виявив витік персональних медичних даних в однієї з найбільших клінік Дніпра. URL: https://www.rnbo.gov.ua/ua/Diialnist/4711.html (дата звернення 05.03.2024).

33. Захист персональних даних під час війни. Списки українців. URL: https://umdpl.info/wp-content/uploads/2023/11/ZPD-v-umovah-vijny.pdf (дата звернення 05.03.2024).

34. Миколенко О.І., Лазарєва М.І. Охорона здоров'я як об'єкт адміністративно-правового та цивільно-правового регулювання (порівняльний

аналіз). *Право та державне управління.* 2022. № 3. С. 240–245. DOI: https://doi.org/10.32840/pdu.2022.3.36.

35. Медицина в Україні. Медична біографістика. Вип. 2. Друга половина XIX століття. Літери А-К. Біобліографічний словник. К.: В-во українського фітосоціологічного центру, 2005. 616 с.

36. Основи законодавства України про охорону здоров'я: Закон України від 19 листопада 1992 року № 2801-XII. URL: https://zakon.rada.gov.ua/laws/show/2801-12#top (дата звернення 05.03.2024).

37. Шамич О.М. Поняття та структура природного права людини на охорону здоров'я. *Актуальні проблеми навчання та виховання людей із особливими вадами.* 2015. № 11. С. 75 – 92.

38. Сенюта І.Я. Медичне право: право людини на охорону здоров'я: монографія. Львів: Астролябія, 2007. 224 с.

39. Сенюта І.Я. Цивільно-правове регулювання відносин у сфері надання медичної допомоги: питання теорії і практики: монографія. Львів: Видавництво ЛОБФ «Медицина і право», 2018. 640 с.

40. Назарко Ю.В. Конституційне право на охорону здоров'я в Україні та державах Європейського Союзу: порівняльно-правове дослідження. дис. ... докт. філософії за спеціальністю 081 «Право». Київ, 2019. 249 с.

41. Майданик Р.А. Законодавство України у сфері охорони здоров'я: система і систематизація. *Медичне право*. 2013. № 2 (12). С. 63–74.

42. Клименко О.В. Законодавство у сфері охорони здоров'я: перспективи розвитку. *Економіка та держава*. 2012. № 5. С. 128–130.

43. Гладун З.С. Проблеми формування галузі медичного права в Україні. *Вісник Львівського національного університету*. 2005. № 3. С. 63–79.

44. Гладун З.С. Державна політика охорони здоров'я в Україні (адміністративно-правові проблеми формування і реалізації): Монографія Тернопіль, «Економічна думка», 2005. 460 с.

45. Санжаровська Л.І. Поняття та сутність персональних даних у сфері охорони здоров'я. *Наука і техніка сьогодні.* 2024. № 3 (31). С. 182-192. DOI: https://doi.org/10.52058/2786-6025-2024-3(31)-182-192.

46. Про захист персональних даних: Закон України від 1 червня 2010 року № 2297-VI. URL: https://zakon.rada.gov.ua/laws/show/2297-17#top (дата звернення 07.03.2024).

47. Брель О. Персональні дані як об'єкт інформаційних правовідносин за участю суб'єктів господарювання. *Право України*. 2011. № 4. С.220-224.

48. Дяковський О.С. Визначення персональних даних як правової категорії: сучасні проблеми та шляхи вирішення. *Інформація і право*. 2017. № 3 (22). С. 51−56.

49. Виноградова Г.В. Правове регулювання інформаційних відносин в Україні. К., 2006. 176 с.

50. Саєнко М.І. Сучасне правове регулювання інформаційних відносин у сфері захисту персональних даних в Україні. *Право і суспільство*. 2015. № 3. С. 102−107.

51. Щербина А.О. Адміністративно-правове регулювання використання персональних даних суб'єктами владних повноважень в Україні: дис. ... канд. юрид. наук. Запоріжжя, 2020. 232 с.

52. Різак М.В. Персональні дані як об'єкт неправомірного посягання. *Право і безпека*. 2015. № 3 (58). С. 57−62.

53. 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). URL: https://zakon.rada.gov.ua/laws/show/984_008-16#Text (дата звернення 07.03.2024).

54. Роз'яснення основних положень Порядку повідомлення Уповноваженого щодо визначення обробки персональних даних, яка становить особливий ризик для прав і свобод суб'єктів персональних даних від 8 січня 2014 року. URL: https://zakon.rada.gov.ua/laws/show/n0003715-14#Text (дата звернення 07.03.2024).

55. Конституція України від 28 червня 1996 року. URL: https://zakon.rada.gov.ua/laws/show/254к/96-вр#Text (дата звернення 07.03.2024).

56. Про інформацію: Закон України від 2 жовтня 1992 року № 2657-XII. URL: https://zakon.rada.gov.ua/laws/show/2657-12#Text (дата звернення 07.03.2024).

57. Рішення Конституційного Суду України у справі щодо офіційного тлумачення статей 3, 23, 31, 47, 48 Закону України «Про інформацію» та статті 12 Закону України «Про прокуратуру» (справа К.Г. Устименка) від 30 жовтня 1997 року № 5-зп. URL: https://zakon.rada.gov.ua/laws/show/v005p710-97#Text (дата звернення 07.03.2024).

58. Рішення Конституційного Суду України у справі у справі за конституційним поданням Жашківської районної ради Черкаської області щодо офіційного тлумачення положень частин 1, 2 ст. 32, частин 2, 3 ст. 34 Конституції України від 20 січня 2012 року № 1-9/2012. URL: https://zakon.rada.gov.ua/laws/show/v002p710-12#Text (дата звернення 07.03.2024).

59. Про інформацію: Закон України в редакції від 2 жовтня 1992 року № 2657-XII. URL: https://zakononline.com.ua/documents/show/151399___591468 (дата звернення 11.03.2024).

60. Дяковський О.С. Правове забезпечення захисту персональних даних: дис. ... канд. юрид. наук. Дніпро, 2019. 208 с.

61. Пилипчук В.В., Брижко В.М. Трансформація системи персональних даних та приватності в контексті євроінтеграції України. *Вісник Національної академії правових наук України.* 2017. № 3 (90). С. 36-50.

62. Про ратифікацію Конвенції про захист осіб у зв’язку з автоматизованою обробкою персональних даних та Додаткового протоколу до Конвенції про захист осіб у зв’язку з автоматизованою обробкою персональних даних стосовно органів нагляду та транскордонних потоків даних: Закон України від 06 липня 2010 року № 2438-VI. URL: https://zakon.rada.gov.ua/laws/show/2438-17#Text (дата звернення 12.03.2024).

63. Конвенція про захист осіб у зв’язку з автоматизованою обробкою персональних даних від 28 січня 1981 року. URL: https://zakon.rada.gov.ua/laws/show/994_326#Text (дата звернення 12.03.2024).

64. Додатковий протокол до Конвенції про захист осіб у зв’язку з автоматизованою обробкою персональних даних стосовно органів нагляду та транскордонних потоків даних від 08 листопада 2001 року. URL: https://zakon.rada.gov.ua/laws/show/994_363#Text (дата звернення 12.03.2024).

65. Мельник К.С. Теоретичні та організаційно-правові засади захисту персональних даних в контексті євроінтеграції України: монографія / заг. ред. В.Г. Пилипчук, В.М. Брижко. К.: ТОВ «ПанТот», 2016. 126 с.

66. Про Положення про Державну службу України з питань захисту персональних даних: Указ Президента України від 06 квітня 2011 року № 390/2011. URL: https://zakon.rada.gov.ua/laws/show/390/2011#Text (дата звернення 12.03.2024).

67. Про внесення змін до деяких законодавчих актів України щодо удосконалення системи захисту персональних даних: Закон України від 03 липня 2013 року № 383-VII. URL: https://zakon.rada.gov.ua/laws/show/383-18#Text (дата звернення 12.03.2024).

68. Про оптимізацію системи центральних органів виконавчої влади: постанова Кабінету Міністрів України від 10 вересня 2014 року № 442. URL: https://zakon.rada.gov.ua/laws/show/442-2014-п#Text (дата звернення 12.03.2024).

69. Про визнання такими, що втратили чинність, деяких указів Президента України: Указ Президента України від 20 червня 2019 року № 419/2019. URL: https://zakon.rada.gov.ua/laws/show/419/2019#Text (дата звернення 12.03.2024).

70. Інформація про Департамент у сфері захисту персональних даних. URL: https://ombudsman.gov.ua/uk/informaciya-pro-pidrozdil-zpd (дата звернення 12.03.2024).

71. Про внесення змін до деяких законодавчих актів України щодо посилення відповідальності за порушення законодавства про захист персональних даних:

Закон України від 02 червня 2011 року № 3454-VI. URL: https://zakon.rada.gov.ua/laws/show/3454-17#Text (дата звернення 12.03.2024).

72. Кодекс України про адміністративні правопорушення: Закон України від 7 грудня 1984 року. URL: https://zakon.rada.gov.ua/laws/show/80731-10#Text (дата звернення 12.03.2024).

73. Кримінальний кодекс України: Закон України від 5 квітня 2001 року № 2341-III. URL: https://zakon.rada.gov.ua/laws/show/2341-14#Text (дата звернення 12.03.2024).

74. Цивільний кодекс України: Закон України від 16 січня 2003 року № 435-IV. URL: https://zakon.rada.gov.ua/laws/show/435-15#top (дата звернення 12.03.2024).

75. Цивільний процесуальний кодекс України: Закон України від 18 березня 2004 року № 1618-IV. URL: https://zakon.rada.gov.ua/laws/show/1618-15#Text (дата звернення 12.03.2024).

76. Кодекс адміністративного судочинства України: Закон України від 6 липня 2005 року № 2747-IV. URL: https://zakon.rada.gov.ua/laws/show/2747-15#Text (дата звернення 12.03.2024).

77. Кримінальний процесуальний кодекс України: Закон України від 13 квітня 2012 року № 4651-VI. URL: https://zakon.rada.gov.ua/laws/show/4651-17#Text (дата звернення 12.03.2024).

78. Про захист інформації в інформаційно-телекомунікаційних системах: Закон України від 05 липня 1994 року № 80/94-ВР. URL: https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80#Text (дата звернення 12.03.2024).

79. Про електронні комунікації: Закон України від 16 грудня 2020 року № 1089-IX. URL: https://zakon.rada.gov.ua/laws/show/1089-20#top (дата звернення 12.03.2024).

80. Про доступ до публічної інформації: Закон України від 13 січня 2011 року № 2939-VI. URL: https://zakon.rada.gov.ua/laws/show/2939-17#Text (дата звернення 12.03.2024).

81. Про електронні документи та електронний документообіг: Закон України від 22 травня 2003 року № 851-IV. URL: https://zakon.rada.gov.ua/laws/show/851-15#Text (дата звернення 12.03.2024).

82. Про електронну ідентифікацію та електронні довірчі послуги: Закон України від 05 жовтня 2017 року № 2155-VIII. URL: https://zakon.rada.gov.ua/laws/show/2155-19#Text (дата звернення 12.03.2024).

83. Про публічні електронні реєстри: Закон України від 18 листопада 2021 року № 1907-IX. URL: https://zakon.rada.gov.ua/laws/show/1907-20#top (дата звернення 12.03.2024).

84. Про національну безпеку України: Закон України від 21 червня 2018 року № 2469-VIII. URL: https://zakon.rada.gov.ua/laws/show/2469-19#top (дата звернення 12.03.2024).

85. Про основні засади забезпечення кібербезпеки України: Закон України від 05 жовтня 2017 року № 2163-VIII. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text (дата звернення 12.03.2024).

86. Про функціонування Реєстру публічних електронних реєстрів: постанова Кабінету Міністрів України від 01 вересня 2023 року № 969. URL: https://zakon.rada.gov.ua/laws/show/969-2023-%D0%BF#Text (дата звернення 12.03.2024).

87. Про затвердження документів у сфері захисту персональних даних: наказ Уповноваженого Верховної Ради України з прав людини від 8 січня 2014 року № 1/02-14. URL: https://zakon.rada.gov.ua/laws/show/v1_02715-14#Text (дата звернення 12.03.2024).

88. Про затвердження Положення про Секретаріат Уповноваженого Верховної Ради України з прав людини: наказ Уповноваженого Верховної Ради України з прав людини від 20 червня 2012 року № 4/8-12. URL: https://zakon.rada.gov.ua/laws/show/v04_8715-12#n10 (дата звернення 12.03.2024).

89. Про затвердження Положення про Секретаріат Уповноваженого Верховної Ради України з прав людини: наказ Уповноваженого Верховної Ради

України з прав людини від 14 жовтня 2022 року № 79.15/22. URL: https://zakon.rada.gov.ua/laws/show/v79_1715-22#Text (дата звернення 12.03.2024).

90. Положення про представників Уповноваженого Верховної Ради України з прав людини: наказ Уповноваженого Верховної Ради України з прав людини від 26 липня 2012 року № 7/8-12. URL: https://zakon.rada.gov.ua/laws/show/v07_8715-12#n57 (дата звернення 12.03.2024).

91. Про затвердження Положення про представників Уповноваженого Верховної Ради України з прав людини: наказ Уповноваженого Верховної Ради України з прав людини від 20 жовтня 2022 року № 84.15/22. URL: https://zakon.rada.gov.ua/laws/show/v84_1715-22#Text (дата звернення 12.03.2024).

92. Про затвердження Положення регіональних представництв Уповноваженого Верховної Ради України з прав людини: наказ Уповноваженого Верховної Ради України з прав людини від 19 лютого 2013 року № 14/02-13. URL: https://zakon.rada.gov.ua/laws/show/v4_02715-13#Text (дата звернення 12.03.2024).

93. Про затвердження Порядку оформлення матеріалів про адміністративне правопорушення: наказ Уповноваженого Верховної Ради України з прав людини від 16 лютого 2015 року № 3/02-15. URL: https://zakon.rada.gov.ua/laws/show/v3_02715-15#Text (дата звернення 12.03.2024).

94. Деякі питання електронної системи охорони здоров’я: постанова Кабінету Міністрів України від 25 квітня 2018 року № 411. URL: https://zakon.rada.gov.ua/laws/show/411-2018-%D0%BF#n11 (дата звернення 12.03.2024).

95. Деякі питання організації ведення Електронного реєстру листків непрацездатності та надання інформації з нього: постанова Кабінету Міністрів України від 17 квітня 2019 року № 328. URL: https://zakon.rada.gov.ua/laws/show/328-2019-%D0%BF#n12 (дата звернення 12.03.2024).

96. Про схвалення Концепції розвитку електронної охорони здоров’я: розпорядження Кабінету Міністрів України від 28 грудня 2020 року № 1671-р.

URL: https://zakon.rada.gov.ua/laws/show/1671-2020-%D1%80#Text (дата звернення 12.03.2024).

97. Про затвердження форм первинної облікової документації та Інструкцій щодо їх заповнення, що використовуються у закладах охорони здоров'я незалежно від форми власності та підпорядкування: наказ Міністерства охорони здоров'я від 14 лютого 2012 року № 110. URL: https://zakon.rada.gov.ua/laws/show/z0661-12#Text (дата звернення 12.03.2024).

98. Про затвердження форм первинної облікової документації, що використовується в медико-соціальних експертних комісіях: наказ Міністерства охорони здоров'я від 30 липня 2012 року № 577. URL: https://zakon.rada.gov.ua/laws/show/z1504-12#n6 (дата звернення 12.03.2024).

99. Про затвердження форм первинної облікової документації та інструкцій щодо їх заповнення, що використовуються у закладах охорони здоров'я, які надають амбулаторно-поліклінічну та стаціонарну допомогу населенню, незалежно від підпорядкування та форми власності: наказ Міністерства охорони здоров'я від 29 травня 2013 року № 435. URL: https://zakon.rada.gov.ua/laws/show/z0990-13#n34 (дата звернення 12.03.2024).

100. Про затвердження нормативних документів щодо застосування телемедицини у сфері охорони здоров'я: наказ Міністерства охорони здоров'я від 19 жовтня 2015 року № 681. URL: https://zakon.rada.gov.ua/laws/show/z1400-15#Text (дата звернення 12.03.2024).

101. 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 від 19 березня 2018 року № 503. URL: https://zakon.rada.gov.ua/laws/show/z0347-18#Text (дата звернення 12.03.2024).

102. Про затвердження Порядку надання первинної медичної допомоги: наказ Міністерства охорони здоров'я від 19 березня 2018 року № 504. URL: https://zakon.rada.gov.ua/laws/show/z0348-18#Text (дата звернення 12.03.2024).

103. Про затвердження Порядку ведення Реєстру пацієнтів в електронній системі охорони здоров'я: наказ Міністерства охорони здоров'я від 30 листопада 2020 року № 2755. URL: https://zakon.rada.gov.ua/laws/show/z0044-21#Text (дата звернення 12.03.2024).

104. Деякі питання ведення Реєстру медичних висновків в електронній системі охорони здоров'я: наказ Міністерства охорони здоров'я від 18 вересня 2020 року № 2136. URL: https://zakon.rada.gov.ua/laws/show/z0952-20#Text (дата звернення 12.03.2024).

105. Деякі питання ведення Реєстру медичних записів, записів про направлення та рецептів в електронній системі охорони здоров'я: наказ Міністерства охорони здоров'я від 28 лютого 2020 року № 587. URL: https://zakon.rada.gov.ua/laws/show/z0236-20#top (дата звернення 12.03.2024).

106. Санжаровська Л.І. Правова інтерпретація інституту захисту персональних даних у сфері охорони здоров'я. *Прикарпатський юридичний вісник.* 2024. № 1 (54). С. 84–87. DOI: https://doi.org/10.32782/pyuv.v1.2024.16.

107. Чернобай А.М. Правові засоби захисту персональних даних працівника: дис. ... канд. юрид. наук: 12.00.05. Одеса, 2006. 200 с.

108. Куценко Р.В. Поняття та склад персональних даних працівників за трудовим законодавством України. *Науковий вісник публічного та приватного права*. 2017. Вип. 1. С. 92-96.

109. Самойленко Ю.С. Адміністративно-правове забезпечення захисту персональних даних в Україні: дис. ... канд. юрид. наук: 12.00.07. Запоріжжя, 2023. 213 с.

110. Бусел В.Т. Великий тлумачний словник сучасної української мови (з дод. і допов.). К.; Ірпінь: ВТФ «Перун», 2005. 1728 с.

111. Українсько-російський словник складної лексики. К.: Вид. центр «Академія», 1998. 712 с.

112. Тимченко В.І. Особливості юридичного змісту термінів «захист» та «охорона» у механізмі забезпечення прав людини. *Вісник Академії управління МВС*. 2007. № 2–3. С. 58–65.

113. Тараненко С.М. Захист прав і свобод громадян у провадженні в справах про адміністративні правопорушення та їх забезпечення в діяльності міліції: автореф. дис. ... канд. юрид. наук: 12.00.07. Київ, 2000. 20 с.

114. Гіда Є.О. Міжнародна поліцейська енциклопедія: у 10-ти томах. Том 2 (Права людини у контексті поліцейської діяльності). К.: Ін Юре, 2005. 1224 с.

115. Миколенко О.М. Сучасний погляд на класифікацію функцій адміністративного права. *Правова держава*. 2017. № 25. С. 78–82.

116. Левицька Н.О. Міжгалузеві нормативно-правові інститути: деякі теоретичні питання. *Науковий вісник Міжнародного гуманітарного університету. Серія: Юриспруденція*. 2015. № 14. Том 1. С. 22-24.

117. Санжаровська Л.І. Правові особливості захисту фізичних осіб у зв'язку з обробкою персональних даних у сфері охорони здоров'я. *Актуальні питання у сучасній науці.* 2024. № 5 (23). С. 666–676. DOI: https://doi.org/10.52058/2786-6300-2024-5(23)-666-676.

118. Червякова О.Б., Мех Ю.В. Зобов'язання держави щодо захисту інформації про стан здоров'я пацієнтів: європейські стандарти та українські реалії. *Право і суспільство.* 2021. № 1. С. 158–168. DOI: https://doi.org/10.32842/2078-3736/2021.1.25.

119. Про подолання туберкульозу в Україні: Закон України від 14 липня 2023 року № 3269-IX. URL: https://zakon.rada.gov.ua/laws/show/3269-20#Text (дата звернення 21.03.2024).

120. Про протидію поширенню хвороб, зумовлених вірусом імунодефіциту людини (ВІЛ), та правовий і соціальний захист людей, які живуть з ВІЛ: Закон України від 12 грудня 1991 року № 1972-XII. URL: https://zakon.rada.gov.ua/laws/show/1972-12#Text (дата звернення 21.03.2024).

121. Про психіатричну допомогу: Закон України від 22 лютого 2000 року № 1489-III. URL: https://zakon.rada.gov.ua/laws/show/1489-14#Text (дата звернення 21.03.2024).

122. Про захист населення від інфекційних хвороб: Закон України від 06 квітня 2000 року № 1645-III. URL: https://zakon.rada.gov.ua/laws/show/1645-14#Text (дата звернення 21.03.2024).

123. Рішення Європейського суду з прав людини суд у справі «Z проти Фінляндії» від 25 січня 1997 року. URL: http://medicallaw.org.ua/fileadmin/user_upload/pdf/Z_against_Finland.pdf (дата звернення 21.03.2024).

124. Конвенція про захист прав людини і основоположних свобод від 04 листопада 1950 року (Європейська конвенція з прав людини). URL: https://zakon.rada.gov.ua/laws/show/995_004#Text (дата звернення 21.03.2024).

125. Куньч З.Й. Універсальний словник української мови. Тернопіль: Навчальна книга. Богдан, 2007. 848 с.

126. Новий тлумачний словник сучасної української мови / уклад.: Радченко І.О., Орлова О.М. Київ: ПП Голяка В.М., 2010. 768 с.

127. Про функціонування інформаційної системи «Моніторинг соціально значущих хвороб»: наказ Міністерства охорони здоров'я від 25 липня 2022 року № 1317. URL: https://zakon.rada.gov.ua/laws/show/z1031-22#Text (дата звернення 27.03.2024).

128. Про затвердження Положення про Міністерство охорони здоров'я України: постанова Кабінету Міністрів України від 25 березня 2015 року № 267. URL: https://zakon.rada.gov.ua/laws/show/267-2015-%D0%BF#n8 (дата звернення 27.03.2024).

129. Про утворення Національної служби здоров'я України: постанова Кабінету Міністрів України від 27 грудня 2017 року № 1101. URL: https://zakon.rada.gov.ua/laws/show/1101-2017-%D0%BF#Text (дата звернення 27.03.2024).

130. Про реабілітацію осіб з інвалідністю в Україні: Закон України від 06 жовтня 2005 року № 2961-IV. URL: https://zakon.rada.gov.ua/laws/show/2961-15#Text (дата звернення 27.03.2024).

131. Про затвердження Положення про централізований банк даних з проблем інвалідності: постанова Кабінету Міністрів України від 16 лютого 2011 року № 121. URL: https://zakon.rada.gov.ua/laws/show/121-2011-п#Text (дата звернення 27.03.2024).

132. Про Кабінет Міністрів України: Закон України від 27 лютого 2014 року № 794-VII. URL: https://zakon.rada.gov.ua/laws/show/794-18#Text (дата звернення 27.03.2024).

133. Бем М.В., Городиський І.М. Захист персональних даних: Правове регулювання та практичні аспекти: науково-практичний посібник. К.: К.І.С., 2021. 160 с.

134. Державне підприємство «Електронне здоров'я». URL: https://ehealth.gov.ua (дата звернення 31.03.2024).

135. Helsi. URL: https://helsi.me (дата звернення 31.03.2024).

136. Medcard24. URL: https://www.mis.coz.kvs.gov.ua (дата звернення 31.03.2024).

137. Moniheal. URL: https://myheal.com.ua (дата звернення 31.03.2024).

138. Health24. URL: https://h24.ua (дата звернення 31.03.2024).

139. Askep. URL: https://askep.net (дата звернення 31.03.2024).

140. Ваші діагнози в їхніх руках: що електронні медсервіси роблять з персональними даними і чим це загрожує. URL: https://cedem.org.ua/analytics/elektronni-medservisy (дата звернення 31.03.2024).

141. Рішення Європейського суду з прав людини у справі «Gardel v. France» («Гардел проти Франції») від 17 грудня 2009 року. URL: https://hudoc.echr.coe.int/eng?i=001-117751#{"itemid":["001-117751"]} (дата звернення 31.03.2024).

142. Коробцова Н. Заклади охорони здоров'я як учасники відносин із захисту персональних даних. *Медичне право*. 2014. Вип. 1(13). С. 26-32.

143. Санжаровська Л.І. Захист персональних даних у сфері охорони здоров'я Уповноваженим Верховної Ради України з прав людини. *Правові засади організації та здійснення публічної влади*: збірник тез VII Міжнародної науково-

практичної конференції, присвяченої світлій пам’яті доктора юридичних наук, професора, академіка-засновника НАПрНУ, першого Голови Конституційного Суду України Леоніда Петровича Юзькова (м. Хмельницький, 17 травня 2024 року). Хмельницький: Хмельницький університет управління та права імені Леоніда Юзькова, 2024. С. 213–214.

144. Марцеляк О.В. Інститут омбудсмана: теорія і практика: монографія. Х.: ХНУВС, 2004. 450 с.

145. Банах С.В. Функції омбудсманів у сучасному світі: порівняльно-правове дослідження: дис. ... канд. юрид. наук: 12.00.02. Маріуполь, 2014. 236 с.

146. Бем М. В., Городиський І. М., Саттон Г., Родіоненко О. М. Захист персональних даних: Правове регулювання та практичні аспекти: науково-практичний посібник. К.: К.І.С., 2015. 220 с.

147. Постанова Дніпровського районного суду м. Києва від 15 квітня 2015 року у справі № 755/3821/15-п. URL: http://reyestr.court.gov.ua/Review/43778626 (дата звернення 11.04.2024).

148. Постанова Дарницького районного суду м. Києва від 11 вересня 2015 року у справі № 753/13021/15-п. URL: http://reyestr.court.gov.ua/Review/50886437 (дата звернення 11.04.2024).

149. Постанова Голосіївського районного суду м. Києва від 02 листопада 2015 року у справі № 752/15256/15-п. URL: http://reyestr.court.gov.ua/Review/53305602 (дата звернення 11.04.2024).

150. Постанова Оболонського районного суду міста Києва від 19 жовтня 2016 року у справі № 756/11255/16-п. URL: http://reyestr. court.gov.ua/Review/62225162 (дата звернення 11.04.2024).

151. Постанова Жовтневого районного суду міста Дніпропетровська від 14 вересня 2017 року у справі № 201/12780/17-п. URL: http://reyestr.court.gov.ua/Review/68948324 (дата звернення 11.04.2024).

152. Постанова Коломийського міськрайонного суду Івано-Франківської області від 14 лютого 2017 року у справі № 346/200/17. URL: http://reyestr.court.gov.ua/Review/64723526 (дата звернення 11.04.2024).

153. Постанова Галицького районного суду Львівської області від 03 квітня 2017 року у справі № 461/2021/17. URL: http://www.reyestr.court.gov.ua/Review/65734627 (дата звернення 11.04.2024).

154. Постанова Московського районного суду міста Харкова від 04 травня 2017 року у справі № 643/3384/17. URL: http://reyestr.court.gov.ua/Review/66441353 (дата звернення 11.04.2024).

155. Постанова Татарбунарського районного суду Одеської області від 09 липня 2018 року у справі № 515/952/18. URL: http://reyestr.court.gov.ua/Review/75208254 (дата звернення 11.04.2024).

156. Постанова Жовтневого районного суду міста Маріуполя від 11 травня 2018 року у справі № 263/4314/18. URL: http://reyestr.court.gov.ua/Review/73915418 (дата звернення 11.04.2024).

157. Постанова Подільського районного суду міста Києва від 29 грудня 2018 року у справі № 758/4389/17. URL: http://reyestr.court.gov.ua/Review/71400435 (дата звернення 11.04.2024).

158. Постанова Городищенського районного суду Черкаської області від 27 листопада 2018 року у справі № 691/1261/17. URL: http://reyestr.court.gov.ua/Review/70667984 (дата звернення 11.04.2024).

159. Постанова Івано-Франківського міського суду Івано-Франківської області від 26 вересня 2018 року у справі № 344/8443/17. URL: http://reyestr.court.gov.ua/Review/70072924 (дата звернення 11.04.2024).

160. Постанова Ковпаківського районного суду м. Суми від 07 липня 2015 року у справі № 592/6260/15-п. URL: http://reyestr.court.gov.ua/Review/46341181 (дата звернення 11.04.2024).

161. Постанова Золочівського районного суду Львівської області від 20 грудня 2016 року у справі 445/2022/16-п. URL: http://reyestr.court.gov.ua/Review/63869054 (дата звернення 11.04.2024).

162. Самойленко Ю.С. Система адміністративно-правових засобів захисту персональних даних. *Верховенство права: доктрина і практика в умовах*

сучасних світових викликів: матеріали Міжнар. наук.-практ. конф. (м. Дніпро, 25 лют. 2021 р.). Дніпро: Дніпроп. держ. ун-т внутр. справ, 2021. С. 222-226.

163. Постанова Жовтоводського міського суду Дніпропетровської області від 31 жовтня 2016 року у справі № 176/2309/16-п. URL: http://reyestr.court.gov.ua/Review/62786003 (дата звернення 11.04.2024).

164. Дем'яненко Ю.І. Кримінальна відповідальність запорушення недоторканності приватного життя: дис. ... канд. юрид. наук: 12.00.08. Харків, 2008. 242 с.

165. Вирок Шевченківського районного суду міста Києва від 08 грудня 2014 року у справі № 761/29030/13-к. URL: https://reyestr.court.gov.ua/Review/42173797 (дата звернення 23.04.2024).

166. Вирок Баглейського районного суду Дніпродзержинська від 13 лютого 2013 року у справі № 404/5528/12. URL: https://reyestr.court.gov.ua/Review/29396197 (дата звернення 23.04.2024).

167. Вирок Придніпровського районного суду міста Черкаси від 29 квітня 2011 року у справі № 1-162/11. URL: https://reyestr.court.gov.ua/Review/49482456 (дата звернення 23.04.2024).

168. Щорічна доповідь Уповноваженого Верховної Ради України з прав людини про стан додержання та захисту прав і свобод людини і громадянина. 136 с. URL: https://ombudsman.gov.ua/storage/app/media/uploaded-files/report-2019-3.pdf (дата звернення 25.04.2024).

169. Щорічна доповідь Уповноваженого Верховної Ради України з прав людини про стан додержання та захисту прав і свобод людини і громадянина. 258 с. URL: https://ombudsman.gov.ua/storage/app/media/uploaded-files/zvit%20za%202019.pdf (дата звернення 25.04.2024).

170. Щорічна доповідь Уповноваженого Верховної Ради України з прав людини про стан додержання та захисту прав і свобод людини і громадянина. 355 с. URL: https://ombudsman.gov.ua/storage/app/media/uploaded-files/schoricha-dopovid-2020.pdf (дата звернення 25.04.2024).

171. Щорічна доповідь Уповноваженого Верховної Ради України з прав людини про стан додержання та захисту прав і свобод людини і громадянина. 428 с. URL: https://ombudsman.gov.ua/storage/app/media/uploaded-files/schoricha-dopovid-2021.pdf (дата звернення 25.04.2024).

172. Щорічна доповідь Уповноваженого Верховної Ради України з прав людини про стан додержання та захисту прав і свобод людини і громадянина у 2023 році. 334 с. URL: https://ombudsman.gov.ua/report-2023/images/documents/annual-report-2023.pdf (дата звернення 25.04.2024).

173. Про виконання рішень та застосування практики Європейського суду з прав людини: Закон України від 23 лютого 2006 року № 3477-IV. URL: https://zakon.rada.gov.ua/laws/show/3477-15#Text (дата звернення дата звернення 30.04.2024).

174. Загальна декларація прав людини від 10 грудня 1948 року. URL: https://zakon.rada.gov.ua/laws/show/995_015#Text (дата звернення 02.05.2024).

175. Міжнародний пакт про громадянські і політичні права від 16 грудня 1966 року. URL: https://zakon.rada.gov.ua/laws/show/995_043#Text (дата звернення 02.05.2024).

176. Конвенція про права осіб з інвалідністю від 13 грудня 2006 року. URL: https://zakon.rada.gov.ua/laws/show/995_g71#Text (дата звернення 02.05.2024).

177. Антонова Л.В., Козлова Л.В. Міжнародний досвід регулювання й дотримання етичних норм в сфері охорони здоров'я. *Державне управління: удосконалення та розвиток.* 2020. № 4. URL: http://www.dy.nayka.com.ua/pdf/4_2020/6.pdf (дата звернення 02.05.2024).

178. Женевська декларація: Міжнародний документ Всесвітньої медичної асоціації від 01 вересня 1948 року. URL: https://zakon.rada.gov.ua/laws/show/990_001#Text (дата звернення 07.05.2024).

179. Міжнародний кодекс медичної етики: Міжнародний документ Всесвітньої медичної асоціації від 01 жовтня 1949 року. URL: https://zakononline.com.ua/documents/show/140842___140842 (дата звернення 07.05.2024).

180. Дванадцять принципів організації охорони здоров'я для будь-якої національної системи охорони здоров'я: Міжнародний документ Всесвітньої медичної асоціації від 01 жовтня 1963 року. URL: https://zakononline.com.ua/documents/show/140460___140460 (дата звернення 07.05.2024).

181. Лісабонська декларація стосовно прав пацієнта: Міжнародний документ Всесвітньої медичної асоціації від 01 жовтня 1981 року. URL: https://zakononline.com.ua/documents/show/159441___159441 (дата звернення 07.05.2024).

182. Щирба М.Ю. Міжнародно-правове регулювання конфіденційності у сфері охорони здоров'я. *Прикарпатський юридичний вісник.* 2016. № 4 (13). С. 15–18.

183. Тимчасове положення про СНІД: Міжнародний документ Всесвітньої медичної асоціації від 30 жовтня 1987 року. URL: https://zakononline.com.ua/documents/show/157773___157773 (дата звернення 07.05.2024).

184. Декларація про проєкт «Геном людини»: Міжнародний документ Всесвітньої медичної асоціації від 01 вересня 1992 року. URL: https://zakononline.com.ua/documents/show/151634___151634 (дата звернення 07.05.2024).

185. Положення про захист прав та конфіденційність пацієнта: Міжнародний документ Всесвітньої медичної асоціації від 01 жовтня 1993 року. URL: https://med.sumdu.edu.ua/images/content/doctors/Deontology/Budapest_1993.pdf (дата звернення 07.05.2024).

186. Декларація про політику в галузі забезпечення прав пацієнта в Європі 1994 року. URL: https://med.sumdu.edu.ua/images/content/doctors/Deontology/Patients_rights_WHO.pdf (дата звернення 07.05.2024).

187. Конвенція про захист прав і гідності людини щодо застосування біології та медицини від 04 квітня 1997 року. URL: https://zakon.rada.gov.ua/laws/show/994_334#Text (дата звернення 07.05.2024).

188. Пазюк А.В. Захист прав людини стосовно обробки персональних даних: міжнародні стандарти / МГО Прайвесі Юкрейн. К.: Інтертехнодрук, 2000. 69 с.

189. Брижко В.М. Про упорядкування законодавства України із захисту персональних даних. *Правова інформатика*. 2008. № 1(17). С. 20-34.

190. Директива Європейського Парламенту і Ради Європейського Союзу про захист фізичних осіб при обробці персональних даних і про вільне переміщення таких даних від 24 жовтня 1995 року № 95/46/ЄС. URL: https://zakon.rada.gov.ua/laws/show/994_242#Text (дата звернення 07.05.2024).

191. Мельник К.С. Правові механізми захисту персональних даних в Європейському Союзі. *Правова інформатика*. 2013. № 4 (40). С. 55-61. URL: http://ippi.org.ua/sites/default/files/13mksdes.pdf (дата звернення 07.05.2024).

192. Хартія Європейського Союзу про основоположні права. URL: https://ccl.org.ua/posts/2021/11/hartiya-osnovnyh-prav-yevropejskogo-soyuzu/ (дата звернення 14.05.2024).

193. Дяковський О.С. Правове регулювання захисту персональних даних в Європейському Союзі. *Юридичний науковий електронний журнал*. 2023. № 7. С. 266–269. DOI: https://doi.org/10.32782/2524-0374/2023-7/61.

194. Захист персональних даних у сфері охорони здоров'я в ЄС: законодавчий ландшафт. URL: https://www.apteka.ua/article/575210 (дата звернення 16.05.2024).

195. Регламент Європейського Парламенту і Ради Європейського Союзу 2017/745 від 5 квітня 2017 року про медичні вироби, внесення змін до Директиви 2001/83/ЄС, Регламенту (ЄС) № 178/2002 і Регламенту (ЄС) № 1223/2009 та скасування директив Ради 90/385/ЄЕС і 93/42/ЄЕС. URL: https://www.kmu.gov.ua/storage/app/sites/1/55-GOEEI/es-2017745.pdf (дата звернення 16.05.2024).

196. Директива Європейського Парламенту і Ради Європейського Союзу 97/66/ЄС від 15 грудня 1997 року стосовно обробки персональних даних і захисту права на невтручання в особисте життя в телекомунікаційному секторі. URL: https://zakon.rada.gov.ua/laws/show/994_243#Text (дата звернення 16.05.2024).

197. Директива Європейського Парламенту і Ради Європейського Союзу 2016/1148 від 6 липня 2016 року про заходи для високого спільного рівня безпеки мережевих та інформаційних систем на території Союзу. URL: https://zakon.rada.gov.ua/laws/show/984_013-16#Text (дата звернення 16.05.2024).

198. Директива Європейського Парламенту і Ради Європейського Союзу 2018/1972 від 11 грудня 2018 року про запровадження Європейського кодексу електронних комунікацій. URL: https://zakon.rada.gov.ua/laws/show/984_013-18#Text (дата звернення 16.05.2024).

199. Посібник з європейського права у сфері захисту персональних даних. К.: К.І.С., 2020. 432 с.

200. Рішення ЄСПЛ у справі Scozzari and Giunta v. Italy. URL: http://eurocourt.in.ua/Article.asp?AIdx=278 (дата звернення 24.05.2024).

201. Рішення Європейського суду з прав людини щодо захисту персональних даних. 132 с. URL: (дата звернення 24.05.2024)

202. Рішення Європейського суду з прав людини щодо доступу до інформації / За заг. редакцією Шевченко Т.С., Розкладай І.Є. К.: Москаленко О.М., 2014. 200 с.

203. Рішення у справі «Ротару проти Румунії». Комюніке Секретаря Суду (Judgment in the case of Rotaru v. Romania). URL: http://eurocourt.in.ua/Article.asp?AIdx=212 (дата звернення 24.05.2024).

204. Рішення ЄСПЛ у справі «Catt v. United Kingdom». URL: https://hudoc.echr.coe.int/fre#{"itemid":["001-189424"]} (дата звернення 24.05.2024).

205. Рішення ЄСПЛ у справі «S. & Marper v. United Kingdom». URL: https://rm.coe.int/168059920d (дата звернення 24.05.2024).

206. Рішення ЄСПЛ у справі GSB v. Switzerland. URL: https://hudoc.echr.coe.int/eng?i=001-159732#{"itemid":["001-159732"]} (дата звернення 24.05.2024).

207. Тимошенко О.А. Захист персональних даних в цивільних правовідносинах: вітчизняне правове забезпечення крізь призму практики Європейського суду з прав людини. Електронне наукове видання «Аналітично-порівняльне правознавство». 2023. № 4. С. 165–172. URL: https://app-journal.in.ua/wp-content/uploads/2023/09/29.pdf (дата звернення 24.05.2024) DOI: https://doi.org/10.24144/2788-6018.2023.04.27.

208. Рішення Європейського суду з прав людини у справі «Пантелеєнко проти України» від 29 червня 2006 року. URL: https://zakon.rada.gov.ua/laws/show/974_274#Text (дата звернення 24.05.2024).

209. Рішення Європейського суду з прав людини у справі «Заїченко проти України (№ 2) від 26 лютого 2015 року. URL: https://zakon.rada.gov.ua/laws/show/974_a87#Text (дата звернення 24.05.2024).

210. Рішення Європейського суду з прав людини у справі «М.К. проти України» від 15 грудня 2022 року. URL: https://zakon.rada.gov.ua/laws/show/974_i18#Text (дата звернення 24.05.2024).

211. Про рішення Ради національної безпеки і оборони України від 15 жовтня 2021 року «Про Стратегію інформаційної безпеки»: Указ Президента України від 28 грудня 2021 року № 685/2021. URL: https://zakon.rada.gov.ua/laws/show/685/2021#Text (дата звернення 04.06.2024).

212. Про Національну стратегію у сфері прав людини: Указ Президента України від 24 березня 2021 року № 119/2021. URL: https://zakon.rada.gov.ua/laws/show/119/2021#top (дата звернення 04.06.2024).

213. Case of M.S. v. Sweden № 20837/92. URL: https://hudoc.echr.coe.int/eng?i=001-58177#{"itemid":["001-58177"]}(дата звернення 04.06.2024).

214. Пономаренко І. С., Гуз А. М. Міжнародна та вітчизняна практика впровадження медичних інформаційних систем. *Наукові записки Міжнародного гуманітарного університету*. 2022. Вип. 36. С. 26-30.

215. В омбудсмена назвали найбільшу загрозу для безпеки персональних медичних даних. URL: https://www.ukrinform.ua/amp/rubric-society/3063627-v-ombudsmena-nazvali-najbilsu-zagrozu-dla-bezpeki-personalnih-medicnih-danih.html (дата звернення 04.06.2024).

216. Положення про порядок обробки персональних даних в медичній мережі «Добробут». URL: https://dobrobut.com/ua/about/c-polozenna-pro-poradok-obrobki-personalnih-danih-v-mm-dobrobut (дата звернення 04.06.2024).

217. Публічний договір про надання медичних послуг. URL: https://dila.ua/publichna-uhoda.html (дата звернення 04.06.2024).

218. Положення про обробку та захист персональних даних пацієнті. URL: https://hh.com.ua/polozhennja-pro-obrobku-ta-zahist-personalnih-danih-paciientiv (дата звернення 04.06.2024).

219. Санжаровська Л.І. Принципи обробки персональних даних у сфері охорони здоров'я. *Проблеми захисту прав та свобод людини і громадянина*: матеріали X Всеукраїнської наук.-практ. конф. молодих учених і студентів (м. Чернігів, 17 травня 2024 р.). Чернігів: НУ «Чернігівська політехніка», 2024. С. 40–42.

220. Про державну реєстрацію геномної інформації людини: Закон України від 9 липня 2022 року № 2391-IX. URL: https://zakon.rada.gov.ua/laws/show/2391-20#Text (дата звернення 07.06.2024).

221. Статистичний звіт за результатами роботи Системи виявлення вразливостей і реагування на кіберінциденти та кібератаки в 2023 році. URL: https://scpc.gov.ua/uk/articles/334 (дата звернення 12.06.2024).

222. Корнєєва С.Р. Вплив застосування технологій штучного інтелекту на реалізацію та захист прав людини. *Електронне наукове видання «Аналітично-порівняльне правознавство»*. 2021. № 4. С. 392-394. URL: https://app-

journal.in.ua/wp-content/uploads/2022/03/71.pdf (дата звернення 12.06.2024). DOI: https://doi.org/10.24144/2788-6018.2021.04.69.

223. Бєлова М.В., Бєлов Д.М. Виклики та загрози захисту персональних даних у роботі зі штучним інтелектом. *Науковий вісник Ужгородського національного університету. Серія Право*. 2023. Випуск 79. Частина 2. С. 17-22. DOI: https://doi.org/10.24144/2307-3322.2023.79.2.2.

224. Санжаровська Л.І. Вплив застосування технологій штучного інтелекту на захист персональних даних у сфері охорони здоров'я. *Актуальні проблеми приватного та публічного права*: матеріали VI Міжнародної науково-практичної конференції присвяченої 95-річчю від дня народження члена-кореспондента НАПрН України, академіка Міжнародної кадрової академії, Заслуженого діяча науки України, доктора юридичних наук, професора Процевського О.І., Ломжа – Харків, 29 березня 2024 року. Ломжа: Міжнародна Академія Прикладних Наук в Ломжі, Республіка Польща; Харків: Харківський національний педагогічний університет імені Г.С. Сковороди, Україна. Видавництво: MANS w Łomży – Харків: ХНПУ імені Г.С. Сковороди, 2024. С. 317–320.

225. Про схвалення Концепції розвитку штучного інтелекту в Україні: розпорядження Кабінету Міністрів України від 2 грудня 2020 року № 1556-р. URL: https://zakon.rada.gov.ua/laws/show/1556-2020-р#Text (дата звернення 12.06.2024).

226. Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) № 300/2008, (EU) № 167/2013, (EU) № 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act). URL: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202401689 (дата звернення 12.06.2024).

227. Про Національну комісію з питань захисту персональних даних та доступу до публічної інформації: Проєкт Закону України від 18 жовтня 2021 року № 6177. URL: http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=72992 (дата звернення 14.06.2024).

228. Деякі питання діяльності Міністерства культури та інформаційної політики: постанова Кабінету Міністрів України від 6 жовтня 2019 року № 885. URL: https://zakon.rada.gov.ua/laws/show/885-2019-п#Text (дата звернення 14.06.2024).

229. Санжаровська Л.І. Адаптація законодавства про захист персональних даних у сфері охорони здоров'я України до законодавства Європейського Союзу. *Історико-філософські, політико-правові та соціальні засади трансформації України та держав європейської спільноти*: матеріали І Міжнародної науково-практичної конференції (19 квітня 2024 р.). Одеса: ОНМУ, 2024. С. 119–121.

230. Угода про асоціацію між Україною, з однієї сторони, та Європейським Союзом, Європейським співтовариством з атомної енергії і їхніми державами-членами, з іншої сторони від 21 березня 2014 року. URL: http://zakon5.rada.gov.ua/laws/show/984_011/page (дата звернення 19.06.2024).

231. Про виконання Угоди про асоціацію між Україною, з однієї сторони, та Європейським Союзом, Європейським співтовариством з атомної енергії і їхніми державами-членами, з іншої сторони: постанова Кабінету Міністрів України від 25 жовтня 2017 року № 1106. URL: https://zakon.rada.gov.ua/laws/show/1106-2017-%D0%BF#Text (дата звернення 19.06.2024).

232. Про захист персональних даних: Проєкт Закону України від 25 жовтня 2022 року № 8153. URL: https://itd.rada.gov.ua/billInfo/Bills/Card/40707 (дата звернення 25.06.2024).

233. Картка проходження Проєкту Закону України від 25 жовтня 2022 року № 8153 «Про захист персональних даних». URL: https://ips.ligazakon.net/document/JI08275I?an=1 (дата звернення 25.06.2024).

234. Правовий висновок проєкту «Підтримка впровадження європейських стандартів прав людини в Україні» на проєкт Закону України від 25 жовтня 2022 року № 8153 «Про захист персональних даних. URL: https://rm.coe.int/ua-opinion-on-the-draft-law-of-ukraine-on-personal-data-protection-/1680ad38bf (дата звернення 25.06.2024).

Додаток А

СПИСОК ПУБЛІКАЦІЙ ЗДОБУВАЧА ЗА ТЕМОЮ ДИСЕРТАЦІЇ:

в яких опубліковані основні наукові результати дисертації:

1. Санжаровська Л.І. Правова інтерпретація інституту захисту персональних даних у сфері охорони здоров'я. *Прикарпатський юридичний вісник.* 2024. № 1 (54). С. 84–87. DOI: https://doi.org/10.32782/pyuv.v1.2024.16.

2. Санжаровська Л.І. Поняття та сутність персональних даних у сфері охорони здоров'я. *Наука і техніка сьогодні.* 2024. № 3 (31). С. 182-192. DOI: https://doi.org/10.52058/2786-6025-2024-3(31)-182-192.

3. Санжаровська Л.І. Правові особливості захисту фізичних осіб у зв'язку з обробкою персональних даних у сфері охорони здоров'я. *Актуальні питання у сучасній науці.* 2024. № 5 (23). С. 666–676. DOI: https://doi.org/10.52058/2786-6300-2024-5(23)-666-676.

які засвідчують апробацію матеріалів дисертації:

4. Санжаровська Л.І. Вплив застосування технологій штучного інтелекту на захист персональних даних у сфері охорони здоров'я. *Актуальні проблеми приватного та публічного права*: матеріали VI Міжнародної науково-практичної конференції присвяченої 95-річчю від дня народження члена-кореспондента НАПрН України, академіка Міжнародної кадрової академії, Заслуженого діяча науки України, доктора юридичних наук, професора Процевського О.І., Ломжа – Харків, 29 березня 2024 року. Ломжа: Міжнародна Академія Прикладних Наук в Ломжі, Республіка Польща; Харків: Харківський національний педагогічний університет імені Г.С. Сковороди, Україна. Видавництво: MANS w Łomży – Харків: ХНПУ імені Г.С. Сковороди, 2024. С. 317–320.

5. Санжаровська Л.І. Адаптація законодавства про захист персональних даних у сфері охорони здоров'я України до законодавства Європейського Союзу. *Історико-філософські, політико-правові та соціальні засади трансформації*

України та держав європейської спільноти: матеріали І Міжнародної науково-практичної конференції (19 квітня 2024 р.). Одеса: ОНМУ, 2024. С. 119–121.

6. Санжаровська Л.І. Принципи обробки персональних даних у сфері охорони здоров'я. *Проблеми захисту прав та свобод людини і громадянина*: матеріали Х Всеукраїнської наук.-практ. конф. молодих учених і студентів (м. Чернігів, 17 травня 2024 р.). Чернігів: НУ «Чернігівська політехніка», 2024. С. 40–42.

7. Санжаровська Л.І. Захист персональних даних у сфері охорони здоров'я Уповноваженим Верховної Ради України з прав людини. *Правові засади організації та здійснення публічної влади*: збірник тез VII Міжнародної науково-практичної конференції, присвяченої світлій пам'яті доктора юридичних наук, професора, академіка-засновника НАПрНУ, першого Голови Конституційного Суду України Леоніда Петровича Юзькова (м. Хмельницький, 17 травня 2024 року). Хмельницький: Хмельницький університет управління та права імені Леоніда Юзькова, 2024. С. 213–214.