УДК 347.13
DOI https://doi.org/10.51547/ppp.dp.ua/2023.3.23

Лепіш Наталія Ярославівна,
кандидат юридичних наук,
доцент кафедри адміністративно-правових дисциплін
Інституту права Львівського державного університету внутрішніх справ
ORCID ID: 0000-0002-5754-3511

ОРГАНІЗАЦІЙНО-ПРАВОВІ ПРОБЛЕМИ РЕАЛІЗАЦІЇ ПРАВА НА БЕЗПЕКУ ІНФОРМАЦІЇ ПРО ПРИВАТНЕ ЖИТТЯ ТА ПЕРСОНАЛЬНІ ДАНІ

ORGANIZATIONAL AND LEGAL PROBLEMS OF IMPLEMENTING THE RIGHT TO SECURITY OF PRIVATE LIFE AND PERSONAL DATA

У статті наведено роз'яснення актуальної наукової проблематики щодо теоретико-методологічного дослідження правового забезпечення інформаційної безпеки особи безпосередньо виводить на аналіз проблем забезпечення таємниці особистого життя, особистих даних, включаючи питання ефективного захисту персональних даних. Досліджується розвиток інформаційних технологій і систем які впливають на зростання загрози інформаційної безпеки в особистому та сімейному житті громадян, при захисті персональних даних, оскільки має місце формальність застосування правових норм сфері захисту персональних даних.

Аналізуються такі закони України «Про симулювання розвитку цифрової економіки» та «Про публічні електронні реєстри» які позитивно позначаються на правозастосовній практиці, ефективності правового регулювання суспільних відносин, пов'язаних з обробкою персональних даних, що здійснюється органами державної влади, місцевими органами державної влади, іншими державними органами, органами місцевого самоврядування, юридичними та фізичними особами з використанням засобів автоматизації або без використання таких засобів, якщо обробка персональних даних без використання таких засобів відповідає характеру дій, що здійснюються з персональними даними з використанням засобів автоматизації, регульованих нормами закону «Про захист персональних даних».

Під персональними даними розуміється інформація, що відноситься прямо чи опосередковано до визначеної фізичної особи (суб'єкта персональних даних). Під обробкою персональних даних розуміється дія (операція) або сукупність дій, що здійснюються з використанням засобів автоматизації або без використання таких засобів з персональними даними, включаючи збирання, запис, систематизацію, накопичення, зберігання, уточнення, вилучення, використання, передачу, знеособлення, блокування, видалення, знищення персональних даних.

Ключові слова: *безпека інформації, приватне життя, персональні дані, реалізація права.*

The article provides an explanation of the current scientific issues regarding the theoretical and methodological research of the legal provision of information security of a person, which directly leads to the analysis of the problems of ensuring the secrecy of personal life, personal data, including the issue of effective protection of personal data. The development of information technologies and systems that affect the growth of the threat of information security in the personal and family life of citizens, in the protection of personal data, is being studied, as there is a formality in the application of legal norms in the field of personal data protection.

The following laws of Ukraine "On simulating the development of the digital economy" and "On public electronic registers" are analyzed, which have a positive effect on law enforcement practice, the effectiveness of legal regulation of social relations related to the processing of personal data carried out by state authorities, local state authorities, other state authorities, local self-government bodies, legal entities and natural persons with or without the use of automation tools, if the processing of personal data without the use of such tools corresponds to the nature of actions carried out with personal data using automation tools regulated by the law "On Personal Data Protection".

Personal data refers to information directly or indirectly related to a specific natural person (subject of personal data). The processing of personal data means an action (operation) or a set of actions carried out with the use of automation tools or without the use of such tools with personal data, including collection, recording, systematization, accumulation, storage, clarification, extraction, use, transfer, depersonalization, blocking, deletion, destruction of personal data.

Key words: *information security, privacy, personal data, enforcement of rights.*

Законом визначено основні принципи обробки персональних даних [1; 2].

Слід зазначити, що ухваленню закону передувала ратифікація Україною Конвенції Ради Європи про захист фізичних осіб під час автоматизованого оброблення персональних даних. Пізніше були прийняті інші важливі міжнародні документи, у тому числі 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 96/46ЄС (Загальний регламент про захист даних) [3].

Положення Регламенту визначають персональну інформацію як дані, які потребують захисту на кожному етапі від збору до зберігання та розповсюдження. Право громадян на доступ до своїх даних і внесення змін до них стало головною складовою цих правил У різних законах і правилах по-різному визначаються умови захисту даних.

Прийнято вважати, що персональна інформація має бути: отримана чесним та законним шляхом; використана тільки для заздалегідь визначених цілей; відповідати задачі, заради якої вона збиралася; точної; оброблятися лише за згодою суб'єктів її отримання; доступна суб'єкту даних; захищена від несанкціонованого доступу; знищено після того, як мети досягнуто.

Безпека персональних даних при обробці в інформаційній системі забезпечує оператор системи, який обробляє персональні дані (далі – оператор), або особа, яка здійснює обробку персональних даних за дорученням оператора на підставі договору. Договір між оператором та уповноваженою особою повинен передбачати обов'язок уповноваженої особи забезпечити безпеку персональних даних при обробці в інформаційній системі, яка є системою, що обробляє спеціальні категорії персональних даних, якщо в ній обробляються персональні дані стосовно національної приналежності, політичних поглядів, релігійних чи філософських переконань, стану здоров'я, інтимного життя суб'єктів персональних даних.

Інформаційна система може обробляти біометричні персональні дані, відомості, що характеризують фізіологічні та біологічні особливості людини, на підставі яких можна встановити її особу та які використовуються оператором для встановлення особи суб'єкта персональних даних. На даний аспект вказують автори наукового дослідження «Theoretical bases of legal regulation of artificial intelligence systems for identification in the context of the activities of executive authorities» [4].

Система ідентифікаційних ознак людини неоднорідна. Доцільно побудувати ієрархічну систему, щоб ефективно використовувати сучасні біометричні технології та будувати систему забезпечення безпеки персональних даних. Законопроєкт від 2 червня 2021 року № 5628 «Про захист персональних даних» передбачає побудову відповідної системи [5].

Пов'язана із захистом персональних даних проблема створення системи ефективного електронного, зокрема міжвідомчого документообігу. У більшості випадків юридичні та фізичні особи звертаються до державних органів для реєстрації та підтвердження своїх прав, для захисту інтересів. Вчинення цих дій супроводжується певною кількістю документів, кінцевим результатом є документ. Щоб юридичні та фізичні особи погодилися спілкуватися через Інтернет з державою, мають бути впевнені, що всі права будуть документовані в електронному вигляді не менш надійно, ніж на папері.

Державні органи повинні бути впевнені в цілісності та автентичності поданих фізичними і юридичними особами електронних документів. Позначена проблематика в умовах глобального інформаційного суспільства ускладнюватиметься, у міру проникнення системи електронного документообігу у різні сфери життя інформаційної держави в цифровою економікою. Реалізація зазначеного питання передбачена у Національній економічній стратегії на період до 2030 року [6].

Автоматизація процесів обміну даними між окремими відомчими інформаційними системами, забезпечення доступу до них інших органів державної влади потребує створення інтеграційної інформаційно-технологічної та комунікаційної інфраструктури для обробки та маршрутизації міжвідомчих інформаційних потоків з урахуванням вимог з кібербезпеки безпеки.

Позитивно на системі електронного документообігу позначилося ухвалення закону «Про електронні довірчі послуги» [7]. Цей Закон розширює сферу використання та допустимі види електронного підпису.

По-справжньому ефективність електронного урядування може бути використана лише тоді, коли буде створено законодавчу основу для створення та використання електронних документів.

Під електронним документообігом розуміють систему ведення документації, коли масив створюваних електронних документів підтримується з допомогою інформаційно-комунікаційних технологій на комп'ютерах, об'єднаних у мережу, що дає можливість формування та ведення розподіленої бази даних.

Відповідно до закону «Про електронні документи та електронний документообіг» документована інформація – це зафіксована на матеріальному носії шляхом документування інформація з реквізитами, що дозволяють визначити інфор-

мацію або у встановлених законодавством випадках її матеріальний носій [8]. Електронний документ – це документована інформація, представлена в електронній формі, у вигляді, придатному для сприйняття людиною з використанням електронних обчислювальних машин, для передачі інформаційно-комунікаційними мережами або обробки в інформаційних системах.

Одним з обов'язкових і важливих реквізитів документа, що забезпечує юридичну силу документа, є власноручний підпис фізичної або посадової особи, яка склала документ, що відображає волю та згоду особи, яка підписала стосовно змісту документа. За реквізитом ідентифікується особа, що підписала документ, оцінюються повноваження.

У процесі розвитку електронного документообігу та технології електронного підпису актуалізуються питання захисту контенту, справжнього змісту документа, як наслідок – проблеми ідентифікації особи. Питання інформаційної безпеки особи у разі безпосередньо пов'язані з інформаційної безпекою електронного документообігу.

Реалізація програми «Електронний уряд» відбувається за двома напрямами, які технологічно досить схожі та засновані на криптографічних алгоритмах з відкритим ключем: ідентифікація та аутентифікація особи; забезпечення безпеки електронних трансакцій.

Створена з метою ефективності інфраструктури електронного уряду Єдиний державний демографічний реєстр та документи, що підтверджують громадянство України, посвідчують особу чи її спеціальний статус функціонально покликана сприяти підвищенню рівня довіри особи у процесі отримання державних послуг в електронному вигляді [9].

Питання правової регламентації правовідносин у сфері електронного документообігу одні із актуальних, потребують швидкого рішення.

Аналізуючи стосовно засобів масової інформації принцип недоторканності приватного життя, неприпустимість збору, зберігання, використання та розповсюдження інформації про приватне життя особи без її згоди, закріплений законом «Про інформацію», автори дослідження «Право на невтручання у приватне та сімейне життя: практика Європейського Суду з прав людини» наголошують, що тільки за наявності згоди особи можлива публікація відомостей про його особисте життя. Згода громадянина, який є неповнолітнім, визнаного судом недієздатним або обмеженого в дієздатності, може дати один із його батьків, опікун, піклувальник або законний представник.

На практиці вимога про обов'язкове отримання згоди на публікацію відомостей про приватне життя особи не завжди дотримується, особливо щодо популярних осіб.

Гарантоване Конституцією право на недоторканність приватного життя поширюється на ту сферу життя, яка відноситься до окремої особи, стосується тільки цієї особи та охоплює охорону таємниці всіх сторін особистого життя особи, оголошення яких особа з певних причин вважає небажаною [10].

Право на недоторканність приватного життя означає надану людині та гарантовану державою можливість контролювати інформацію про себе, перешкоджати розголошенню відомостей особистого, інтимного характеру.

Резолюцією № 428 (1970) Консультативної асамблеї Ради Європи «Щодо Декларації про засоби масової інформації та права людини» наголошується, що існує сфери, в якій здійснення права на свободу інформації та свободу вираження думки може суперечити правом на повагу особистого життя, гарантованим ст. 8 Конвенції про права людини. Не можна допускати, щоб здійснення першого права завдавало шкоди останньому праву [11].

Резолюція досить повно розкриває зміст права на повагу до особистого життя. Пояснюється, що представляє право вести своє життя на власний розсуд при мінімальному сторонньому втручанні. Це стосується особистого, сімейного та домашнього життя, фізичної та духовної недоторканності, честі та репутації, необхідності не допускати, щоб людину представляли у хибному світлі, не розкриття не мають відношення до справи та несприятливих факторів, несанкціонованої публікації приватних фотографій, захисту від шпигунства та невиправданих неприпустимих безтактних дій, захисту від неправильного використання матеріалів особистого листування, захисту від розкриття інформації, наданої чи отриманої індивідом у конфіденційному порядку.

Ті особи, які власними діями сприяли поширенню інформації безтактного характеру, оскарженій пізніше, не можуть посилатися на право на повагу до особистого життя.

Складнощі судової практики у справах охорони приватного життя громадянина при неправомірному поширенні такої інформації без згоди через відсутність балансу між публічними та приватними інтересами актуалізують проблему законодавчого врегулювання питання встановлення меж приватного життя особи.

Питання приватності у глобальному інформаційному суспільстві, балансу інтересів особи та держави, не нове, проте в умовах інформаційного простору підніматиметься регулярно.

Противники порушення приватності побоюються порушення прав людини, вторгнення у сферу особистої інформації, порушення етики, використання отриманої особистої інформації проти людини. віднесення відомостей до такої інформації з урахуванням державних, громадських чи інших громадських інтересів.

На думку В. А. Сокуренко В.А., Н. О. Хрякової, перед правом на приватність у сучасному діджиталізованому світі постає досить багато загроз та небезпек: незаконне поширення та заволодіння персональними даними, транскордонне переміщення, недостатнє нормативне врегулювання механізмів захисту від порушення, пошук балансу між втручанням держави у приватну інформацію та громадськими інтересами [12, с. 283].

За основу повинні бути прийняті критерії статусу особи (громадського, політичного), змістовна сторона інформації, яка розповсюджується, що становить основу суспільного та публічного інтересу.

Поняття інформації про приватне життя особи, на відміну від персональних даних, на нашу думку, більш широко характеризує особу, не спрямовану на ідентифікацію за допомогою фіксації на матеріальному носії, але має безпосереднє відношення до характеристики конкретної людини незалежно від суспільного чи професійного статусу: біографічні відомості, переконання, погляди, подробиці особистого життя тощо.

Уповноваженим органом захисту прав суб'єктів персональних даних, на який покладається забезпечення контролю та нагляду за відповідністю обробки персональних даних є Уповноважений Верховної Ради України з прав людини.

О.М. Бойко зазначає, що Українське законодавство не відповідає вимогам Конвенції щодо передбачення положень, що регулюють збирання, оброблення, використання та захист біометричних персональних даних, відповідно, відсутня вимога контролю та нагляду за цим процесом з боку Уповноваженого [13, с. 162].

Обробка біометричних персональних даних може здійснюватися лише за наявності згоди у письмовій формі суб'єкта персональних даних, за винятком випадків, передбачених чинним законодавством, яке передбачає винятки, пов'язані з реалізацією міжнародних договорів України про реадмісію, у зв'язку із здійсненням правосуддя та виконанням судових актів, у випадках, передбачених законодавством України про оборону, про безпеку, про протидію тероризму, про транспортну безпеку, про запобігання корупції, про оперативно-розшукову діяльність, щодо кримінально-виконавчого законодавства України, законодавства України про порядок виїзду з України та в'їзду в Україну.

На думку К. В. Дубаноса, нормативно-правова база, яка регулює використання баз біометричних даних в Україні, потребує оновлення в частині визначення основних термінів, закріплення процедури реєстрації біометричних даних і їх використання в кримінальному провадженні та експертній діяльності. Акцентовано увагу на необхідності прийняття Закону України «Про державну реєстрацію геномної інформації людини» [14, с. 219].

Відзначимо позитивний досвід створення Міністерства цифрової трансформації спеціальних Інтернет ресурсів, спрямованих на формування правової культури. Серед завдань створеного порталу допомогти дітям зрозуміти важливість конфіденційності особистого життя при використанні цифрових технологій, але також для молодих людей, які з легкістю та ентузіазмом використовують середовище Інтернету.

Подібні проекти доцільно розвивати, поширивши подібні та інші аудиторні групи – пенсіонерів, студентів та інших.

СПИСОК ЛІТЕРАТУРИ:

1. Про симулювання розвитку цифрової економіки : Закон України від 15.07.2021 р. № 1667-IX. URL: https://zakon.rada.gov.ua/laws/show/1667-20#Text

2. Про публічні електронні реєстри : Закон України від 18.11.2021 р. № 1907-IX. URL: https://zakon.rada.gov.ua/laws/show/1907-20#Text

3. 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/984008-16#Text

4. Kovaliv M., Yesimov S., Kravchuk S. Theoretical bases of legal regulation of artificial intelligence systems for identification in the context of the activities of executive authorities. *Соціально-правові студії.* 2020. Випуск 2 (8). С. 8–15.

5. Законопроєкт від 02.06.2021 року № 5628 «Про захист персональних даних». URL: http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=72160

6. Про затвердження Національної економічної стратегії на період до 2030 року: Постанова Кабінету Міністрів України від 03.03.2021 р. № 179. URL: https://zakon.rada.gov.ua/laws/show/179-2021-%D0%BF#n25

7. Про електронні довірчі послуги: Закон України від 01.06.2010 р. № 2155- VIII. URL. https://zakon.rada.gov.ua/laws/card/2155-19

8. Про електронні документи та електронний документообіг: Закон України від 22.05.2003 р. № 851-IV. URL: https://zakon.rada.gov.ua/laws/card/851-15

9. Про Єдиний державний демографічний реєстр та документи, що підтверджують громадянство України, посвідчують особу чи її спеціальний статус: Закон України від 20.11.2012 р. № 5492-VI. URL: https://zakon.rada.gov.ua/laws/card/5492-17

10. Конституція України : Закон України від 28.06.1996 р. № 254к/96-ВР. URL: https://zakon.rada.gov.ua/laws/show

11. Резолюція № 428 (1970) Консультативної асамблеї Ради Європи «Щодо Декларації про засоби масової інформації та права людини». URL: https://zakon.rada.gov.ua/laws/show/994_107#Text

12. Сокуренко В. А., Хрякова Н. О. Право на приватність у мережі Інтернет у контексті європейської системи захисту прав. *Юридичний науковий електронний журнал*. 2021. № 4. С. 280–284.

13. Бойко А. М. Захист біометричних персональних даних Уповноваженим Верховної Ради України з прав людини. *Юридичний науковий електронний журнал*. 2021. № 2. С. 169–163.

14. Дубонос К. В. Використання баз біометричних даних підрозділів експертної служби МВС України під час розслідування кримінальних правопорушень: дис. … д-ра філософії; спец. 081. Київ, 2021. 286 с.