УДК 342.5
DOI https://doi.org/10.32782/TNU-2707-0581/2025.1/12

Кобрусєва Є.А.
Дніпровський національний університет імені Олеся Гончара

ІНФОРМАЦІЙНА БЕЗПЕКА «ЧУТЛИВИХ ДАНИХ» ЯК СКЛАДОВА ЗАХИСТУ ПРАВ ЛЮДИНИ: ВІТЧИЗНЯНИЙ ТА МІЖНАРОДНИЙ ДОСВІД

У статті проаналізовано основні норми вітчизняного та міжнародного законодавства у частині щодо права на захист «чутливих» персональних даних. Констатовано, що незважаючи на чіткі законодавчі норми, мають місце факти порушень у частині, що стосується: відсутності як мети, так і доцільності об'ємного збору даних; неврахування індивідуальних обставин осіб, чиї дані зберігаються; зміни визначеної мети обробки «чутливих даних», яка є несумісною з попередньою; відсутності підстави для подальшого зберігання та обробки інформації. Досліджено загальні, спеціальні та основні норми міжнародного права з питань регламентації діяльності з питань захисту «чутливої» інформації». Розглянуто прецедентну практику Європейського суду з прав людини у контексті досліджуваної тематики (рішення ЄСПЛ у справах: «M. C. проти Швеції», «Z проти Фінляндії», «I. v. Finland», «Avilkina and Others v. Russia»). Окреслено основні принципи обробки «чутливих» персональних даних (законності, справедливості, легітимної мети, підзвітності, необхідності, пропорційності, ефективного захисту). Виокремлено типові порушення щодо порядку збору, обробки та захисту інформації: неповідомлення особи про обробку «чутливих» персональних даних; транскордонна передача даних; порушення строків зберігання; неповідомлення суб'єкта про дії з персональними даними; ідентифікація особи отримувача. Аргументовано, що найсерйозніші порушення законодавства виникають саме внаслідок неправомірної передачі персональних даних третім особам, яка повинна здійснюватися за наявності підстав, визначених ст. 7 та 11 Закону України «Про захист персональних даних» та відповідати визначеним принципам. Теоретично обгрунтовано, що забезпечення права людини на захист «чутливих» персональних даних – важливий показник як демократичності держави, так і інтеграції національного права у світове співтовариство, відповідно, як держава, так і організації, які є володільцями персональних даних, повинні вживати необхідні заходи щодо захисту даних та запобігання їх витоку.

Ключові слова: *«чутливі» персональні дані, право на захист, норми законодавства, інформаційна безпека, автоматизована обробка.*

Постановка проблеми. Захист персональних даних – не лише обов'язок держави, але й складова захисту прав людини. «Кожен має право на вільне одержання, використання, поширення, зберігання та захист інформації, необхідної для реалізації своїх прав, свобод і законних інтересів», – визначено у Законі України «Про інформацію» [1]. Декларацією про політику в галузі забезпечення прав пацієнта в Європі, яка є загальноєвропейською програмою дій, передбачено: «…. уся інформація щодо стану здоров'я пацієнта, прогноз і лікування його захворювання, а також будь-яка інша інформація особистого характеру повинна зберігатись у таємниці навіть після смерті пацієнта …» (п. 4.1), «… пацієнти, які потрапляють у лікувально-профілактичні заклади, мають право розраховувати на наявність у цьому закладі устаткування, необхідного для гарантії зберігання медичної таємниці» (п. 4.8) [2]. Загальним регламентом Європейського Парламенту і Ради (ЄС) «Про захист фізичних осіб у зв'язку з опрацюванням персональних даних і про вільний рух таких даних, та про скасування Директиви 95/46/ЄС» (Регламент) передбачено, що персональні дані, які є особливо чутливими, потребують особливого захисту, так як контекст їх обробки може створити значні ризики щодо прав і свобод людини. Оброблення та використання спеціальних категорій персональних даних можливе без згоди об'єкта даних лише з метою забезпечення їх суспільних інтересів у медичній сфері [3].

Проте незважаючи на чіткі законодавчі норми, мають місце факти порушень у частині, що стосується: відсутності як мети, так і доцільності

об'ємного збору даних; неврахування індивідуальних обставин осіб, чиї дані зберігаються; зміни визначеної мети обробки «чутливих даних», яка є несумісною з попередньою; відсутності підстави для подальшого зберігання та обробки інформації. Проблема забезпечення права на захист інформації на сьогодні стала визначальним чинником не тільки інформаційної, а й загальної безпеки на індивідуальному, регіональному і глобальному рівнях. Доволі часто ця проблематика посилюється недосконалістю правової системи, нерозвиненістю суспільної правосвідомості й правової культури, що створює умови неповаги до верховенства права й інших загальнолюдських цінностей [4, с. 4–5].

Аналіз останніх досліджень і публікацій. Проблематику дотримання прав людини на захист інформації у сфері охорони здоров'я досліджували М. Банчук, М. Бем, І. Демченко, Б. Михайличенко, В. Москаленко, О. Родіоненко, І. Сенюта, А. Січкар, Х. Терешко, О. Тихомиров та інші. Разом з тим, як свідчить аналіз вітчизняного та міжнародного законодавства, наукових досліджень у даному напрямі, а також судової практики Європейського суду з прав людини, у зв'язку з останніми законодавчими змінами вони частково втратили актуальність.

Постановка завдання. Мета статті дослідження основних законодавчих норм права людини на захист «чутливих» персональних даних як складової права на безпеку у контексті захисту інформаційних прав, визначення проблематики та окреслення шляхів удосконалення.

Виклад основного матеріалу. У контексті права на повагу до особистого (приватного) життя у сфері охорони здоров'я виокремлюють два напрями – право на доступ та право на захист інформації [5]. Міжнародним законодавством виокремлено наступні напрями закріплення прав пацієнта: універсальний (універсальні нормативно-правові акти, які, як правило, мають декларативний характер і виступають у якості рекомендацій), регіональний (нормативно-правові акти регіонального рівня – документи, прийняті Радою Європи, які мають обов'язковий характер) та спеціалізований (документи, прийняті спеціально створеною організацією) [6]. Що стосується регламентації діяльності з питань захисту «чутливої» інформації», то, відповідно до норм міжнародного права, вони поділяються на три групи: загальні норми (право на приватність – ст. 12 Загальної декларації прав людини, ст. 17 Міжнародного пакту про громадянські і політичні права, ст. 8-1 Конвенції про захист прав людини і основоположних свобод, Міжнародна конвенція про охорону осіб при автоматизованій обробці особистих даних (Конвенція), Додатковий протокол до Конвенції про захист осіб у зв'язку з автоматизованою обробкою персональних даних щодо органів нагляду та транскордонних потоків даних (ETS № 181), Директива 95/46/ES про охорону фізичних осіб у зв'язку з обробкою персональних даних та про вільний рух таких даних (Директива) [7]), спеціальні норми (визначено питання щодо захисту інформації у медичній сфері – Женевська декларація, Міжнародний кодекс медичної етики, шостий з Дванадцяти принципів організації охорони здоров'я для будь-якої національної системи охорони здоров'я, Лісабонська декларація стосовно прав пацієнта) та основні норми.

Право на захист «чутливої інформації» регламентовано також прецедентною практикою Європейського суду з прав людини (ЄСПЛ). Так, у рішеннях ЄСПЛ у справах: «M. C. проти Швеції» та «Z проти Фінляндії» звертається увага на те, що конфіденційність відомостей про здоров'я є основним принципом правової системи держав-учасниць Конвенції, а тому дуже важливо не лише дотримуватись конфіденційності медичної інформації, але й забезпечувати довіру пацієнта до медичних послуг загалом [8]; «I. v. Finland» (заява № 20511/03) зазначено, що факт відсутності обліку фактів щодо надання доступу до медичної документації заявниці призвів до унеможливлення встановлення особи, яка ймовірно поширила інформацію, що містилася у ній; «Avilkina and Others v. Russia» (заява № 1585/09) наголошено на законодавчій невизначеності повноважень прокуратури щодо збору медичної інформації про особу [7].

Типові положення зазначених вище рішень ЄСПЛ стали основою для прийнятої Конвенції Ради Європи «Про захист осіб у зв'язку з автоматизованою обробкою персональних даних» та Додаткового протоколу до міжнародного договору, яким аргументовано важливість створення Конвенції наглядового органу, основним завданням якого буде контроль щодо дотримання норм законодавства про захист персональних даних [7].

Обробка «чутливих персональних даних», відповідно до ст. 5 Конвенції, ст. 6 Директиви, ст. 5 Регламенту, ст. 6 Закону України «Про інформацію» здійснюється з використанням принципів законності, справедливості, легітимної мети, підзвітності, необхідності, пропорційності, ефективного захисту. Вартим уваги є принцип необ-

хідності та пропорційності збору персональних «чутливих» даних. Відповідно до ч. 1 ст. 5 Конвенції про захист осіб у зв'язку із автоматизованою обробкою персональних даних, персональні дані, які підлягають автоматизованій обробці, зберігаються виключно для легітимних цілей і використовуються у спосіб, який не суперечить їм. Персональні дані, зібрані для різних цілей, не повинні об'єднуватися, крім випадків, коли вказані цілі є сумісними, а склад персональних даних, які необхідні для досягнення обох цілей, збігається [9; 7].

Серед типових порушень права на захист «чутливих» персональних даних варто виокремити:

– неповідомлення особи про обробку «чутливих» персональних даних (у разі, якщо компанія здійснює обробку «чутливих» персональних даних, вона зобов'язана забезпечити посилений контроль як за обробкою, так і захистом даних);

– транскордонна передача даних (відповідно до чинного законодавства передача «чутливих» персональних даних здійснюється виключно за умови забезпечення державою, яка їх отримує (держави-учасниці Європейського економічного простору, держави, що підписали Конвенцію), належного захисту таких даних);

– порушення строків зберігання («чутливі» персональні дані підлягають видаленню або знищенню у разі закінчення строку їх зберігання. Проблематика визначення та дотримання строків зберігання обумовлена: неврегульованістю питань зберігання інформації на рівні внутрішніх нормативно-правових актів; недостатнім контролем за реалізацією цих процесів, що сприяє необґрунтовано довгому та безстроковому їх зберіганню. Слід зазначити, що Загальним регламентом захисту персональних даних 2016/679 (GDPR), норми якого передбачено у проєкті Закону України «Про захист персональних даних» № 8153, визначено вищі стандарти стосовно інформованої згоди та обов'язків щодо повідомлення (ст. 7), а також посилення захисту права на доступ до персональних даних щодо стану здоров'я. Заслуговує на увагу і те, що у разі витоку персональних даних (ст.ст. 33, 34) контролери упродовж 72 год. повинні проінформувати контролюючий орган, у разі ж порушення безпеки даних – інформують пацієнтів [10]. Даним документом розширено і питання щодо прав пацієнтів – передбачено право вимагати від контролерів та процесорів видаляти інформацію щодо стану їх здоров'я. Також GDPR визначено, що найвищий рівень конфіденційності автоматично застосовується до нового сервісного продукту щодо стану здоров'я [11]);

– неповідомлення суб'єкта про дії з персональними даними (відповідно до чинного законодавства, володільці персональних даних зобов'язані упродовж 10 робочих днів повідомити суб'єкта про зміну, видалення, знищення чи передачу даних третій особі [12]. Зазначимо, що найсерйозніші порушення законодавства виникають саме внаслідок неправомірної передачі персональних даних третім особам, яка повинна здійснюватися за наявності підстав, передбачених ст. 7 та 11 Закону України «Про захист персональних даних» та визначених законодавством принципів;

– ідентифікація особи отримувача (для отримання відповідної інформації треті особи повинні направити відповідний запит, у якому вказується мета та інформація відповідно до п. 4 ст. 16 Закону України «Про захист персональних даних». Разом з тим, виникає питання, чи дійсно особа є тим, за кого себе видає).

У разі порушення прав у сфері захисту персональних даних, суб'єкт має право звернутися до володільця чи розпорядника їх персональних даних, дії чи бездіяльність якого призвели до порушення його права на їх захист У разі незадоволення особою відповіддю на звернення, вона може звернутися до Уповноваженого з прав людини, який наразі є наглядовим органом у сфері захисту персональних даних, та суду. Для прикладу, до Уповноваженого з прав людини надійшло звернення за фактом незаконного поширення «чутливих» персональних даних психоневрологічним диспансером (ПД). Як зазначає заявник, під час розгляду судом справи за позовом до лікарні виникла необхідність отримання інформації про звернення заявника до ПД у період з 2010 до 2013 року та його діагнозу. На запит суду, з ПД надійшла відповідь, у якій було викладено інформацію про обстеження та діагноз заявника у 2014 році (період виходить за межі запиту). Що ж до інформації за запитуваний період, ПД повідомив, що у даний проміжок часу звернення заявника не надходили. За результатами проведеної перевірки Уповноваженим з прав людини прийнято рішення про незаконне поширення «чутливих» персональних даних щодо обстеження заявника ПД – ч. 4 ст. 188-39 Кодексу України про адміністративні правопорушення («недодержання встановленого законодавством про захист персональних даних порядку захисту персональних даних, що призвело до незаконного доступу до них та порушення прав заявника» [13]. Варто

звернути увагу на те, що у разі одночасного звернення суб'єкта і до Уповноваженого з прав людини, і до суду, Уповноважений припиняє розпочатий розгляд звернення.

Висновки. Таким чином, незважаючи на чіткі законодавчі норми щодо забезпечення захисту «чутливих» персональних даних, мають місце факти порушень у частині, що стосується: відсутності як мети, так і доцільності об'ємного збору даних; неврахування індивідуальних обставин осіб, чиї дані зберігаються; зміни визначеної мети обробки «чутливих даних», яка є несумісною з попередньою; відсутності підстави для подальшого зберігання та обробки інформації. Типовими порушеннями порядку збору, обробки та захисту інформації є неповідомлення особи про обробку «чутливих» персональних даних, транскордонна передача даних, порушення строків зберігання, неповідомлення суб'єкта про дії з персональними даними, ідентифікація особи отримувача. Найсерйозніші порушення законодавства виникають внаслідок неправомірної передачі персональних даних третім особам.

Право на захист персональних даних передбачає, що людина має право на захист своїх персональних даних від несанкціонованого доступу і використання третіми особами. Тобто як держава, так і організації, які є володільцями персональних даних, повинні вживати необхідні заходи щодо захисту даних та запобігання їх витоку. Адже забезпечення права людини на захист «чутливих» персональних даних – важливий показник як демократичності держави, так і інтеграції національного права у світове співтовариство.

Список літератури:

1. Про інформацію: Закон України від 02.10.1992 р. № 2657-XII. URL: https://zakon.rada.gov.ua/laws/show/2657-12#Text.

2. Декларація про політику у напрямі забезпечення прав пацієнта у Європі. Європейська нарада по правах пацієнта, Амстердам, Нідерланди, березень 1994 р. URL: https://med.sumdu.edu.ua/images/content/doctors/Deontology/ Patients_rights_WHO.pdf.

3. Загальний регламент Європейського Парламенту і Ради (ЄС) «Про захист фізичних осіб у зв'язку з опрацюванням персональних даних і про вільний рух таких даних, та про скасування Директиви 95/46/ЄС» від 27.04.2016 № 2016/679. URL: https://zakon.rada.gov.ua/laws/show/984_008-16#Text.

4. Юридична відповідальність за правопорушення в інформаційній сфері : навчальний посібник /О.О. Тихомиров, О.К. Тугарова. К.: Нац. акад. СБУ, 2015. 172 с.

5. Демченко І.С. Інформація про стан здоров'я у контексті права на повагу до приватного життя: міжнародно-правовий аспект. *Альманах міжнародного права*. Випуск 15. С. 41–50.

6. Медичне законодавство: правова регламентація лікарської діяльності: підручник / М.В. Банчук, В.Ф. Москаленко, Б.В. Михайличенко та ін. Київ: Медицина, 2012. Кн. 2. 494 с.

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

8. Справа «Z v. Finland». Judgement ECHR, applicationno. 22009/93. / Strasbourg, 25 February1997 http://hudoc.echr.coe.int/eng?i=001-58033.

9. Конвенція про захист осіб у зв'язку з автоматизованою обробкою персональних даних від 28.01.1981 р. /Рада Європи. *Офіційний вісник України* від 14.01.2011 № 58. Стаття 85.

10. Захист персональних даних у сфері охорони здоров'я в ЄС: законодавчий ландшафт. Аптека. 07.12.2020 № 47 (1268). URL: https://www.apteka.ua/article/575210.

11. Захист персональних даних у сфері охорони здоров'я. 2021. URL: http://medosvita.info/2021/05/09.

12. Січкар А. Обробка персональних даних в Україні: 5 найпоширеніших помилок. URL: https://jurliga.ligazakon.net/analitycs/222164_obrobka-personalnikh-danikh-v-ukran-5-nayposhirenshikh-pomilok.

13. Кодекс України про адміністративні правопорушення від 07.12.1984 № 8074-10 (із змінами). *Відомості Верховної Ради УРСР.* 1984. додаток до № 51. Ст. 1122. URL: https://zakon.rada.gov.ua/laws/show/80731-10.

Kobrusieva Ye.A. INFORMATION SECURITY OF "SENSITIVE DATA" AS A COMPONENT OF HUMAN RIGHTS PROTECTION: DOMESTIC AND INTERNATIONAL EXPERIENCE

The article analyzes the main norms of domestic and international legislation in relation to the right to protection of "sensitive" personal data. It is stated that despite clear legislative norms, there are facts of violations in relation to: the absence of both the purpose and the expediency of bulk data collection; failure to take into account the individual circumstances of the persons whose data are stored; changes in the specified purpose of processing "sensitive data" that is incompatible with the previous one; the absence of grounds for

further storage and processing of information. The general, special and basic norms of international law on the regulation of activities on the protection of "sensitive" information are studied. The case law of the European Court of Human Rights is considered in the context of the researched topic (the decisions of the ECHR in the cases: "M. S. v. Sweden", "Z v. Finland", "I. v. Finland", "Avilkina and Others v. Russia"). The main principles of processing "sensitive" personal data (lawfulness, fairness, legitimate purpose, accountability, necessity, proportionality, effective protection) are outlined. Typical violations of the procedure for collecting, processing and protecting information are identified: failure to notify a person about the processing of "sensitive" personal data; cross-border data transfer; violation of storage periods; failure to notify a subject about actions with personal data; identification of the recipient. It is argued that the most serious violations of the law arise precisely as a result of the unlawful transfer of personal data to third parties, which must be carried out on the grounds specified in Articles 7 and 11 of the Law of Ukraine "On the Protection of Personal Data" and comply with the specified principles. It is theoretically justified that ensuring the human right to the protection of «sensitive» personal data is an important indicator of both the democracy of the state and the integration of national law into the world community, respectively, both the state and organizations that are the owners of personal data must take the necessary measures to protect data and prevent its leakage.

Key words: *«sensitive» personal data, the right to protection, legal norms, information security, automated processing.*