ХМЕЛЬНИЦЬКА ОБЛАСНА РАДА
ХМЕЛЬНИЦЬКИЙ УНІВЕРСИТЕТ УПРАВЛІННЯ ТА ПРАВА
ІМЕНІ ЛЕОНІДА ЮЗЬКОВА

Кваліфікаційна наукова праця на правах рукопису

БЄЛОВА Юлія Дмитрівна

УДК 347.121.1:342.723

ДИСЕРТАЦІЯ

ЦИВІЛЬНІ ПРАВОВІДНОСИНИ ЩОДО ПЕРСОНАЛЬНИХ ДАНИХ

Спеціальність 081 Право
Галузь знань 08 Право

Подається на здобуття ступеня доктора філософії

Дисертація містить результати власних досліджень. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело _____ **Ю. Д. Бєлова**

Науковий керівник:
Чорна Ж. Л.
кандидат юридичних наук, доцент

Хмельницький – 2021

АНОТАЦІЯ

Бєлова Ю. Д. **Цивільні правовідносини щодо персональних даних.** – Кваліфікаційна наукова праця на правах рукопису.

Дисертація на здобуття наукового ступеня доктора філософії за спеціальністю 081 Право. – Хмельницький університет управління та права імені Леоніда Юзькова Хмельницької обласної ради, Хмельницький, 2021.

Дисертаційне дослідження присвячене аналізу особливостей цивільних правовідносин щодо персональних даних та вирішення комплексу теоретичних і практичних проблем, пов'язаних із цивільно-правовими аспектами статики та динаміки персональних даних; розроблення конкретних пропозицій та рекомендацій щодо удосконалення правового регулювання цивільних відносин, пов'язаних із персональними даними.

У вступі наголошено, що прискорення процесів інформатизації сучасної цивілізації постмодерну набуває надзвичайного характеру. Цифрові інновації змінюють якість життя суспільства та навіть впливають на черговий етап еволюції людини. Радикальні зміни призводять до формування нової якості «цифрової» особистості людини, що лише поглиблює різноманітні аспекти захисту її свободи, недоторканості та гідності. Зростає важливість охорони та захисту інформаційних потоків та сформованих ними баз даних.

У першому розділі зазначено, що персональні дані є нематеріальними благами, оскільки не належать до предметів матеріального світу, не мають матеріальної (фізичної) субстанції, не мають геометричних форм, розмірів, кольору тощо. Попри нематеріальну природу персональні дані можуть бути збережені на матеріальних носіях (у формі картотек персональних даних) або відображені в електронному вигляді (база персональних даних в електронній формі). При цьому персональні дані, будучи інформацією, водночас виступають об'єктом особистих немайнових прав (особистим немайновим

благом). Персональні дані як особисте немайнове благо характеризується немайновою природою, хоча, в силу сучасного рівня розвитку матеріальної та духовної культури, соціально-економічних відносин та інформаційного простору, об'єктивно можуть набувати майнової цінності. При цьому відомості про фізичну особу самі по собі залишаються немайновими благами, оскільки не створюються в процесі виробництва та не мають грошової оцінки. Майнова же цінність персональних даних може бути обумовлена особистістю індивіда (наприклад, загальновідомої особи) або створюватись в процесі їх обробки.

Попри невіддільність персональних даних як особистого немайнового блага, вони наділені відособленістю завдяки об'єкту відомостей (інформація про конкретну фізичну особу), кількісному та якісному змісту відомостей (склад персональних даних, що обробляються), зовнішній формі (електронній формі та/або формі картотек). Персональні дані належать до об'єктивованих нематеріальних благ, котрі виражені в доступній для сприйняття органами людських чуттів об'єктивній формі. Об'єктивованість вказує на зовнішній стосовно суб'єкта характер персональних даних. У свою чергу, об'єктивована форма персональних даних створює можливість їх використання у відриві від особи-носія (суб'єкта персональних даних), що свідчить про віддільність таких даних.

Персональні дані як особисте немайнове благо наділені такими ознаками: 1) відособленість; 2) об'єктивованість; 3) віддільність прав на персональні дані; 4) мають економічну цінність; 5) мають властивості товару; 6) здатність брати участь в економічному обороті. Зроблено висновок про те, що дефініція персональних даних в національному законодавстві в цілому відповідає європейським стандартам, закріпленим у вказаних міжнародних документах. При цьому визначення персональних даних у вітчизняному законі фактично запозичене з Директиви 95/46/ЄС. Визначення персональних даних структурно охоплює п'ять ознак: 1) відомості чи сукупність відомостей (включати 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.

Поняття «персональні дані» необхідно відмежовувати від суміжних йому понять: «інформація про особу», «відомості про особисте життя фізичної особи», «ознаки, що індивідуалізують фізичну особу». Усі ці поняття мають спільний обсяг, тобто, ті чи інші відомості можуть бути одночасно персональними даними та інформацією про особу, відомостями про особисте життя фізичної особи, ознаками, що індивідуалізують фізичну особу. Для розмежування цих понять за змістом слід використовувати факт обробки відповідних відомостей. Тобто, відомості набувають правового режиму персональних даних внаслідок того, що стають предметом обробки.

У другому розділі наголошено, що право на персональні дані належить до основоположних прав людини, прояв якого в цивільних правовідносинах обґрунтований теорією горизонтальної дії прав людини. Законодавство повинно забезпечувати пропорційність між правом на персональні дані та правом на свободу висловлювання думок та інформації, у тому числі, щодо обробки персональних даних для журналістських цілей та академічної, художньої та літературної свободи.

Право на персональні дані є цивільно-правовим за своєю природою, оскільки відносини, що виникають із приводу персональних даних, цілком відповідають ознакам, закріпленим в ч. 1 ст. 1 ЦК України.

У зв'язку із обробкою персональних даних необхідно розмежовувати правовий режим бази персональних даних як об'єкта права інтелектуальної власності та об'єкта захисту. Потрібно враховувати таке: по-перше, ні матеріальний носій бази персональних даних, ні її внутрішнє інформаційне наповнення не є об'єктом права інтелектуальної власності автора бази (творця, розробника); по-друге, ні визнання бази персональних даних об'єктом авторського права, ні встановлення щодо неї права особливого роду, не виключають застосування законодавства щодо охорони персональних даних та не можуть йому суперечити.

Право на персональні дані є самостійним особистим немайновим правом, що обумовлено специфікою персональних даних як об'єкта цивільних правовідносин. Так, персональні дані за своєю суттю є інформацією про фізичну особу, в тому числі – й про її особисті немайнові блага та ознаки, які її індивідуалізують.

Право на персональні дані – це особисте немайнове право, специфіка котрого полягає в його: об'єкті – персональні дані; меті – захист права на приватність та інших особистих немайнових прав у зв'язку з обробкою персональних даних; змісті – активні та пасивні правомочності, а також правомочність захисту, що можуть бути реалізовані як в абсолютних, так і відносних правовідносинах.

Зміст права на персональні дані станом на сьогодні потребує доповнення новими правомочностями. До таких правомочностей віднесено право на мобільність та право на забуття.

Зміст права на мобільність персональних даних включає в себе можливість суб'єкта персональних даних: отримати від володільця персональні дані у форматі, придатному для подальшого використання; передати такі

персональні дані іншому володільцю; вимагати від володільця безпосередньої передачі таких персональних даних іншому володільцю при технічній можливості. Право на мобільність слід розглядати як окреме право в системі прав суб'єкта персональних даних, відрізняється від права на доступ, права на забуття, та тісно пов'язане з правом на захист персональних даних.

Наступним є право на забуття, зміст котрого полягає у можливості суб'єкта персональних даних вимагати від володільця видалення даних, які його стосуються.

У третьому розділі зазначено, що згода суб'єкта персональних даних є проявом можливості вільно визначати свою поведінку в сфері особистого життя, яка спрямована уповноважити володільця персональних даних на їх подальшу обробку та забезпечує контроль суб'єкта персональних даних за їх обробкою.

Згода суб'єкта персональних даних має щонайменше три значення: 1) можливість фізичної особи діяти певним чином; 2) юридичний факт; 3) об'єктивована форма. Згода суб'єкта персональних даних має усі ознаки одностороннього правочину: є дією особи (добровільним волевиявленням фізичної особи), спрямованою на набуття, зміну або припинення цивільних прав та обов'язків (щодо надання дозволу на обробку її персональних даних).

Об'єктивована форма згоди суб'єкта персональних даних повинна давати змогу зробити висновок про надання згоди та може бути вчинена: в письмовій формі, як правило, у вигляді окремого документу (згода на обробку персональних даних) або як одна з умов договору; шляхом конклюдентних дій, тобто якщо поведінка суб'єкта засвідчує волю на обробку його персональних даних, зокрема, шляхом проставлення відмітки про надання дозволу на обробку своїх персональних даних під час реєстрації в інформаційно-телекомунікаційній системі суб'єкта електронної комерції.

Виділено та охарактеризовано умови дійсності згоди суб'єкта персональних даних: добровільність, поінформованість, конкретність,

однозначність. Вказані умови застосовуються у сукупності. Здійснено доктринальний аналіз умов дійсності згоди, наведених у Загальному регламенті про захист даних, та порядку її надання.

Наголошено, що право на персональні дані може бути захищено як в неюрисдикційній, так і юрисдикційній формах. Неюрисдикційна форма захисту прав суб'єкта персональних даних має низку особливостей: 1) пріоритетне значення використання самозахисту обумовлено інформаційною природою персональних даних; 2) на володільців, розпорядників та третіх осіб покладено обов'язок забезпечити захист персональних даних, навіть захист від випадкових втрати або знищення, від незаконної обробки, у тому числі незаконного знищення чи доступу до персональних даних; 3) суб'єкт персональних даних має право пред'явити вмотивовану вимогу до володільця, розпорядника щодо припинення порушення своїх прав. Юрисдикційна форма захисту персональних даних охоплює загальний (судовий) порядок захисту, оскільки юрисдикція судів поширюється на будь-який спір, що виникає з приводу персональних даних, та спеціальний (адміністративний) порядок захисту, котрий сьогодні забезпечується діяльністю Уповноваженого Верховної Ради України з прав людини.

За порушення права на персональні дані можуть застосовуватися заходи цивільно-правової відповідальності, такі як відшкодування майнової та моральної шкоди. Право на відшкодування шкоди надається суб'єкту персональних даних ст. 82 Загального регламенту про захист даних (ст. 23 Директиви 95/46/ЄС). Порядок застосування такої цивільно-правової санкції закріплено у главі 82 ЦК України.

Обґрунтовано необхідність при вирішенні справ щодо захисту прав на персональні дані виходити з презумпції спричинення позивачу моральної шкоди відповідачем, а також права відповідача спростувати таку презумпцію.

У висновках узагальнено розуміння правововової природи, поняття та види персональних даних. Розкрито європейські стандарти цивільно-правового

регулювання відносин щодо персональних даних. Виявлено особливості участі у відносинах щодо персональних даних осіб, які їх обробляють, а також підстави виникнення цивільних правовідносин щодо персональних даних. Визначено підстави, форми та способи захисту прав суб'єкта персональних даних.

Ключові слова: *персональні дані, право на персональні дані, немайнові блага, особисті немайнові права, суб'єкт права персональних даних, стандарти правового регулювання цивільних відносин щодо персональних даних, право на мобільність персональних даних, право на забуття, розпорядник, володілець, підстави виникнення цивільних правовідносин щодо персональних даних, обробка персональних даних, цивільно-правові способи захисту, способи захисту персональних даних.*

SUMMARY

Belova Yu. D. **Civil and Law Relationships on Personal Data.**

Qualifying scientific work on the rights of the manuscript.

Thesis for a Philosophy Doctor Degree in specialty 081 Law. Leonid Yuzkov Khmelnytskyi University of Management and Law of Khmelnytskyi Regional Rada, Khmelnytskyi, 2021.

The thesis is dedicated to analysis of peculiarities of Civil and Law Relationships on Personal Data, and to resolving of complex of theoretical and practical issues that are related to Civil and Law aspects of statics and dynamics of Personal Data. Development of specific suggests and recommendations on improvement of Law regulation of Civil and Law Relationships in the field of Personal Data are included into the subject of the thesis too.

There is emphasized in introduction, that acceleration of informatization processes acquires extraordinary features in current Postmodern Civilization. Digital innovation changes a quality of society life and, moreover, impacts on the following

stage of human evolution. Formation of new feature of «digital» human personality is caused by radical changes; and it only deepens various aspects of the protection of her freedom, inviolability and dignity. Significance of safety and protection of information flows and data bases that are formed by them is growing. The first section states that Personal Data are intangible assets as they are not a part of tangible world, do not have material (physical) substance, and do not have geometric shapes, sizes, colors, etc. Simultaneously with intangible nature, Personal Data can be saved on tangible media (as a Personal Data files) or displayed electronically (Personal Data Digital Base). At the same time, Personal Data are an object of Personal Intangible Rights (Personal Intangible Assets) as they are information. Personal Data as Personal Intangible Assets has intangible nature; however, they can objectively acquire property value according to current level of development of tangible and intangible culture, social and economic relationships and informational space. Herewith, information about an individual in itself remains an intangible asset as they are not created in the process of production and do not have money value. Tangible value can be caused by personality of a person (for instant, well-known person) or can be created at the processing of Personal Data.

Despite the inseparability of Personal Data as Personal Intangible Assets, they are characterized as isolated with the help of Data Object (information about a specific individual), quantitative and qualitative Data Content (composition of Personal Data which are in processing), and external form (electronic form and / or files). Personal Data are included into objective Intangible Assets that are expressed as an objective form accessible to the human senses. Objectivity shows an external – as for subject – character of Personal Data. In turn, the objectified form of Personal Data creates opportunity of its using separated from a person-holder (Personal Data Subject). The mentioned above indicates the separation of such data.

Personal Data as Personal Intangible Assets has such features: 1) separation; 2) objectivity; 3) separation of Personal Data Rights; 4) economic value; 5) have features of goods; 6) ability to be involved into economic turnover. There is

concluding that concept of «Personal Data» meets European standards declared in international legislation, in general. Herewith, concept of «Personal Data» in national legislation is involved from Directive 95/46 /EU. The composition of the concept of «Personal Data» consists of four signs. They are: 1) information or a set of information (including any information about a person); 2) Personal Data are related directly or indirectly to individual («about individual»); 3) a subject of Personal Data is a person regardless of his / her citizenship, permanent residence or other legal relationship with the state; an individual is identified (in a group of persons he / she is «distinguished» from other members of the group or can be specifically identified based on the circumstances of each case); 5) personal information acquires the legal regime of Personal Data with the beginning of Personal Data Processing. Personal Data Processing is any action or set of actions, such as collection, registration, accumulation, storage, adaptation, change, renewal, use and distribution (distribution, sale, transfer), depersonalization, destruction of Personal Data, including with the use of information (automated) systems.

The concept of «Personal Data» should be distinguished from related concepts such as «information about the person», «information about the personal life of an individual», «signs that individualize the individual». All of these concepts have mutual volume; this means that any information could be both Personal Data and information about the person, information about the personal life of an individual and signs that individualize the individual. It is necessary to use a fact of processing of appropriate information to distinguish these concepts by content. Thus, information becomes covered by Personal Data Legal Regime as a result of becoming of processing subject.

The second section emphasizes that Personal Data Right is one of the fundamental human rights. Reflection of Personal Data Right in Civil Relationship is grounded by theory of horizontal action of human rights. Legislation has to provide proportionality between Personal Data Right and freedom of expression and

information including personal Data Processing for journalistic goals and academic, artistic and literary freedom.

The nature of Personal Data Right is Civil and Law, as relationships arising on Personal Data are appropriate to signs that are fixed in p. 1 Art. 1 of Civil Code of Ukraine.

It is necessary to identify the Personal Data Base Legal Regime as an object of Intellectual Property Right and as an object of protection regarding to Personal Data Processing. There is a demand to take into account the following. On the one hand, both a physical Personal Data Base carrier and its internal informational content is not an object of Intellectual Property Right of author of the base (creator, developer). On the other hand, neither the recognition of a personal data base as an object of copyright, nor the establishment of a special kind of right to it, exclude the application of legislation on the protection of Personal Data and may not contradict it.

Personal Data Right is an independent Personal Non-property Right; this is caused by peculiarities of Personal Data as an object of Civil Relationship. Thus, Personal Data essentially is information about individual including her or his Personal Intangible Assets and signs which individualizing a person.

Personal Data Right is a Personal Intangible Right specific of which includes: the object is Personal Data; the aim is protection of protection of the Right to Privacy and other Personal Non-property Rights in connection with the processing of Personal Data; the content consists of active and passive competencies and competency of protection that can be applying both in absolute and relative legal relations.

Current essence of Personal Data Right needs adding of new competencies. These competencies include Mobility Right and Forgetting Right.

The essence of Mobility Personal Data Right covers such possibilities of Personal Data Subject as: to receive Personal Data from holder in a format suitable for further use; to transfer these Personal Data to other holder; to require from holder to transfer Personal Data to other holder directly where technical opportunity is.

Mobility Right has to be reviewed as a separate right in the system of rights of Personal Data Subject. There is different between Mobility Right and Forgetting Right, and Access Right, whereas Mobility Right is closely connected with Personal Data Protection Right.

The next one is Forgetting Right, the essence of which is possibility of Personal Data Subject to require from holder to delate data related with him / her.

The third section indicates that an agreement of Personal Data Subject is a display of possibility for free choice of own behavior in the field of private life. This possibility is ordered to authorize a holder of Personal Data to the following processing of its and provides a control Personal Data Subject for processing of Personal Data.

An agreement of Personal Data Subject has at least three contexts: 1) possibility of individual to act in the specific way; 2) legal fact; 3) objectified form. An agreement of Personal Data Subject has all features of unilateral transaction. These features are: an agreement of Personal Data Subject is action of a person (voluntary expression of will of individual); an agreement of Personal Data Subject is ordered to acquisition, modification or termination of Civil Rights and Obligations (on permission to Personal Data Processing).

Objectified form of agreement of Personal Data Subject has to provide opportunity to concluding about consent and could be expressed: in a writing form, as a rule, either as a separate document (agreement for Personal Data Processing) or as one of the terms of the contract; in the way of implicit actions where the behave of a person certifies a will for Personal Data Processing, particularly, in the way of marking about permission to Personal Data Processing during the registration in the information and telecommunication system of the e-commerce entity.

Terms of validity of consent of Personal Data Subject are separated and characterized. They are voluntary, knowledge, specificity, unambiguity. These terms are used as a complex. The doctrinal analysis of terms of the validity of the consent

and the procedure for its provision that are represented in General Regulation on Data Protection is carried out.

There is stressed on possibility of protection of Personal Data Right in both non-jurisdictional and jurisdictional forms. Non-jurisdictional form of protection of Personal Data Right has a number of features. They are: 1) priority significance of using of self-protection is caused by informational origin of Personal Data; 2) owners, holders, and the third persons are obligated to provide a protection of Personal Data including protection from accidental loss or destruction, illegal processing, and illegal destruction or illegal access to Personal Data; 3) Personal Data Subject is authorized to require to owner or holder to stop violating her or his rights.

Jurisdictional form of protection of Personal Data includes both general (court) procedure of protection as the jurisdiction of the courts extends to any dispute arising over Personal Data, and specific (administrative) procedure of protection which is protected by activities of Commissioner for Human Rights of the Verkhovna Rada of Ukraine

Such measures of Civil and Law liability as compensation for property and moral damage could be implemented for violation Personal Data Rights. Right for compensation of damage of Personal Data Subject is provided by Art. 82 of General Regulation on Data Protection (Art. 23 of Directive 95/46/EU). The order of implementation of this Civil Sanction is stated in the Chapter 82 of Civil Code of Ukraine.

Demand to implement the presumption of causing moral damage to the plaintiff by the defendant and the rights of defendant to refute such a presumption during the resolving cases on protection of Personal Data Right, are grounded.

The law nature, concept and types of Personal Data are found. European standards of Civil and Law Regulation of Personal Data Relationships are indicated. Peculiarities of participation of persons processing Personal Data in Personal Data Relationships are identified; the basis of arising of Civil and Law Relationships on Personal Data is identified too.

Grounds, forms and methods of protection of the Personal Data Subject Rights are determined.

Key words: *Personal Data, Personal Data Right, Intangible Assets, Personal Non-property Rights, Personal Data Right Subject, standards of legal regulation of civil relations regarding Personal Data, Personal Data Mobility Right, Forgetting Right, holder, owner, basis of arising of Civil Relationship on Personal Data, Personal Data Processing, Civil and Law ways of protection; ways of protection of Personal Data.*

СПИСОК ОПУБЛІКОВАНИХ ПРАЦЬ ЗА ТЕМОЮ ДИСЕРТАЦІЇ

в яких опубліковані основні наукові результати дисертації:

1. Бєлова Ю.Д. Право на мобільність як новий стандарт захисту персональних даних в ЕС. *Наукові записки Інституту законодавства Верховної Ради України*. 2017. № 2. С. 56-61.

2. Бєлова Ю.Д. Стандарти захисту права на персональні дані відповідно до Директиви 95/46/ЕС. *Часопис «Університетські наукові записки» Хмельницького університету управління та права*. 2017. № 3 (63). С. 130-139.

3. Бєлова Ю.Д. Умови дійсності згоди на обробку персональних даних. *Підприємництво, господарство і право*. 2017. № 11. С. 14-18.

4. Бєлова Ю.Д. Поняття та зміст прав суб'єкта персональних даних. *Науково-практичний журнал «Соціологія права»*. 2017. № 3-4. С. 13-21.

5. Бєлова Ю.Д. Підстави захисту прав суб'єкта персональних даних. *Jurnalul Juridic National: teorie si practica*. 2018. № 8. С. 74-78.

6. Бєлова Ю.Д. Система спеціальних цивільно-правових способів захисту права на персональні дані. *Юридичний журнал «Право України»*. 2019. Вип. 1. С. 314-327.

7. Белова Ю.Д. Защита прав субъекта персональных данных. *Visegrad Journal on Human Rights*. 2020. № 4. С. 24-39.

8. Бєлова Ю.Д. Згода та інші підстави виникнення цивільних правовідносин щодо персональних даних. *Юридичний вісник*. 2020. № 3. С. 348-355.

які засвідчують апробацію матеріалів дисертації:

9. Бєлова Ю.Д. *Цивільні правовідносини щодо персональних даних*: Монографія. Хмельницький: ФОП Мельник А.А., 2019. 192 с.

10. Бєлова Ю.Д. Право на мобільність персональних даних. *Інформаційні технології у судочинстві*: зб. матер. всеукр. наук.-практ. конф., яка проводиться в рамках тижня цивільного процесу . Одесса: Фенікс, 2017. С. 89-92.

11. Бєлова Ю.Д. Стандарти захисту права на персональні дані відповідно до Директиви 95/46/ЄС: теоретико-адаптаційні аспекти. *Теорія та практика адаптації законодавства України до законодавства ЄС*: матеріали міжнар. наук.-практ. столу. Єреван: Видавництво Eurasian Social Science Assjciation, 2017. С. 16-18.

12. Бєлова Ю.Д. Стандарти захисту права на персональні дані відповідно до практики ЄСПЛ. *Україна на шляху до Європи: реформа цивільного процесуального законодавства*: зб. наук. праць Матеріали Міжнар. наук.-практ. конф. Київ: ВД Дакор, 2017. С. 86-89.

13. Бєлова Ю.Д. Участь розпорядника у відносинах щодо персональних даних. *Актуальні проблеми юридичної науки:* зб. тез Міжнародної наукової конференції «Шістнадцяті осінні юридичні читання»: (у 2-х част). Частина перша. Хмельницький: Хмельницький університет управління та права, 2017. С. 101-102.

14. Бєлова Ю.Д. Право суб’єкта персональних даних на забуття. *Актуальні проблеми інтелектуального, інформаційного та ІТ права:* зб. матеріалів Другої Всеукраїнської науково-практичної конференції. Львів: Юрид. ф –т Львів. нац. ун –ту ім. І. Франка, 2017. С. 76- 79.

15. Бєлова Ю.Д. Сучасні підходи до розуміння категорії персональних даних. *Актуальні питання розвитку юридичної науки та практики:* матеріали Міжнародної науково-практичної конференції: в 2-х томах. Том 2. К.:, 2018. С. 15-16.

16. Бєлова Ю.Д. Сучасні підходи до класифікації персональних даних. *Проблеми цивільного права та процесу, присвячена світлій пам'яті Пушкіна О.А.:* матеріали науково-практичної конференції. Харків. 2018. С. 311-314.

17. Бєлова Ю.Д. Персональні дані як об'єкт спадкових правовідноси. *Правове регулювання суспільних відносин: актуальні проблеми та вимоги сьогодення:* матеріали Міжнародної науково-практичної конференції. Запоріжжя: Запорізька міська громадська організація «Істина». 2018. С. 25-28.

18. Бєлова Ю.Д. Порушення прав суб'єкта персональних даних як підстава їх захисту. *Актуальні проблеми юридичної науки:* зб. тез Міжнародної наукової конференції «Сімнадцяті осінні юридичні читання» : (у 2-х част). Частина друга. Хмельницький: Хмельницький університет управління та права, 2018. С. 8-11.

19. Бєлова Ю. Д. Правова природа персональних даних. *Конституційні цінності: правова природа та практика реалізації : збірник тез Міжнародної науково-практичної конференції «Конституційні цінності: правова природа та практика реалізації»* (м. Хмельницький, 17 травня 2019 року) [у 2-х част.]. Частина 1. Хмельницький : Хмельницький університет управління та права імені Леоніда Юзькова, 2019. С. 51-54.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

ВРУ – Верховна Рада України;

ГК України – Господарський кодекс України;

ЄС – Європейський Союз;

ЗУ – закон України;

КК України – Кримінальний кодекс України;

КМУ – Кабінет Міністрів України;

КУпАП – Кодекс України про адміністративні правопорушення;

КСУ – Конституційний Суд України

МК України – Митний кодекс України;

ПК України – Податковий кодекс України;

ЦК України – Цивільний кодекс України;

ЦПК України – Цивільно-процесуальний кодекс України;

GDPR – General Data Protection Regulation.

ВСТУП

Актуальність теми. Прискорення процесів інформатизації сучасної цивілізації постмодерну набуває надзвичайного характеру. Цифрові інновації змінюють якість життя суспільства та навіть впливають на черговий етап еволюції людини. Радикальні зміни призводять до формування нової якості «цифрової» особистості людини, що лише поглиблює різноманітні аспекти захисту її свободи, недоторканості та гідності. Зростає важливість охорони та захисту інформаційних потоків та сформованих ними баз даних. Масштаби їх збору і використання значно зросли. Нові технології та інформаційна глобалізація принесли з собою нові проблеми захисту персональних даних. Технології змінюють як економіку, так і соціальне життя. Незважаючи на різноманітні виклики та труднощі, ці процеси активно торкаються і суспільного життя в Україні.

Побудова демократичної соціальної правової держави, найвищою цінністю в якій є людина, її честь і гідність, недоторканність і безпека, як і підтримання ефективного функціонування державних інститутів перебувають у нерозривному зв’язку із необхідністю вдосконалення захисту суб'єктивних цивільних прав. Прогрес інформаційних технологій та активність у формуванні баз персональних даних надзвичайно загострили проблему захисту різноманітних прав і свобод людини. Без досконалого дослідження міжнародних стандартів щодо захисту персональних даних, базових принципів їх захисту, вивчення особливостей національних регулятивних підходів окремих держав, які мають розвинене законодавство і багаторічний досвід з питань захисту прав і свобод людини, у тому числі права на захист персональних даних, украй ускладнюється розуміння сучасних проблем національного правового регулювання відносин із захисту персональних даних.

Питання про нові інформаційні технології досі розглядалися переважно з точки зору розвитку комунікацій, електронної торгівлі й вільного обігу

інформації. Однак названі події призвели до появи занепокоєння щодо небезпеки для основних прав: свобод людини і громадянина, зокрема права на недоторканність приватного життя. Ще ніколи так гостро не стояло питання можливостей зберігання досьє на осіб для різних «потреб» і породжених цим ризиків порушення недоторканності приватного життя, з боку як публічних, так і приватних установ за допомогою комплексного використання новітніх технологій.

Особливої актуальності у цьому світлі, зазначене питання набуло у контексті прийнятого 27 квітня 2016 р. Регламенту (Євросоюз) 2016/679 Європейського Парламенту та Ради від 27 квітня 2016 р. про захист фізичних осіб стосовно обробки персональних даних та про вільне переміщення таких даних. Положення цього Регламенту спрямовані на гармонізацію захисту основних прав і свобод фізичних осіб, щодо діяльності з переробки і на забезпечення вільного потоку персональних даних між державами-членами ЄС. Відповідно виникла необхідність в подальшій фрагментації і уніфікації законодавства про захист персональних даних у всіх державах Євросоюзу. Регламент значно розширює вже існуючі права фізичної особи як суб'єкта персональних даних та вводить нові, серед яких посилення права доступу до персональних даних, право на мобільність персональних даних, право бути забутим, право знати про випадки незаконного доступу до персональних даних. Нові європейські стандарти захисту персональних даних порушують гостро актуальні питання, вирішенню яких присвячено це дисертаційне дослідження.

Сучасний розвиток інформаційних технологій зумовив набуття цінності такими інформаційними об'єктами, як персональні дані, не лише для їх суб'єктів, але й для інших учасників цивільних правовідносин. Відтак саме персональні дані дедалі частіше стають об'єктом протиправних посягань та, відповідно, потребують правового захисту. Надзвичайної актуальності набирає саме цивільно-правовий захист із урахуванням його привентивно-присікального та відновлювально-компенсаційного спрямування.

Проблемам особливостей правовідносин щодо персональних даних сьогодні присвячено значну кількість публіцистики. Водночас, у цивілістичних наукових дослідженнях це питання розкривається не достатньо. При цьому більшість науковців розглядає проблематику захисту персональних даних у контексті захисту особистих немайнових прав (В. Бобрик, О. Гуменюк, Н. Давидова, Л. Красицька, О. Кулініч, Р. Стефанчук, Н. Устименко, Л. Федюк та ін.) або інформаційних прав (О. Кохановська, А. Кодинець та ін.), і лише незначна кількість – у контексті саме права на персональні дані (О. Дмитренко, І. Романюк).

Наукові підходи до розв'язання проблем із цивільно-правовим захистом баз даних було здійснено у монографічній праці О. О. Хавронюка (2016 р.), де основну увагу акцентовано на визначенні механізмів захисту прав та інтересів, пов'язаних із використанням баз даних авторського права, та на основі права sui generis. Водночас проблеми, пов'язані з персональними даними, розглядалися автором лише в контексті порівняльного аналізу із базою даних авторського права.

Проблематиці захисту персональних даних присвячено праці іноземних вчених-юристів, серед яких Свіре П., Ґраеф І., Лундквіст Б., Слоот Б., Лінскей О. та інші.

Загалом питання комплексного дослідження персональних даних як об'єкту цивільних правовідносин є актуальним, що зумовлює доцільність їх розгляду на рівні дисертації доктора філософії.

Зв'язок роботи з науковими програмами, планами, темами. Дисертацію виконано відповідно до планів науково-дослідної роботи кафедри цивільного права та процесу Хмельницького університету управління та права на 2013–2017 роки «Удосконалення механізму правового регулювання особистих немайнових та майнових відносин у контексті приведення законодавства України до європейських стандартів» та на 2017–2023 роки «Актуальні питання правового регулювання особистих немайнових та майнових відносин у контексті приведення законодавства України до

європейських стандартів» (державний реєстраційний номер 0117U000105), що є складовою наукової теми Хмельницького університету управління та права «Управлінські та правові засади забезпечення сталого розвитку України як європейської держави» на 2017–2026 роки (державний реєстраційний номер 0117U000103).

Тему дисертації затверджено вченою радою Хмельницького університету управління та права імені Леоніда Юзькова 30 січня 2017 року (протокол № 10) та уточнено 23 жовтня 2019 року (протокол № 2).

Мета і задачі дослідження. *Мета* дисертаційного дослідження полягає в тому, щоб на основі досягнень юридичної науки, вдосконалення законодавства України та практики його застосування визначити загально-правові засади цивільних правовідносин щодо персональних даних та вирішити комплекс теоретичних і практичних проблем, пов'язаних із цивільно-правовими аспектами статики та динаміки правовідносин щодо персональних даних; розроблення конкретних пропозицій та рекомендацій щодо удосконалення правового регулювання цивільних відносин, пов'язаних із персональними даними.

Для досягнення поставленої мети передбачено вирішити такі *завдання:*

– з'ясувати правову природу персональних даних;

– сформулювати поняття персональних даних та охарактеризувати їх види;

– охарактеризувати суб'єкта персональних даних і проблеми його встановлення;

– розкрити європейські стандарти правового регулювання цивільних відносин щодо персональних даних;

– визначити поняття, правову природу та види прав суб'єкта персональних даних;

– виявити особливості участі у правовідносинах щодо персональних даних осіб, які їх обробляють;

– з’ясувати підстави виникнення цивільних правовідносин щодо персональних даних;

– визначити підстави, форми та способи захисту прав суб’єкта персональних даних;

– розробити конкретні пропозиції та рекомендації з удосконалення правового регулювання відносин, пов’язаних із персональними даними.

Об’єктом дослідження є цивільні правовідносини, пов’язані зі здійсненням та захистом персональних даних, та проблеми їх правового регулювання.

Предметом дослідження є цивільні правовідносини щодо персональних даних.

Методи дослідження. З урахуванням комплексного характеру досліджуваної проблематики для виконання поставлених завдань у дисертації були використані спеціальні та загальнонаукові методи дослідження, а саме: спостереження, теоретичного і практичного моделювання, формально-логічного узагальнення правових явищ. Використовувалися також традиційні методи: діалектичний метод пізнання суспільних, у тому числі правових явищ, формально-логічний, системно-структурний, порівняльно-правовий та історичний. Дисертаційне дослідження, а також використані у ньому наукові методи пізнання ґрунтуються на діалектичному сприйнятті правової дійсності. Достовірність результатів дослідження забезпечується методологічним плюралізмом. Зроблені висновки і пропозиції ґрунтуються на вимогах формальної логіки з урахуванням визначеності, несуперечності, послідовності та обґрунтованості у рамках понятійного апарату правової науки. За допомогою логіко-семантичного методу сформульовано та поглиблено понятійний апарат, використовуваний у дослідженні. *Історико-правовий метод* дозволив проаналізувати розвиток законодавства у частині, що стосується правового регулювання відносин, пов’язаних із персональними даними, у динаміці, виявити основні етапи та тенденції розвитку законодавства у цій частині

(*підрозділи 1.1, 3.1*). *Метод моделювання* та *метафізичний* метод дали можливість запропонувати нові конструкції статей, що стосуються правового регулювання відносин, пов'язаних із персональними даними (*підрозділи 1.2, 2.3*). *Діалектичний метод* пізнання було використано для визначення взаємозв'язків між особистими немайновими правами та правами, пов'язаними із персональними даними (*підрозділи 1.1, 2.1*). За допомогою *порівняльно-правового методу* було проаналізовано законодавство зарубіжних держав у частині, що стосується правового регулювання відносин, пов'язаних із персональними даними, визначено загальні тенденції розвитку відповідних положень, сформульовано пропозиції щодо удосконалення чинного законодавства України (*підрозділи 1.3, 2.2*).

Методи тлумачення законодавства та аналізу широко використано у другому та третьому розділах дисертації. Вибір та подальше використання зазначених методів має комбінований характер залежно від вирішення конкретних завдань дослідження.

Нормативно-правовою основою роботи стали положення Конституції України, Цивільний кодекс України, Закон України «Про захист персональних даних», та інші нормативно-правові акти України, а також нормативно-правові акти європейських країн та ЄС із питань, пов'язаних із персональними даними.

Емпіричну базу дисертаційного дослідження складають узагальнення практики застосування чинного законодавства України, практики ЄСПЧ, матеріали та публікації у вітчизняних та зарубіжних періодичних виданнях щодо цивільних правовідносин, пов'язаних із персональними даними.

Наукова новизна одержаних результатів полягає у тому, що дисертаційна робота є першим в Україні комплексним дослідженням персональних даних як об'єкта цивільних правовідносин. За результатами дослідження сформульовано та обґрунтовано низку наукових положень, що виносяться на захист, зокрема:

вперше:

1) визначено *поняття персональних даних* як відомостей або сукупності відомостей, що безпосередньо чи опосередковано стосуються фізичної особи, незалежно від її громадянства, постійного місця проживання чи іншого правового зв'язку з державою, яка 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 з використанням інформаційних (автоматизованих) систем;

2) доповнено перелік *ознак персональних даних* вказівкою на момент, з якого відомості про особу набувають правового режиму персональних даних. Такий момент пов'язаний із початком обробки персональних даних шляхом збирання, реєстрації, накопичення, зберігання, адаптування, зміни, поновлення, використання, поширення (розповсюдження, реалізація, передача), знеособлення, знищення персональних даних, у тому числі із використанням інформаційних (автоматизованих) систем;

3) запропоновано поділ цивільних правовідносин 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.

При цьому треті та четверті види відносин можуть мати як самостійний характер, так і бути додатковими щодо основних;

4) з'ясовано правову природу права на мобільність персональних даних шляхом встановлення співвідношення з іншими суб'єктивними цивільними правами, а також зміст та межі його здійснення. Зроблено висновок про те, що за змістом право на мобільність найбільш дотичне до права на доступ до своїх персональних даних;

5) обґрунтовано доцільність наділення суб'єкта персональних даних правом на забуття. Запропоновано критерії при встановлені балансу між колідуючими правами та правом на забуття;

6) запропоновано проект статті 302^1 Цивільного кодексу України, якою віднесено право фізичної особи на персональні дані до її особистих немайнових прав;

удосконалено:

7) позицію щодо суб'єкта персональних даних. Обґрунтовано доцільність поширення законодавства про захист персональних даних на відносини щодо обробки відомостей про померлу особу («посттанативні права»). Запропоновано доповнити Закон України «Про захист персональних даних» статтею 4^1;

8) поняття «згода суб'єкта персональних даних». Запропоновано згоду суб'єкта персональних даних розуміти як прояв можливості вільно визначати свою поведінку в сфері особистого життя, яка спрямована уповноважити володільця персональних даних на їх *подальшу обробку* та *забезпечує контроль суб'єкта персональних даних за їх обробкою;*

9) позицію щодо розуміння поняття «вмотивована вимога» для здійснення захисту прав на персональні дані. Запропоновано віднести до підстав для визнання вимоги вмотивованою такі обставини: 1) для зміни персональних даних – доведення того, що персональні дані суб'єкта (їх частина) є недостовірними; 2) для знищення персональних даних –

встановлення одного з таких фактів: а) закінчення строку зберігання даних, визначеного згодою суб'єкта персональних даних на обробку цих даних або законом; б) припинення правовідносин між суб'єктом персональних даних та володільцем чи розпорядником, якщо інше не передбачено законом; в) видання відповідного припису Уповноваженого або визначених ним посадових осіб секретаріату Уповноваженого; г) набрання законної сили рішенням суду щодо видалення або знищення персональних даних; д) зібрання персональних даних з порушенням вимог законодавства про захист персональних даних; 3) для заперечення проти обробки персональних даних – доведення незаконності обробки персональних даних суб'єкта (їх частини);

дістали подальшого розвитку:

10) вчення про суб'єкта персональних даних. Виокремлено ознаки володільця персональних даних: 1) власна правосуб'єктність; 2) можливість діяти самостійно чи разом з іншими суб'єктами; 3) можливість визначати мету та інші умови обробки персональних даних;

11) положення про європейські стандарти захисту права на персональні дані. Зроблено висновок про те, що Закон України «Про захист персональних даних» є по факту імплементацією стандартів Директиви 95/46/ЄС. Обґрунтовано необхідність приведення змісту Закону України «Про захист персональних даних» у відповідність до Загального регламенту про захист даних Європейського Парламенту та Ради, який застосовується з 25 травня 2018 р.;

12) позиція щодо правової природи договору між володільцем і розпорядником персональних даних. Обґрунтовано цивільно-правову природу такого договору, якщо його сторони не виступають суб'єктами владних повноважень;

13) теоретичні та нормативні позиції щодо підстав для обробки персональних даних. Зроблено висновок про те, що згода суб'єкта персональних даних відрізняється від інших підстав обробки персональних

даних тим, що інші підстави обробки обтяжені додатковою умовою – «тестом на необхідність»;

14) положення про форми захисту прав суб'єкта персональних даних. Виділено такі особливості форм захисту таких прав: 1) пріоритетне значення надається самозахисту; 2) на володільців, розпорядників та третіх осіб покладено обов'язок забезпечити захист персональних даних, зокрема нести ризик випадкових втрати або знищення, незаконної обробки персональних даних; 3) суб'єкт персональних даних вправі пред'явити вмотивовану вимогу до володільця, розпорядника з вимогою припинити порушення своїх прав;

15) вчення про способи захисту цивільних прав та інтересів. Зроблено висновок про те, що основними спеціальними способами захисту права на персональні дані є вимоги про: припинення обробки персональних даних, зміну персональних даних, знищення персональних даних. При цьому, такі вимоги можуть бути реалізовані як в юрисдикційній, так і неюрисдикційній формах.

Практичне значення одержаних результатів полягає у тому, що положення, висновки і пропозиції проведеного дослідження, викладені автором, можуть бути використані у:

– *науково-дослідній роботі* – як основа для подальшого поглибленого теоретичного вивчення персональних даних як об'єкта цивільних правовідносин;

– *правотворчості* – для вдосконалення чинного цивільного законодавства, яке регулює питання у сфері персональних даних як об'єкта цивільних правовідносин;

– *навчальному процесі* – під час викладання та підготовки навчально-методичних матеріалів з дисциплін «Цивільне право», «Право інтелектуальної власності» та ін.

Наукові концепції, висновки та пропозиції дисертаційної роботи використано при підготовці лекцій та навчально-методичних матеріалів у Хмельницькому університеті управління та права імені Леоніда Юзькова

(*Акт про реалізацію результатів наукових досліджень від 20 травня 2020 року – Додаток Б).*

Особистий внесок здобувача. Дисертаційна робота є самостійним дослідженням автора. Висновки, пропозиції та рекомендації, у тому числі й ті, що характеризують наукову новизну, одержані автором особисто.

Апробація результатів дослідження. Дисертація виконана й обговорена на кафедрі цивільного права та процесу Хмельницького університету управління та права імені Леоніда Юзькова. Окремі висновки та узагальнення дослідження висвітлювалися дисертантом на таких наукових заходах: Всеукраїнській науково-практичній конференції *«Інформаційні технології у судочинстві»* (2017 року, м. Одеса), Міжнародному науково-практичному круглому столі *«Теорія та практика адаптації законодавства України до законодавства ЄС»* (2017 року, м. Єреван), Міжнародній науково-практичній конференції *«Україна на шляху до Європи: реформа цивільного процесуального законодавства»* (2017 року, м. Київ), Міжнародній науково-практичній конференції *«Шістнадцяті осінні юридичні читання»* (2017 року, м. Хмельницький), Всеукраїнській науково-практичнійї конференції *«Актуальні проблеми інтелектуального, інформаційного та IT права»* (2017 року, м. Львів), Міжнародній науково-практичній конференції «Актуальні питання розвитку юридичної науки та практики» (2018 року, м. Харків), Науково-практичній конференції «Проблеми цивільного права та процесу, присвячена світлій пам'яті Пушкіна О.А» (2018 року, м. Харків), Науково-практичній конференції «*Запорізька міська громадська організація «Істина»* (2018, м. Запоріжжя); Міжнародній науково-практичній конференції «Сімнадцяті осінні юридичні читання» (2017 року, м. Хмельницький); Міжнародній науково-практичній конференції *«Конституційні цінності: правова природа та практика реалізації»* (17 травня 2019 року, м. Хмельницький).

Публікації. Основні положення та висновки дисертації знайшли своє відображення у 19 публікаціях, а саме: шість у наукових виданнях України, визначених фаховими з юридичних наук; дві у наукових періодичних виданнях інших держав; а також у десяти збірниках тез матеріалів науково-практичних конференцій та монографії, присвяченій темі дисертаційного дослідження.

Структура та обсяг роботи. Дисертаційна робота складається зі вступу, трьох розділів, які охоплюють девять підрозділів, висновків, списку використаних джерел та додатків. Повний обсяг дисертаційного дослідження становить 248 сторінки, із них 191 сторінок основного тексту. Список використаних джерел складає 233 найменування. Додатки викладено на 6 сторінках.

РОЗДІЛ 1
ЗАГАЛЬНО-ПРАВОВІ ЗАСАДИ ЦИВІЛЬНИХ ПРАВОВІДНОСИН ЩОДО ПЕРСОНАЛЬНИХ ДАНИХ

1.1 Правова природа, поняття та види персональних даних

Термін «персональні дані», попри своє закріплення на рівні цілої низки спеціальних законів, відсутній в ЦК України [1]. У зв'язку із цим постає питання про з'ясування правової природи персональних даних та їх місця серед об'єктів цивільних правовідносин. Насамперед зауважимо, що персональні дані можуть виступати об'єктом як приватних, так і публічних правовідносин, а інститут захисту персональних даних носить міжгалузевий характер. Тому необхідно обмежити предмет нашого дослідження тільки такими відносинами з приводу персональних даних, які засновані на юридичній рівності, вільному волевиявленні, майновій самостійності їх учасників (цивільними відносинами).

Виходячи із законодавчого закріплення терміну «персональні дані» як «інформації про фізичну особу» (ст. 11 Закону України «Про інформацію» [2]) та як «відомостей чи сукупності відомостей про фізичну особу» (ст. 2 Закону України «Про захист персональних даних» [3]) можемо сформулювати три твердження щодо правової природи персональних даних. Перше – персональні дані належать до нематеріальних благ як об'єктів цивільних відносин. Друге – персональні дані є різновидом інформації. Третє – персональні дані належать до особистих немайнових благ.

Поділ об'єктів цивільних прав на матеріальні та нематеріальні блага закладений в ст. 177 ЦК України [1]. При цьому слід погодитись із С. О. Сліпченком, який наголошує, що використання законодавцем прикметників «матеріальний» і «нематеріальний» вказує на характерні особливості об'єктів того чи іншого виду. Матеріальність вказує на те, що благо має фізичну субстанцію, належить до предметів матеріального світу, має

властивості форми, розміру, кольору, структури. Відповідно, нематеріальність вказує на те, що таке благо не має фізичної субстанції, не належить до предметів матеріального світу, не окреслюється властивостями форми, розміру, кольору, структури. При цьому очевидно, що матеріальні та нематеріальні блага утворюють собою дихотомію. Інакше кажучи, законодавець поділив усі об'єкти цивільного права на дві взаємовиключні групи. Вони можуть бути або матеріальними, або нематеріальними. В основу такої класифікації покладено природу того чи іншого блага [4, с. 93]. Отже, безсумнівним є те, що персональні дані є нематеріальними благами, а отже, не належать до предметів матеріального світу, не мають матеріальної (фізичної) субстанції, не мають геометричних форм, розмірів, кольору тощо. Одночасно з нематеріальною природою персональні дані можуть бути збережені на матеріальних носіях (у формі картотек персональних даних) або відображені в електронному вигляді (база персональних даних в електронній формі).

Очевидним також є розуміння персональних даних як різновиду інформації. У цьому контексті вважаємо за доцільне взяти за основу запропонований О. В. Кохановською поділ інформації як об'єкту цивільного права на такі її прояви: як особисте немайнове благо у комплексі благ, перерахованих у ст. 201 і Книзі 2 ЦК України; як результат творчої інтелектуальної діяльності, тобто, як об'єкт виключних прав, врегульованих у ст. 199 і Книзі 4 ЦК України; як 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 [5, с. 6]. Таким чином, можем констатувати, що персональні дані, будучи інформацією одночасно виступають об'єктом особистих немайнових прав (особистим немайновим благом). Саме це визначає особливості їх правового режиму як на рівні статики, насамперед, щодо змісту та меж прав суб'єкта персональних даних, так і на рівні динаміки, зокрема, при визначенні підстав для обробки персональних даних, способів та форм захисту

від їх порушення, що буде продемонстровано нами в другому та третьому розділах.

На розуміння персональних даних як особистих немайнових благ вказують і положення законодавства. Насамперед, згадана ст. 11 Закону України «Про інформацію» прирівнює їх до «інформації про *фізичну особу*». Більше того, 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 [6, с. 125]. Використовуючи запропонований в літературі підхід, відповідно до якого ознаки особистих немайнових благ слід розглядати в системі, що дозволяє визначити їх сутність та з'ясувати специфіку цивільно-правового режиму [7, с. 67-68], спробуємо розкрити поняття персональних даних. Для цього спочатку визначимо ознаки персональних даних, що характеризують їх як особисте немайнове благо та відмежовують від інших нематеріальних благ, а потім – ознаки, притаманні лише персональним даним.

У науці цивільного права виділяють дві ознаки особистих немайнових благ, що різнять їх від інших: «невіддільність від особи носія», під якою розуміють неможливість відокремлення даного блага від особи, яка ним наділена; та «немайновість», яка означає відсутність економічного змісту [8, с. 14–15]. Однак, екстраполяція цих ознак на персональні дані зустрічає певні складнощі. Так, легальне визначення поняття «обробки персональних даних» ставить під сумнів як їх невіддільність (внаслідок збирання, реєстрації, накопичення, зберігання, адаптування, зміни, поновлення, використання і поширення, знеособлення, знищення персональних даних), так і немайновість (обробка створює майнову варстість персональних даних, тому робота, пов'язана з обробкою персональних даних, а також робота з консультування та організації доступу до відповідних даних повинна бути оплачена). Це призводить до наукової дискусії щодо особистої немайнової природи

персональних даних. З цього приводу можна виділити дві альтернативні концепції: пропрієтарну концепцію персональних даних фізичної особи та концепцію виключних прав на персональні дані.

Пропрієтарна теорія персональних даних фізичної особи представлена переважно представниками західної правової традиції, зокрема, Л. Хантером, Д. Рул, А. Кавукян, Л. Лессігом, Р. Мерфі. Для забезпечення абсолютної можливості індивіда контролювати власні персональні дані прихильники цієї теорії пропонують регулювати правовідносини з їх обігу за допомогою інституту права власності [9, с. 195]. Так, на думку Р. Познера, інтерес, який стоїть за бажанням індивіда контролювати обіг інформації про себе, пов'язаний не стільки з особистою автономією і бажанням «бути залишеним на самоті», скільки з бажанням «маніпулювати світом» [10, с. 393]. Тому, на думку дослідника, держава не по винна захищати право громадян на «маніпулювання свідомістю» інших. Замість того їй слід віддати інформацію про особу під владу ринкових механізмів [10, с. 393]. На думку Д. Бріна, цей ринок вже функціонує належним чином. Люди за власним бажанням віддають свої персональні дані в обмін на певні блага, такі як доступ до веб-сайтів, товарів, послуг. Господарюючі суб'єкти, у свою чергу, зацікавлені у збереженні конфіденційності отриманих відомостей, оскільки за інших умов вони можуть втратити клієнтів [11, с. 508].

Концепція виключних прав на персональні дані визначає правовий режим обігу персональних даних фізичної особи через правовідносини особливого виду, які потребують не спеціального регулювання внаслідок їх нематеріальності, а оборотоздатності відповідного об'єкта права – sui generis. Зазначається, що нематеріальна природа персональних даних фізичної особи зближує її з природою результатів інтелектуальної, творчої діяльності. Це стосується також і майнового характеру прав, які випливають з обігу персональних даних фізичної особи і результатів інтелектуальної діяльності [9, с. 197].

Обидві вказані концепції, попри їх наукову цінність, наділені, на наш погляд, однією тією ж вадою – намагання схожим з економічної точки зору відносинам надати подібне правове регулювання, однак без урахування при цьому правової природи благ, з приводу яких такі відносини виникають. Насправді відповідь на питання про специфіку персональних даних як особистих немайнових прав криється в розумінні самих ознак немайновості та невіддільності.

Досліджуючи немайновість як ознаку персональних даних слід враховувати, що за сучасного рівня розвитку суспільства та економіки персональні дані стали цінним ресурсом для підприємницької діяльності. У різних державах діють безліч організацій, що займаються збиранням та наданням інформації для рекламної індустрії. Такі компанії пропонують цілі адресні списки споживачів, що розподілені за різними ринковими категоріями, такими як «мистецтво», «діти», «робота» тощо. Подібні адресні списки здаються в оренду, причому бази даних можуть бути отримані щотижня і слугувати основою для створення нових інформаційних продуктів. За деякими даними, ринок персональних даних досягає 3 млрд. доларів на рік [12, с. 234]. Економічна цінність використання імені, зображення та інших персональних даних особи обумовлена, по-перше, сучасним рівнем розвитку інформаційних технологій, які надають змогу миттєво зафіксувати відображення ознак особистості, зберігати таке відображення фактично необмежено в часі, відтворювати безліч разів та в різноманітних формах, а також поширювати на територію та між особами, обмеженими лише наявністю відповідних технічних пристроїв. По-друге, потреба комерційного використання персональних даних особи обумовлена масовим характером виробництва та споживання, при якому виробник зацікавлений у привертанні до своїх товарів, робіт та послуг уваги якнайбільшої кількості споживачів задля найширшого представлення на ринку. По-третє, каталізатором комерційного використання персоніфікованої інформації особи виступає небачений за все існування людства ступінь

глобалізації матеріальної та духовної культури, що має свої тенденції до посилення [13, с. 16-17].

Отже, в силу сучасного рівня розвитку матеріальної та духовної культури, соціально-економічних відносин та інформаційного простору персональні дані об’єктивно можуть набувати майнової цінності. Однак, на нашу думку, це не змінює їх немайнову природу. Пояснюється це тим, що відомості про фізичну особу самі по собі залишаються немайновими благами, оскільки не створюються в процесі виробництва та не мають грошової оцінки. А майнова цінність персональних даних може бути обумовлена або особистістю самої особи (наприклад, загальновідомої), або створюватись в процесі обробки персональних даних.

Наявність майнової цінності персональних даних свідчить, насамперед, про їх участь в цивільному обороті. Це, в свою чергу, зумовлює необхідність переосмислення й такої ознаки, як невіддільність. Методологічне підґрунтя оборотоздатності окремих об’єктів особистих немайнових прав була закладена ще М. М. Агарковим, який писав, що «не слід ототожнювати невіддільність від особи таких благ, як честь, авторство і так далі, з невід’ємністю від людини особистих прав. Особисті блага невід’ємні від особи людини, але про невід’ємність особистих прав говорити не доводиться» [14, с. 301–302]. Тобто, питання про відділення від особи носія особистих немайнових благ, що є об’єктами тих чи інших суб’єктивних прав, і питання про можливість відчуження самих цих прав – це два різні питання, пов’язані один з одним через міркування технічної зручності, але що не зумовлюють вирішення один одного [15, с. 640]. У вітчизняній науці характеристиці оборотоздатних об’єктів особистих немайнових правовідносин було присвячене комплексне дослідження С. О. Сліпченка [16, с. 147–294], обґрунтування якого цілком може бути застосовано до персональних даних.

Так, персональні дані як об’єкт цивільних прав наділені відособленістю завдяки об’єкту відомостей (інформація про конкретну фізичну особу),

кількісного та якісного змісту відомостей (склад персональних даних, які обробляються), зовнішній формі (електронній формі та/або у формі картотек). Персональні дані належать до об'єктивованих нематеріальних благ, що виражені в доступній для сприйняття органами людських чуттів об'єктивній формі. Об'єктивованість вказує на зовнішній стосовно суб'єкта характер персональних даних. У свою чергу, об'єктивована форма персональних даних створює можливість їх використання у відриві від особи-носія (суб'єкта персональних даних), що свідчить про віддільність таких даних. Персональні дані як об'єктивовані віддільні особисті немайнові блага можуть мати свою ціну, виражену в грошах. При цьому їх немайнова цінність не втрачається. Отже, персональні дані, маючи ознаки відособленості, об'єктивованості, віддільності та економічної цінності, мають властивості товару і здатні брати участь в економічному обороті.

Таким чином, ***персональні дані як особисте немайнове благо наділені такими ознаками:*** 1) відособлені; 2) об'єктивовані; 3) віддільні права на персональні дані; 4) мають економічну цінність; 5) наділені властивостями товару; 6) здатні брати участь в економічному обороті (наділені властивісттю споживчої вартості –властивість задовольняти певну людську потребу, тобто це – її корисність).

Встановивши правову природу персональних даних як інформаційних особистих немайнових благ, надалі з'ясуємо їх місце серед суміжних правових категорій. До таких категорій необхідно віднести: «інформацію про фізичну особу» (ст. 11 Закону України «Про інформацію») та «інформацію про особисте життя фізичної особи» (ст. 302 ЦК України). При цьому зауважимо, що рівень законодавчої техніки при закріплені відповідних категорій на рівні спеціальних законів міг би бути значно кращим, оскільки термінологія, що при цьому використовується, є дещо відмінною: «відомості, що дають можливість ідентифікувати фізичну особу» (Закон України «Про доступ до судових рішень» [17]); «відомості, що ідентифікують особу»(Закон України «Про

організацію формування та обігу кредитних історій» [18]);«відомості про особисте життя громадян» (Закон України «Про звернення громадян» [19]);«інформація про приватне життя громадянина» (Закон України «Про телебачення і радіомовлення» [20]) тощо. Очевидно, що кожен із цих термінів може бути цілком замінений на поняття «інформація про фізичну особу» та/або «інформація про особисте життя фізичної особи».

В науковій літературі співвідношення понять «персональні дані» та «інформація про особу» також розуміється по-різному. При цьому можна виділити принаймні два підходи. Відповідно до першого з них «персональні дані» та «інформація про особу» розглядаються як тотожні поняття. Певно, основним аргументом на користь такого підходу є нормативний, тобто використання в Законі України «Про інформацію» вислову «інформація про фізичну особу (персональні дані)», що тлумачиться як фактично встановлена тотожність понять «інформація про фізичну особу» та «персональні дані» [21, с. 108]. Інший аргумент є більш змістовий та полягає у сприйнятті твердження, відповідно до котрого вся інформація, здатна індивідуалізувати людину як біопсихосоціальну істоту, належить до її «персональних даних», що спричиняє визнання, що поняття «персональні дані» є практично тотожним поняттю «інформація про особу» [22, с. 86].

Представники другого підходу розуміють персональні дані вузько, розглядаючи їх особливим підвидом загального поняття «інформація про особу», вичерпний перелік яких наведено в Законі України «Про інформацію» [23, с. 902]. Наприклад, О. О. Серебряник визначає поняття інформації про фізичну особу як будь-яку інформацію (відомості та/або дані) про конкретну людину, що включає в себе її персональні дані, комунікаційні дані (метадані) та інформацію про приватне життя; розкриває расове або етнічне походження, політичні погляди, віросповідання чи філософські погляди, ставлення до конкретних подій або дій, членство у професійній спілці,

місцезнаходження людини, а також дані, щостосуються її здоров'я, інтимного життя, творчості, іміджу [24, с. 10].

Також як приклад вузького розуміння персональних даних приводять рішення Конституційного Суду України від 20.01.2012 р. № 2-рп/2012 [25]. У цьому рішенні Конституційний Суд України тлумачить поняття персональних даних як конфіденційну інформацію про фізичну особу: «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».

Як ще один аргумент на користь розмежування понять «персональні дані» та «інформація про особу» використовують включення до обсягу останнього недостовірної інформації. Зокрема, А. В. Кардаш вказує, що персональні дані є елементом інформації про особу у широкому розумінні, оскільки крім персональних даних фізична особа має право формувати про себе будь-яку інформацію – як достовірну, так і недостовірну. Тому співвідносити інформацію про фізичну особу лише з персональними даними є обмеженням права людини на самостійне формування інформації про себе, яка може складатися з будь-яких відомостей/даних. Зовнішній вигляд людини є певним

видом інформації про фізичну особу, але це не буде персональними даними [26, с. 90]. Вважаємо, що кожен із зазначених підходів має раціональне зерно, й, водночас, не позбавлений певних вад. Так, вузьке розуміння персональних даних може призвести до безпідставного обмеження захисту прав суб'єкта персональних даних, тоді як поширення правового режиму персональних даних на усю без виключення інформацію про особу може мати зворотній ефект. Вирішення цієї дилеми вбачаємо у визначенні співвідношення цих понять окремо за їх обсягом (коло відомостей, на котрі поширюється дане поняття) та змістом (сукупність існуючих ознак таких відомостей, відображених у понятті). За обсягом ці поняття є фактично тотожні, оскільки будь-яка інформація про особу може її ідентифікувати. У той же час, за змістом ці поняття потрібно розмежовувати. В якості розмежувальної ознаки пропонуємо використовувати факт обробки відповідних відомостей. Тобто, інформація про особу набуває правового режиму персональних даних внаслідок того, що стає предметом обробки.

При співвідношенні понять «персональні дані» та «інформація про особисте життя фізичної особи» також відсутня єдність поглядів, аналіз яких дозволяє виділити два підходи. Перший з них полягає в ототожненні персональних даних та інформації про особисте життя фізичної особи. Такий підхід продемонстрований у вже згадуваному рішенні Конституційного Суду України від 20.01.2012 р. № 2-рп/2012 [25].

Відповідно до другого підходу, поняття «персональні дані» є ширшим за поняття «інформація про особисте життя фізичної особи» та включає останнє. Методологічне підґрунтя такого підходу закладено ще Л. О. Красавчиковою, яка обґрунтовувала необхідність відокремлення «інформації про особу» від «інформації про особисте життя», вбачаючи відмінність між об'єктами правової охорони цих понять [27, с. 117]. У вітчизняній цивілістиці цей тезис знайшов додатковий розвиток у працях: О. А. Дмитренко, яка вважає, що поняття «персональні дані», тобто, будь-яка інформація, що стосується ідентифікованої

фізичної особи або фізичної особи, яку можна ідентифікувати, є родовим відносно поняття «інформація про особисте життя» [28, с. 6]; І. І. Романюк, де доведено, що при звуженому тлумаченні персональних даних, зокрема, як інформації, яка стосується особистого життя, значний масив інформації про особу може бути необґрунтовано позбавлений правової охорони. А якщо ні, то при поширенні терміну «інформація про особисте життя» на весь масив інформації, яка індивідуалізує особу, можна створити штучні правові перепони для руху інформації, обіг якої не лише доречний, а й необхідний для нормального перебігу низки суспільних відносин, передумовами яких є індивідуалізація фізичної особи [22, с. 87]. Загалом підтримуємо такий підхід, з уточненням того, що відомості про особисте життя фізичної особи набувають правового режиму персональних даних внаслідок того, що стають предметом обробки.

Також поняття «персональні дані» слід відмежувати від іншого суміжного поняття, а саме «засобів (ознак), що індивідуалізують фізичну особу». В науці під такими ознаками розуміють комплекс властивостей, притаманних конкретній фізичній особі, що підкреслюють її індивідуальність у цивільних правовідносинах та характеризують особливості її суспільного буття [29, с. 153]. ЦК України до ознак, що індивідуалізують фізичну особу, відносить ім’я фізичної особи, місце її проживання та акти цивільного стану. Очевидно, що відомості про вказані ознаки фізичної особи відповідно до законодавства є її персональними даними, тобто надають можливість конкретно ідентифікувати цю особу. Більше того, ст. 11 Закону України «Про інформацію» до персональних даних безпосередньо відносить дані про національність, освіту, сімейний стан фізичної особи, відомості про її релігійні переконання, адресу, дату та місце народження. Ознаки, що індивідуалізують фізичних осіб, прийнято поділяти на ознаки, котрі здійснюють, по-перше, поіменну персоніфікацію (формальна індивідуалізація), по-друге, соціальну

персоніфікацію (соціальна індивідуалізація) і, по-третє, правосуб'єктну персоніфікацію (правосуб'єктна індивідуалізація) [30, с. 241].

Таким чином, поняття «ознаки, що індивідуалізують фізичну особу», оскільки вони ідентифікують або здатні конкретно ідентифікувати фізичну особу, охоплюються поняттям «персональні дані», однак не вичерпують його.

Вищезазначене відмежування поняття «персональних даних» від суміжних йому понять: «інформація про особу», «відомості про особисте життя фізичної особи», «ознаки, що індивідуалізують фізичну особу», дозволило зробити висновки, наведені далі. *Усі ці поняття мають спільний обсяг*, тобто ті чи інші відомості можуть бути одночасно персональними даними та інформацію про особу, відомостями про особисте життя фізичної особи, ознаками, що індивідуалізують фізичну особу. Для *розмежування цих понять за змістом слід використовувати факт обробки відповідних відомостей.* Тобто, відомості набувають правового режиму персональних даних внаслідок того, що стають предметом обробки.

Поняття «персональні дані» отримало своє легальне визначення не тільки на рівні національного законодавства, але й міжнародних документів. Зокрема, Конвенція про захист осіб у зв'язку з автоматизованою обробкою персональних даних [31] визначає термін «персональні дані» як будь-яку інформацію, що стосується конкретно визначеної особи або особи, що може бути конкретно визначеною (ст. 2). Директива 95/46/ЄС Європейського Парламенту і Ради «Про захист фізичних осіб при обробці персональних даних і про вільне переміщення таких даних» [32] розуміє під персональними даними будь-яку інформацію, що стосується встановленої фізичної особи чи фізичної особи, яку можна встановити (ст. 2). Закони України «Про захист персональних даних»(ст. 2) [3] та «Про інформацію» (ст. 11) [2] дають таке їх визначення: «персональні дані – відомості чи сукупність відомостей про фізичну особу, яка ідентифікована або може бути конкретно ідентифікована».

Вказане визначення не позбавлене певних логічних вад. Наприклад, О. В. Кохановська вказує, що пояснення явища фактично здійснюється через саме це явище: персональні дані – це відомості; а відомості – це інформація. Отже, коло замикається, бо персональні дані – це інформація. У такому разі йдеться лише про коло виокремленої інформації, а саме про інформацію «про фізичну особу» [33, с. 30]. Тобто, вказана дефініція може бути критикована в силу своєї невизначеності та неконкретності. Однак, це навряд чи можна віднести до її недоліків. Справа в тому, що в такому визначенні закладений принцип широкого розуміння персональних даних, який би дозволяв: охопити усю інформацію про особу, яка може бути ідентифікована; уникати безпідставного обмеженого тлумачення поняття «персональні дані». Таким чином, можемо констатувати, що дефініція персональних даних в національному законодавстві в цілому відповідає європейським стандартам, закріпленим у вказаних міжнародних документах. Оскільки визначення персональних даних у вітчизняному законі фактично є запозиченням з Директиви 95/46/ЄС, в основу характеристики ознак персональних даних доцільно покласти рекомендації, розроблені робочою групою із захисту фізичних осіб у зв'язку із обробкою персональних даних (Робочої групи за статтею 29) [34].

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. Проаналізуємо їх окремо.

Словосполучення «відомості чи сукупність відомостей», не зважаючи на те, що наш законодавець не вжив у їх контексті займенник «будь-які», повинно тлумачитись широко та включати будь-яку інформацію про особу, а саме:

– будь-яку за характером: як об'єктивну інформацію, яка не залежить від волі суб'єкта персональних даних та інших осіб, так і суб'єктивну

інформацію, що відображає суб'єктивну точку зору, наприклад, оцінка, характеристика, рецензія;

– будь-яку за змістом: інформацію про інтимну сферу (тобто найбільш особистісних аспектів життя, інформацію про здоров'я, статеві відносини), інформацію про особистісну сферу (сімейні взаємини, поведінку особи у своєму приватному володінні, стосунки з друзями тощо), сферу громадської, господарської, професійної діяльність особи (повсякденна участь у суспільному житті та активність особи, що спрямована на привертання уваги громадськості), але не обмежується ними;

– попри те, що персональні дані мають бути точними, достовірними та оновлюватися в міру потреби, їх змістом охоплюються також і неточні, недостовірні, застарілі відомості;

– будь-яку за форматом: текстову, графічну (фотографічну), звукову (акустичну), відео-інформацію, в тому числі цифрову, але не обмежується ними;

– на будь-якому носії: паперовому, електронному, плівці, компактному оптичному диску, карті, магнітному диску, але не обмежується ними.

Закріплення другої ознаки в нашому законі також відступає від європейських зразків: замість дієслова «стосується», вжито прийменник «про». Семантичне значення вказаних слів дещо відрізняється. Так, «про» вказує на конкретну особу предмет або абстрактне поняття, що виступають об'єктом розмови, думки і т. ін. [35, с. 1141]. Тоді як «стосуватися» означає мати відношення до кого-, чого-небудь, бути пов'язаним із кимсь, чимсь [35, с. 1398]. Попри очевидну різницю, вважаємо, що тлумачення цієї ознаки також повинно бути широким та охоплювати як відомості, що безпосередньо стосуються фізичної особи (особова справа, медична картка, історія хвороби), так і ті, що стосуються фізичної особи лише опосередковано (реєстр речових прав на нерухоме майно, реєстр обтяжень рухомого майна). Для пояснення цієї ознаки запропоновано виділяти три її елементи: зміст, ціль або результат. Зміст

вказує на випадки, коли інформація надається про конкретну людину, незалежно від цілей володільця персональних даних або третіх осіб, або впливу цієї інформації на суб'єкта персональних даних. Тобто, коли відомості безпосередньо стосуються фізичної особи. Елемент «цілі» передбачає використання даних із урахуванням усіх обставин певної справи, для оцінки певного ставлення або впливу на стан чи поведінку людини. При відсутності двох попередніх елементів, можна вважати, що дані стосуються особи, коли їх використання може вплинути на права та інтереси певної особи з урахуванням усіх обставин певної ситуації. Слід зазначити, що потенційний результат не обов'язково повинен чинити великий вплив. Достатньо, щоб інші особи могли ставитися по-іншому до конкретної особи в результаті обробки таких даних. Ці три елементи (зміст, ціль, результат) повинні розглядатися як альтернативні (взаємовиключні) умови, а не в сукупності. Наслідком цього є те, що одна й та ж інформація може стосуватися різних осіб одночасно залежно від того, який елемент присутній у відношенні до кожної з осіб [36, с. 54].

Третя ознака вказує на суб'єкта персональних даних – фізичну особу, тобто людину, як учасника цивільних відносин. Тобто, право на захист персональних даних має кожна людина, незалежно від її громадянства, постійного місця проживання чи іншого правового зв'язку з державою. Натомість відомості про юридичну особу не охоплюються поняттям «персональні дані» і, відповідно, захист, передбачений законом, їм не надається. Щоправда, відомості про юридичну особу можуть стосуватися окремих фізичних осіб (засновників, учасників), і в цьому контексті вважатися персональними даними останніх. Варто також зауважити, що законодавство окремих країн, наприклад, Італії, Австрії, Люксембургу, може поширювати дію окремих положень про захист персональних даних, таких як забезпечення захисту персональних даних, на обробку відомостей про юридичну особу [34].

Четверта ознака встановлює вимогу щодо спроможності ідентифікації або конкретної ідентифікації фізичної особи. Загальне правило зводиться до того,

що фізична особа може бути «прямо» або «опосередковано» ідентифікована за допомогою одного чи більше факторів, притаманних фізичним, фізіологічним, розумовим, економічним, культурним чи соціальним аспектам її особистості. Загалом, фізична особа може вважатися «ідентифікованою», якщо в групі осіб вона «виділяється» з-поміж інших членів групи. Відповідно, фізична особа є такою, яка «може бути ідентифікована», якщо, незважаючи на те, що її ще не було ідентифіковано, це можливо зробити [36, с. 56]. Термін «конкретно» у цьому контексті вказує на те, що можливість фізичної особи бути ідентифікованою за допомогою тих чи інших засобів повинна визначатись, виходячи із обставин кожного окремого випадку.

Ідентифікувати особу можна в ряді випадків і за однією ознакою – за прізвищем, посадою, псевдонімом (коли йдеться про відомих письменників, політиків, державних діячів, вчених тощо), але, переважно, ідентифікація звичайної фізичної особи (пересічної) відбувається за певним достатнім комплексом ознак, що вказують на конкретну особу – це повне ім’я фізичної особи, домашня адреса, професія, вік тощо. Тобто при роз’єднанні цих даних може бути втрачена можливість точної ідентифікації особи, що і має бути бажаним результатом, судячи з визначення терміну [33, с. 31]. У науці виділяють об’єктивну та суб’єктивну можливості ідентифікації суб’єкта даних. У першому випадку ідентифікація проводиться виключно на основі уже наявної інформації, яка є предметом розгляду. Суб’єктивно можлива ідентифікація додатково передбачає аналіз й іншої інформації, одержання якої потребує «розумних зусиль», або до якої може одержати доступ особа, відповідальна за обробку даних. Враховуючи інтереси особи, у вітчизняному законодавстві варто було би надати перевагу суб’єктивно можливій ідентифікації, так як це забезпечить більш надійний ступінь захисту прав фізичної особи, особливо у стосунках із професійними організаціями, котрі можуть мати значні ресурси для пошуку і аналізу інформації [28, с. 60]. Ознака ідентифікації є ключовою в понятті «персональних даних»; саме вона є визначальною при поширенні на

відомості правового режиму персональних даних. Натомість, виокремлюють так зване знеособлення персональних даних, вилучення відомостей, які дають змогу прямо чи опосередковано ідентифікувати особу. Це, наприклад, може бути потрібно у тих випадках, коли законні цілі, відповідно до котрих дані збиралися або надалі оброблялися, відпали. При цьому слід пам'ятати, що для знеособлення персональних даних можливість прямо чи опосередковано ідентифікувати фізичну особу повинна встановлюватися в кожному окремому випадку.

Також О. А. Дмитренко обґрунтовує розширення переліку ознак персональних даних як об'єкта цивільного права тими властивостями, що притаманні їм як різновиду інформації, а саме: відокремлюваність, невідчужуваність, поширюваність, невичерпність, здатність до тиражування, екземплярність та нематеріальна природа [28, с. 10]. Загалом погоджуючись, що персональні дані наділені такими ознаками, зауважимо, що ці ознаки характеризують персональні дані з точки зору їх належності до родових понять, а саме нематеріального блага, інформації, особистого немайнового блага. Тобто, притаманні усім поняттям відповідного роду. Вважаємо, що перелік ознак персональних даних слід доповнити ще вказівкою на момент, з якого відомості про особу набувають правового режиму персональних даних. Такий момент пов'язаний 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, із використанням інформаційних (автоматизованих) систем.

Проведений аналіз свідчить, що персональні дані є загальним поняттям, яке можна і навіть необхідно поділити на види. В науковій літературі дослідниками запропоновано різноманітні варіанти класифікації персональних даних:

1) за ступенем пов’язаності з особою персональні дані поділяють на постійні (колір очей) та змінювані (адреса проживання, місце роботи) [37, с. 153-162];

2) за співвідношенням із метою використання – на повні, неповні та надмірні (виходячи з тлумачення ст. 6 Закону «Про захист персональних даних»);

3) залежно від того, якими органами чуття сприймаються персональні дані – на звукові і зорові (включаючи символьні (зокрема текст) та образні (зокрема фото)); ті, що сприймаються безпосередньо органами чуття (містяться в документах, портретах), і ті, для обробки яких потрібна спеціальна апаратура (зчитувач скану сітківки ока, комп’ютер тощо) [28, с. 28];

4) за особливостями правового регулювання: загальні персональні дані – прізвище, ім’я та по батькові, дата народження, а також 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; 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 дані, що стосуються здоров’я чи статевого життя; спеціальні персональні дані – персональні дані, що не входять до вразливих чи загальних персональних даних, межі обігу яких визначаються суб’єктом цих даних [38, с. 94].

Персональні дані можуть класифікуватися й за іншими критеріями: за предметом (біографічні, фінансові, біометричні тощо), ступенем потенційної шкідливості неконтрольованого обігу (звичайні, вразливі), здатністю до ідентифікації (прямо та опосередковано ідентифікуючі), формою фіксації (символи, образи, сигнали), співвідносністю з метою використання (повні, неповні, надмірні), адекватністю відображення дійсності (достовірні, недостовірні), способом сприйняття людиною (безпосередньо або за

допомогою технічних засобів) тощо [28, с. 9]. Враховуючи закріплений підхід щодо широкого розуміння персональних даних, перелік таких класифікаційних критеріїв може бути продовжений. Більше того, кожна із таких класифікацій може мати наукове та (або) практичне значення. У контексті нашого дослідження доцільно персональні дані ділити на види таким чином, щоб відображати відмінності в їх правовому режимі.

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 персональні дані»), є вичерпним та не підлягає розширеному тлумаченню. Значення виокремлення чутливих персональних даних полягає в тому, що законодавство встановлює особливі вимоги до обробки таких даних. Однак, чутливі персональні дані, які були явно оприлюднені суб'єктом таких даних, обробляються на загальних підставах.

Персональні дані також можуть бути поділені на ті, що належать, та ті, що не належать до інформації з обмеженим доступом. Режим конфіденційної інформації може бути поширений на персональні дані законом або відповідною особою. За загальним правилом, конфіденційною є інформація про фізичну особу, а також інформація, доступ до якої обмежено фізичною. При цьому, окремі науковці обґрунтовують необхідність віднесення усіх персональних даних до інформації з обмеженим доступом і спростовують можливість надання персональним даним режиму загальнодоступної (відкритої) інформації за певних умов [28, с. 10]. Однак, на сьогодні така позиція не узгоджується із чинним законодавством, що передбачає низку випадків, коли забороняється вважати персональні дані інформацією з обмеженим доступом:

1) персональні дані, що стосуються здійснення особою, яка займає посаду, пов'язану з виконанням функцій держави або органів місцевого самоврядування, посадових або службових повноважень;

2) персональні дані, зазначені у декларації про майно, доходи, витрати і зобов'язання фінансового характеру, крім відомостей, визначених законом;

3) персональні дані фізичної особи, яка отримала у будь-якій формі бюджетні кошти, державне чи комунальне майно, щодо факту такого отримання;

4) інші випадки, передбачені законом.

За правовим режимом також слід окремо виділяти персональні дані, які містяться в публічній інформації. Такі персональні дані можуть надаватися у формі відкритих даних за умови: 1) знеособлення персональних даних; 2) згоди суб'єкта персональних даних; 2) заборони віднесення таких персональних даних до інформації з обмеженим доступом; 4) в інших випадках, передбачених законом (ч. 3 ст. 10^1 Закону України «Про доступ до публічної інформації» [39]). Таким чином, правовий режим персональних даних відрізняється залежно від того, чи належать вони до чутливих даних, даних з обмеженим доступом чи даних, що містяться в публічній інформації. В усіх цих випадках за суб'єктом персональних даних зберігається можливість з власної волі оприлюднити чи іншим чином надати доступ до своїх персональних даних.

Характеристика поняття «персональні дані» як об'єкта цивільних відносин буде неповною без дослідження похідного від нього поняття – «база персональних даних». Під останньою розуміють іменовану сукупність упорядкованих персональних даних в електронній формі та/або у формі картотек персональних даних (ст. 2 Закону України «Про захист персональних даних» [3]). Із цієї дефініції можемо констатувати висновок, що база персональних даних є нічим іншим, як систематизованою сукупністю відомостей, тобто, власне, є самостійним збірним інформаційним об'єктом з усіма наслідками, що з цього випливають. Термін «іменована сукупність»

доктринально тлумачиться як вказівка на таку сукупність персональних даних, яку можна виокремити, і її можна конкретно назвати (іменувати) [33, с. 30]. Упорядкування персональних даних може відбуватись за різними критеріями, але необхідно розуміти, що зміна такого упорядкування (наприклад, зміна цілей) приводить до виникнення нової бази персональних даних. Правова охорона бази персональних даних виникає з моменту її створення, тобто надання їй об'єктивної форми. Виникнення об'єктивної форми бази персональних даних здійснюється при її фіксації на певному матеріальному носії і тому вважається закріпленою [24, с. 55]. Залежно від такого носія може бути база персональних даних в електронній формі або база персональних даних у формі кортотек. При цьому, одна і та сама база персональних даних може мати одночасно обидві форми (наприклад, дублювання електронної форми на паперовому носії).

Базу персональних даних як об'єкт захисту персональних даних необхідно відмежовувати від бази даних як об'єкта авторського права. Під базою даних (компіляцією даних) розуміють сукупність творів, даних або будь-якої іншої незалежної інформації у довільній формі, в тому числі – електронній, підбір і розташування складових частин якої та її упорядкування є результатом творчої праці, і складові частини якої є доступними індивідуально та можуть бути знайдені за допомогою спеціальної пошукової системи на основі електронних засобів (комп'ютера) чи інших засобів (ст. 1 Закону України «Про авторське право і суміжні права» [40]). Аналіз двох понять – «база персональних даних» і «база даних» – дозволяє прийти до висновку, що законодавець не виключає випадки, коли база персональних даних буде одночасно відповідати умовам охороноздатності бази даних як об'єкта авторського права.

Цей тезис знаходить своє додаткове підтвердження в Директиві 96/9/ЄС Європейського Парламенту та Ради «Про правовий захист баз даних» від 11 березня 1996 року [41]. Мета цієї Директиви – надання належного і

рівномірного рівня захисту баз даних як способу забезпечення винагороди розробнику бази даних – відрізняється від мети Директиви 95/46/ЄС Європейського Парламенту і Ради від 24 жовтня 1995 року про захист фізичних осіб при обробці персональних даних і про вільне переміщення таких даних, котра має гарантувати вільний обіг персональних даних відповідно до гармонізованих правил, призначених захистити ключові права і, насамперед, право на повагу до приватного життя, враховуючи, що положення цієї Директиви не завдають шкоди законодавству про захист даних. Тобто, одна і та ж база персональних даних може підпадати під захист персональних даних та захист права авторства.

Вище вказане дозволяє визначити персональні дані як 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.

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.

При цьому ознака ідентифікованості персональних даних є визначальною при поширенні на відомості правового режиму персональних даних.

Враховуючи з'ясовану нами правову природу та ознаки персональних даних, можемо визначити види цивільних правовідносин, які можуть виникати щодо персональних даних:

1) абсолютні правовідносини між суб'єктом персональних даних (управомочена особа) та усіма іншими особами (зобов'язані не порушувати права суб'єкта персональних даних) з приводу охорони персональних даних;

2) абсолютні правовідносини 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 правовідносини між суб'єктом персональних даних з одного боку і володільцем, розпорядником персональних даних та третіми особами – з іншого боку, що виникають з приводу обробки персональних даних. Такі відносини щодо обробки персональних даних можуть мати як самостійний характер, так і бути додатковими по відношенню до основних;

4) відносні правовідносини володільця, розпорядника персональних даних та третіх осіб між собою, що виникають з приводу обробки персональних даних. Такі відносини, так само як і попередні, можуть мати як самостійний характер, так і бути додатковими по відношенню до основних.

1.2 Суб’єкт персональних даних

Ключовим суб’єктом цивільних відносин, що виникають з приводу персональних даних, є їх суб’єкт. Легальне визначення поняття «суб’єкт персональних даних» дано в ч. 1 ст. 2 Закону України «Про захист персональних даних» [3], відповідно до якої під суб’єктом персональних даних розуміється фізична особа, персональні дані якої обробляються. Аналіз цієї дефініції дає підстави виділити дві ознаки: суб’єктивну та об’єктивну. Суб’єктивна ознака вказує на те, що суб’єктом персональних може бути лише фізична особа, тобто, людина як учасник цивільних відносин. При цьому поняття «фізична особа» охоплює громадян України, іноземців та осіб без громадянства, що перебувають в Україні на законних підставах. Останні користуються тими самими правами суб’єкта персональних даних, що і громадяни України, за винятками, встановленими Конституцією, законами чи міжнародними договорами України. Об’єктивна ознака передбачає, що суб’єктом персональних даних визнається лише та фізична особа, персональні дані якої обробляються, тобто, щодо яких здійснюється 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. Отже, фізична особа отримує статус суб’єкта персональних даних при здійсненні процедури її ідентифікації, тому будь-яка фізична особа не може автоматично розглядатися як суб’єкт правовідносин щодо персональних даних [42, с. 72].

Важливо також дати родову та видову характеристику суб’єкта персональних даних та визначити його місце серед учасників цивільних відносин, що виникають з приводу персональних даних. Оскільки персональні дані є за своєю суттю інформацією, а їх обробка належить до основних видів інформаційної діяльності, то однозначним є твердження, що відносини з

приводу персональних даних є інформаційними. Це означає, що вони повинні відповідати основним принципам інформаційних відносин, а саме: гарантованості права на інформацію; відкритості, доступності інформації, свободи обміну інформацією; достовірності і повноті інформації; свободі вираження поглядів і переконань; правомірності одержання, використання, поширення, зберігання та захисту інформації; захищеності особи від втручання в її особисте та сімейне життя (ст. 2 Закону України «Про інформацію» [2]). Більше того, персональні дані належать до такого виду інформації, як інформація про особу, а тому до відносин, які виникають з приводу персональних даних застосовуються загальні правила відносин, об'єктом яких виступає інформація про особу (ч. 2 ст. 11 Закону України «Про інформацію» [2]). З поміж інших учасників відносин з приводу персональних даних їх суб'єкт вирізняється, щонайменше, двома ознаками. По-перше, саме відомості про нього виступають об'єктом вказаних правовідносин, а тому суб'єкт персональних даних є обов'язковим учасником таких відносин, без якого вони не можуть відбутися. По-друге, суб'єкт персональних даних наділений особистими немайновими правами на персональні дані, а тому виступає у вказаних правовідносинах управомоченою особою, правам якої кореспондують обов'язки інших учасників.

Суб'єкт персональних даних, як і будь-який суб'єкт цивільних відносин, повинен бути наділений правосуб'єктністю, тобто правоздатністю та відповідним обсягом дієздатності. З цього приводу запропоновано виділяти: інформаційну правоздатність фізичної особи щодо інформації про себе – здатність особи мати цивільні права й обов'язки у сфері інформації, формувати, поширювати та захищати інформацію про себе [42, с. 67]; інформаційну дієздатність фізичної особи щодо інформації про себе – це можливість повнолітньої особи власними діями набувати права та нести обов'язки відносно відомостей/даних про себе [42, с. 68]. Оскільки інше не встановлено законом, правоздатність та дієздатність суб'єкта персональних даних визначається

загальними положеннями ЦК України про правоздатність та дієздатність фізичної особи. Отже, здатність фізичної особи бути суб'єктом персональних даних виникає з моменту народження, що підтверджується ч. 1 ст. 8 Закону України «Про захист персональних даних» [3], котра вказує, що особисті немайнові права на персональні дані, які має кожна фізична особа. Новонароджена особа ідентифікується через персональні дані матері, які містяться в обмінній картці вагітної. Натомість факт народження дитини змінює персональні дані матері, зокрема відомості про склад сім'ї та про стан здоров'я [43, с. 73]. У подальшому народження дитини як акт цивільного стану підлягає державній реєстрації з одночасним визначенням її походження та присвоєнням їй прізвища, власного імені та по батькові (ч. 1 ст. 13 Закону України «Про державну реєстрацію актів цивільного стану» [44]). Таким чином, вже з моменту народження фізична особа набуває певний обсяг персональних даних та наділяється правами суб'єкта персональних даних.

Здатність фізичної особи своїми діями набувати для себе особистих немайнових прав суб'єкта персональних даних і самостійно їх здійснювати, як і дієздатність загалом, залежить від віку та психічного стану здоров'я. На жаль, Закон України «Про захист персональних даних» не містить жодної норми, яка б встановлювала особливості захисту персональних даних неповнолітніх та малолітніх осіб. Як випливає зі змісту ст. 31 ЦК України, малолітні особи не можуть самостійно здійснювати права суб'єкта персональних даних [1]. Постає питання про те, чи можуть неповнолітні особи самостійно здійснювати особисті немайнові права суб'єкта персональних даних, якщо так, то в яких межах. При відповіді на це питання необхідно враховувати, що може мати місце два випадки: коли обробка персональних даних неповнолітніх осіб здійснюється у зв'язку із правовідносинами, що охоплюються обсягом їх дієздатності; коли обробка персональних даних неповнолітніх осіб здійснюється у зв'язку із правовідносинами, що знаходяться за межами обсягу їх дієздатності. У першому випадку неповнолітня особа може самостійно здійснювати права

суб'єкта персональних даних; у другому – ці права здійснюються за згодою батьків (усиновлювачів) або піклувальників.

З цього приводу ми підтримуємо твердження про необхідність правового закріплення юридичної відповідальності за порушення правил використання персональних даних неповнолітніх осіб, так як їхній правовий статус залишився поза увагою науковців та практики законотворення [45, с. 70]. Пояснюється це тим, що діти потребують особливого захисту своїх персональних даних, оскільки вони у меншій мірі усвідомлюють ризики, наслідки, відповідні гарантії і права при обробці персональних даних. Вказаний особливий захист повинен, зокрема, застосовуватися щодо використання персональних даних дітей в цілях маркетингу або створення особистого профілю чи профілю користувача і збору персональних даних дітей при наданні послуг, пропонованих безпосередньо дітям. При цьому згода батьків або осіб, які їх замінюють, на обробку персональних даних дітей не завжди є необхідна, особливо щодо профілактичного технічного обслуговування і консультаційних послуг, що надаються безпосередньо дитині. Тому пропонуємо доповнити Закон України «Про захист персональних даних» нормою, яка б надавала фізичній особі у віці від чотирнадцяти до вісімнадцяти років (неповнолітній особі) право самостійно надавати згоду на обробку персональних даних та здійснювати права суб'єкта таких даних.

Із визначенням часових рамок правоздатності та дієздатності суб'єкта персональних даних постає питання щодо правового режиму відомостей про зачату, але ще не народжену дитину, та відомостей про померлу особу. ЦК України (ч. 2 ст. 25) закріплює загальне правило, відповідно до якого, інтереси зачатої, але ще не народженої дитини охороняються у випадках, встановлених законом. Однак, Закон України «Про захист персональних даних» не містить спеціальних положень із цього питання. Якщо звернутися до досвіду європейських країн, то можна привести Висновок Робочої групи із захисту даних, утвореної відповідно до статті 29 Директиви № 95/46/ЄС, № 4/2007

(WP 136) від 20 червня 2007 року щодо концепції персональних даних [34]. Так, у висновку зазначено, що міра, в якій правила захисту даних можуть застосовуватися до народження дитини, залежить від загальної позиції національних систем права стосовно захисту ненароджених дітей. Для того щоб, наприклад, врахувати права спадщини, деякі держави визнають принцип, що діти, котрі зачаті, але ще не народжені, вважаються такими, що начебто народилися, коли справа стосується благ (і таким чином можуть отримати спадщину або прийняти пожертву), за умови, що вони зможуть бути народжені живими. В інших державах спеціальний захист надається конкретними правовими нормами також з дотриманням цієї ж умови. Щоб визначити, чи положення національного законодавства про захист даних також захищають інформацію про ненароджених дітей, потрібно брати до уваги цей загальний підхід, разом з думкою, що призначення правил захисту даних – захищати дані про особу.

Таким чином, відомості чи сукупність відомостей про зачату, але ще не народжену дитину, яка ідентифікована або може бути конкретно ідентифікована, становлять персональні відомості такої особи після її народження живою, а сама вона набуває статусу суб'єкта персональних даних. Однак, при цьому необхідно враховувати два моменти. По-перше, часові рамки таких відомостей не обмежуються строком вагітності матері, особливо у випадках, коли така дитина народжена за допомогою допоміжних репродуктивних технологій (внутрішньоматкова інсемінація; донація гамет та ембріонів; сурогатне (замінне) материнство; кріоконсервація сперми, ооцитів, ембріонів та біологічного матеріалу, отриманого з яєчка або його придатка, оваріальної тканини; редукція ембріонів тощо). По-друге, такі відомості будуть складати персональні дані не тільки народженої дитини, а насамперед її матері, а також можливо і батька дитини (сурогатної матері, генетично споріднених батьків, донорів статевих клітин тощо). У цьому випадку можливе зіткнення прав на персональні дані народженої дитини та вказаних інших фізичних осіб,

котре може бути вирішено лише при дотриманні справедливого балансу та забезпеченні розумного співвідношення між інтересами, що зачіпаються, як це має місце в практиці ЄСПЛ [46].

Не вирішеним сьогодні на рівні закону залишається питання про правову долю персональних даних після смерті їх суб'єкта. Так, у момент смерті суб'єкта персональних даних припиняється його цивільна правоздатність як фізичної особи. Права суб'єкта персональних даних, який помер, не переходять до його спадкоємців, оскільки належать до особистих немайнових прав та не входять до складу спадщини як такі, що нерозривно пов'язані з особою спадкодавця. Однак, відомості чи сукупність відомостей про померлу фізичну особу, які оброблялись як персональні дані за її життя, будуть продовжувати існувати в електронній формі та/або у формі картотек, упорядкованих у тих самих базах персональних даних. Спробуємо з'ясувати правовий режим таких відомостей.

Насамперед слід зазначити, що в Україні вже була спроба законодавчо врегулювати правовий режим персональних даних померлої особи. Так, ще у проекті Закону України «Про захист персональних даних» [47] містилось таке положення: «Право на розпорядження персональними даними фізичної особи, яка померла, належить її спадкоємцям в частині персональних даних». Очевидним є дискусійність зазначеного формулювання, оскільки персональні дані фактично розглядаються як елемент складу спадщини, що може викликати сьогодні певні заперечення. Проте, сама ідея захисту персональних даних після смерті їх суб'єкта, на наш погляд, заслуговує на увагу. Пояснення цього полягає в наступному. По-перше, чинне законодавство вже містить норму про захист інформації про померлу особу. Так, ст. 7 Закону України «Про поховання та похоронну справу» [48] встановлює гарантію конфіденційності інформації про померлого. Більше того, ЦК України відома низка випадків, коли за членами сім'ї та (або) родичами померлої особи закріплюються окремі права, пов'язані зі сферою приватного життя останньої. Наприклад, право на

відповідь, а також на спростування недостовірної інформації щодо особи, яка померла (ч. 2 ст. 277); право бути присутніми при дослідженні причин її смерті та ознайомитись із висновками щодо причин смерті, а також право на оскарження цих висновків до суду (ч. 4 ст. 285); право на використання імені померлої особи в літературних та інших творах, крім творів документального характеру, як персонажа (ч. 2 ст. 296); право на використання особистих паперів померлої особи, у тому числі шляхом опублікування (ч. 4 ст. 303); право на використання кореспонденції померлої особи, зокрема шляхом її опублікування (ч. 3 ст. 306); право на публічний показ, відтворення, розповсюдження фотографії, інших художніх творів, на яких зображено померлу особу (ч. 1 ст. 308) тощо. Стефанчук Р. О. такі права пропонує називати «посттанативними» особистими немайновими правами, під якими слід розуміти такі особисті немайнові права фізичних осіб, що виникають внаслідок та в момент смерті фізичної особи в інших осіб, які конкретно визначені законом чи встановлені померлим, і, як правило, спрямовані на захист доброго імені померлого [6, с. 534]. Більшість таких прав стосується відомостей про померлу особу, яка ідентифікована або може бути конкретно ідентифікована. Тому не зовсім зрозуміло, чому таке право не передбачено щодо персональних даних.

Частковим виправданням цьому є те, що Директива 95/46/ЄС [32], у відповідність до якої привести національне законодавство був покликаний Закон України «Про захист персональних даних», не містить положень, котрі б визначали порядок обробки персональних даних померлих осіб.

При цьому, щоправда, Робоча група 29 розглядала питання персональних даних померлих осіб у Висновку 4/2007 щодо концепції персональних даних [34]. Основні правові позиції цього висновку можна звести до наступних. По-перше, відомості про померлу особу не можуть вважатися персональними даними, оскільки людина, яка померла, не може вважатися фізичною особою як учасником цивільних відносин. По-друге, володілець, розпорядник

персональних даних можуть продовжувати обробляти відомості про померлу особу так само, як персональні дані живих фізичних осіб. З одного боку, володілець та (або) розпорядник персональних даних не завжди можуть взнати про факт смерті суб'єкта персональних даних. З іншого боку, інформація про померлих осіб може також ідентифікувати живих суб'єктів персональних даних. У випадках, коли інформація, що є відомостями про померлу особу, одночасно стосується і живих суб'єктів персональних даних, така інформація відноситься до персональних даних та опосередковано підпадає під правила захисту персональних даних. По-третє, відомості про померлих осіб можуть бути предметом спеціального захисту, що забезпечується набором норм спеціального законодавства по відношенню до законодавства про захист персональних даних. По-четверте, законодавство на національному рівні може розширити межі захисту персональних даних на відомості про померлих осіб.

Загальний регламент про захист даних [49], більше того, неодноразово в преамбулі повторює, що він не застосовується до персональних даних померлих осіб (п. 27, 158, 160). Однак, при цьому прямо вказується, що країни-члени ЄС можуть передбачати спеціальні правила обробки персональних даних померлих осіб. З цього приводу можна виділити два підходи європейських країн щодо регулювання обробки персональних даних померлої особи. Перший з них умовно можна назвати негативним, і полягає він у безпосередньому виключені відносин з приводу відомостей про померлу особу зі сфери дії законодавства про захист персональних даних. Наприклад, Закон Великобританії Про захист персональних даних (Data Protection Act, 1998) [50], визначає персональні дані як дані, що стосуються живої фізичної особи. Аналогічна норма закріплена в Законі Швеції про захист персональних даних (Personal Data Act, 1998): персональні дані – будь-яка інформація, яка безпосередньо чи опосередковано може стосуваттся фізичної особи, яка є живою [51].

Другий підхід – позитивний – представлений країнами, які поширюють дію законодавства про захист персональних даних на відносини щодо обробки відомостей про померлу особу Так, Закон Болгарії про захист персональних даних передбачає, що у випадку смерті фізичної особи, її права суб'єкта персональних даних можуть здійснювати її спадкоємці [52]. Французький закон про захист фізичних осіб при обробці персональних даних [53] надає спадкоємцям померлої особи право вимагати від розпорядника оновити персональні дані, що стосуються такої померлої особи. Більше того, цим законом встановлюється презумпція згоди фізичної особи на обробку її персональних даних після її смерті. Найбільш прогресивним у цьому плані є Закон Словенії про захист персональних даних [54], який містить спеціальну статтю, присвячену обробці персональних даних померлої особи. Зокрема, закріплено наступні правила: персональні дані померлої особи можуть оброблятися на підставі закону; спадкоємці померлої особи можуть вимагати доступу до її персональних даних, за винятком випадків, коли остання ще за свого життя письмово заборонила такий доступ; будь-хто може вимагати доступу до персональних даних померлої особи з метою історичних, статистичних та наукових досліджень, за винятком випадків, коли остання ще за свого життя письмово заборонила такий доступ, або такий доступ заборонили спадкоємці померлої особи.

Проведений аналіз свідчить, що чинний Закон України «Про захист персональних даних» потребує вдосконалення в частині визначення, чи поширює він свою дію на обробку відомостей про померлу особу. Вважаємо, що більш доцільним є позитивний підхід, котрий відповідає концепції посттанативних особистих немайнових прав, визнаних вітчизняною наукою, та традиції їх закріплення на рівні цивільного законодавства. У зв'язку із цим, пропонуємо доповнити зазначений Закон статтею, яка б передбачала захист персональних даних померлої особи. Така стаття повинна передбачати, принаймні, такі положення: закріплювати як додаткову підставу для обробки

персональних даних померлої особи згоду членів її сім'ї або близьких родичів, надану вже після смерті такої особи; надавати суб'єкту персональних даних право висловити свою волю щодо обробки його даних після смерті (заборонити в цілому або в частині), якщо законодавством не передбачено обробку таких даних незалежно від згоди їх суб'єкта; надати членам сім'ї та близьким родичам померлої особи, персональні дані якої обробляються після її смерті, реалізовувати щодо таких даних права їх суб'єкта; дозволити обробку персональних даних померлої особи в історичних, статистичних чи наукових цілях за умови забезпечення їх належного захисту.

Таким чином, можемо запропонувати поширити дію законодавства про захист персональних даних на відносини щодо обробки відомостей про померлу особу («посттанативні права»), та доповнити Закон України «Про захист персональних даних» статтею 4-1 «Захист персональних даних при обробці відомостей про померлу особу». Відповідно, диспозицію статті викласти у такому вигляді: «1. Суб'єкт персональних даних має право висловити свою волю щодо обробки його даних після смерті (заборонити в цілому або в частині), якщо законодавством не передбачено обробку таких даних не залежно від згоди їх суб'єкта.

2. Члени сім'ї або близьких родичів померлої особи мають право надавати згоду або забороняти обробку персональних даних померлої особи в історичних, статистичних чи наукових цілях за умови забезпечення їх належного захисту».

Поняття «суб'єкт персональних даних» є загальним, тобто, своїм обсягом охоплює будь-яку фізичну особу, відомості про яку підлягають обробці, незалежно від типу правовідносин, в яких така обробка відбувається. Тому спробуємо здійснити поділ суб'єктів персональних даних на види. За класифікаційний критерій візьмемо спеціальний правовий модус, який суб'єкт персональних даних набув в силу законодавства. Значення такого поділу полягає в тому, що той чи інший правовий модус може спричиняти зміну

правового режиму персональних даних та (або) особливості здійснення та захисту особистих немайнових прав їх суб'єкта. Зрозуміло, що перелік таких правових модусів не може бути ні повним, ні вичерпним. Тому акцентуємо свою увагу лише на трьох із них, які фактично можуть стосуватися будь-якої фізичної особи: здобувач освіти, працівник, пацієнт.

Здобувачі освіти (вихованці, учні, студенти, курсанти, слухачі, стажисти, аспіранти (ад'юнкти), докторанти, інші особи, які здобувають освіту за будь-яким видом та формою здобуття освіти) виступають суб'єктом персональних даних, що обробляються закладами освіти (в особових справах), та тих, що містяться в Єдиній державній електронній базі з питань освіти – автоматизованій системі, функціями якої є збір, верифікація, оброблення, зберігання та захист інформації про систему освіти. Персональні дані вносяться до Єдиної бази у випадках, передбачених законом, у порядку та обсягах, що визначаються розпорядником Єдиної бази. Внесення персональних даних в Єдину базу в інших випадках здійснюється за згодою суб'єкта персональних даних (п. 5 Положення про Єдину державну електронну базу з питань освіти [55]). Також треба враховувати, що поняття «здобувачі освіти» охоплює здобувачів дошкільної та повної загальної середньої освіти, здобувачів позашкільної, професійної (професійно-технічної), фахової передвищої та післядипломної освіти, здобувачів вищої освіти. Тобто, здобувачами освіти є фізичні особи різні за віком (діти та дорослі) та обсягом дієздатності (малолітні, неповнолітні, повнолітні).

Особливість правового модусу пацієнта, тобто фізичної особи, яка звернулася за медичною допомогою та (або) якій надається така допомога, як суб'єкта персональних даних полягає в наступному. Насамперед, інформація про стан здоров'я, належать до так званої «чутливої» інформації [56, с. 190], а тому підпадає під дію особливих вимог до обробки персональних даних (ст. 7 Закону України «Про захист персональних даних»). Більше того, персональні дані пацієнта, а саме: відомості про стан свого здоров'я, факт звернення за

медичною допомогою, діагноз, а також про відомості, одержані при його медичному обстеженні, охоплюються правом на таємницю про стан здоров'я (ст. 39[1]Основ законодавства України про охорону здоров'я [57]); відомості про хворобу, медичне обстеження, огляд та їх результати, інтимну і сімейну сторони життя громадянина підпадають під правовий режим лікарської таємниці (ст. 40 Основ законодавства України про охорону здоров'я [57]). Саме тому ЄСПЛ урішенні у справі «M.C. проти Швеції» (M.C. v. Sweden) (1997) [58] зазначив, що охорона даних особистого характеру (особливо медичних даних) має основоположне значення для здійснення права на повагу до приватного і сімейного життя. Дотримання конфіденційності відомостей про здоров'я становить основний принцип правової системи усіх держав-учасниць Конвенції. Він є важливим не лише для захисту приватного життя хворих, а й для збереження їхньої довіри до працівників медичних закладів і системи охорони здоров'я загалом. Національне законодавство має забезпечувати відповідні гарантії, щоб унеможливити будь-яке повідомлення чи розголошення даних особистого характеру стосовно здоров'я, якщо це не відповідає гарантіям, передбаченим ст. 8 Конвенції».

Крім того, персональні дані пацієнта обробляються різноманітними за своїм правовим статусом суб'єктами, а саме: медичним працівником або іншою особою закладу охорони здоров'я чи фізичною особою-підприємцем, яка одержала ліцензію на провадження господарської діяльності з медичної практики, та її працівниками, на яких покладено обов'язки щодо забезпечення захисту персональних даних та на яких поширюється дія законодавства про лікарську таємницю, працівниками центрального органу виконавчої влади, що реалізує державну політику у сфері державних фінансових гарантій медичного обслуговування населення, на яких покладено обов'язки щодо забезпечення захисту персональних даних. Саме тому в Україні запроваджено електронну систему охорони здоров'я (ст. 11 Закону України «Про державні фінансові гарантії медичного обслуговування населення» [59]) – інформаційно-

телекомунікаційну систему, що забезпечує автоматизацію ведення обліку медичних послуг та управління медичною інформацією шляхом створення, розміщення, оприлюднення та обміну інформацією, даними і документами в електронному вигляді, до складу якої входять центральна база даних та електронні медичні інформаційні системи, між якими забезпечено автоматичний обмін інформацією, даними та документами через відкритий програмний інтерфейс (API). Функціонування електронної системи охорони здоров'я повинно здійснюватися з урахуванням вимог законодавства про захист персональних даних. Особливості обробки персональних даних пацієнтів спонукають науковців виділити кілька ключових положень, які формуватимуть алгоритм дій при обробці персональних даних у сфері охорони здоров'я [60, с. 218–220].

Специфіка захисту персональних даних в трудових правовідносинах обумовлена насамперед ціллю їх обробки. Тобто, роботодавець має законні підстави для обробки персональних даних працівника, але лише в межах, які необхідні при прийнятті його на роботу та подальшим виконанням ним трудової функції. Наприклад, при укладенні трудового договору громадянин зобов'язаний подати паспорт або інший документ, що посвідчує особу, трудову книжку, а у випадках, передбачених законодавством, – також документ про освіту (спеціальність, кваліфікацію), про стан здоров'я та інші документи (ч. 2 ст. 24 Кодексу законів про працю України [61]). Отже, в межах трудових відносин обробці підлягають серед іншого і чутливі персональні дані. Саме тому заборона обробки таких персональних даних не поширюється на випадки, коли це необхідно для здійснення прав та виконання обов'язків володільця у сфері трудових правовідносин відповідно до закону із забезпеченням відповідного захисту (п. 2 ч. 2 ст. 7 Закону України «Про захист персональних даних»). Саме тому, в науці запропоновано виділяти поняття «персональні дані працівника», які є видовим поняттям по відношенню до персональних даних. Під персональними даними працівника слід розуміти інформацію, необхідну

роботодавцю у зв'язку з трудовими відносинами, що стосується конкретного працівника. При цьому слід визначити кваліфікуючі ознаки персональних даних працівника, що можуть бути об'єктом захисту. Персональні дані працівника повинні дозволити ідентифікувати його не стільки як людину, а саме як працівника [62, с. 277].

Також необхідно враховувати, що працівник по відношенню до роботодавця виступає слабкою стороною, а тому потребує встановлення на законодавчому рівні додаткових гарантій та механізмів захисту. З цього приводу Робоча група 29 прийшла до висновку, що відсутність економічної рівноваги між роботодавцем, який просить згоди, і працівниками, які надають її, часто викликає сумніви щодо того, чи було цю згоду надано вільно [63]. Відповідно до положень Закону України «Про захист персональних даних» обробка персональних даних працівників у сфері трудових відносин та соціального захисту здійснюється володільцем персональних даних на підставі дозволу, наданого володільцю персональних даних відповідно до закону виключно для здійснення його повноважень (п. 2 ч. 1 ст. 11 Закону України «Про захист персональних даних). Водночас, поширеним є явище, коли роботодавці, ігноруючи зазначене положення Закону, продовжують отримувати у працівників згоду на обробку їх персональних даних з метою ведення кадрового діловодства, забезпечення реалізації трудових відносин [64]. Усе сказане дає підстави підтримати висловлену пропозицію про необхідність розробки галузевого механізму захисту персональних даних працівників, необхідно розглядати з урахуванням специфіки, цілей і завдань трудового права та законодавства про працю [65, с. 20].

До спеціальних категорій суб'єктів персональних даних можна також віднести:

1) фізичну особу-підприємця, відомості про яку вносяться до Єдиного державного реєстру юридичних осіб, фізичних осіб-підприємців та громадських формувань, до частини яких надається безоплатний доступ в електронній формі

через портал електронних сервісів з метою перегляду, копіювання та друку [66];

2) фізичну особу-платника податків, персональні дані якої обробляються у базі персональних даних – Державному реєстрі фізичних осіб-платників податків, який формує та веде Державна фіскальна служба України [67];

3) публічну особу, а саме особу, яка займає посаду, пов'язану з виконанням функцій держави або органів місцевого самоврядування. Згідно із законодавством України не належать до інформації з обмеженим доступом: відомості, зазначені у декларації особи, уповноваженої на виконання функцій держави або місцевого самоврядування, поданій відповідно до законодавства про запобігання корупції, крім відомостей, зазначених в законі (ч. 6 ст. 6 Закону України «Про доступ до публічної інформації» [39]); персональні дані, зазначені у декларації про майно, доходи, витрати і зобов'язання фінансового характеру, оформленій за формою і в порядку, встановленими законодавством про запобігання корупції (ч. 3 ст. 5 Закону України «Про захист персональних даних»);

4) покупця (замовника, споживача) товарів, робіт, послуг у сфері електронної комерції, щодо яких встановлені спеціальні правила захисту їх персональних даних (ст. 14 Закону України «Про електронну комерцію» [68]);

5) фізичну особу-суб'єкта кредитної історії, тобто фізичну особу, яка уклала кредитний правочин та щодо якої формується кредитна історія. Під кредитною історією розуміють сукупність інформації про особу, що її ідентифікує, відомостей про виконання нею зобов'язань за кредитними правочинами, іншої відкритої інформації, а саме: прізвище, ім'я та по батькові; дата народження; паспортні дані; місце проживання; ідентифікаційний номер згідно з Державним реєстром фізичних осіб – платників податків та інших обов'язкових платежів; відомості про поточну трудову діяльність; сімейний стан особи та кількість осіб, які перебувають на її утриманні; дата і номер державної реєстрації, відомості про орган державної реєстрації та основний

предмет господарської діяльності фізичної особи – суб'єкта підприємницької діяльності [69].

Перелік спеціальних категорій суб'єктів персональних даних відповідно до чинного законодавства може бути ще продовжений. Більше того, можна припустити появу з часом нових категорій. Проведений аналіз різних видів суб'єктів персональних даних залежно від набутого ними спеціального правового модусу дозволяє прийти до таких висновків. По-перше, правовий режим персональних даних (їх відкритість, віднесення до інформації з обмеженим доступом), а також порядок здійснення та захисту суб'єктом таких даних своїх особистих немайнових прав може значно відрізнятися, в силу набутого правового модусу у випадках, передбачених законом. По-друге, який би правовий модус не набув суб'єкт персональних даних, правовий режим його даних, зміст його прав, в частині, яка не врегульована спеціальним законодавством, повинні відповідати загальним положенням Закону України «Про захист персональних даних».

1.3 Європейські стандарти цивільно-правового регулювання відносин щодо персональних даних

Правове регулювання цивільних відносин з приводу персональних даних має тривалу історію, упродовж котрої було вироблено систему стандартів, які, на наш погляд, найбільш повно розкриваються в джерелах права Ради Європи та ЄС. До них, насамперед, слід віднести Конвенцію про захист прав людини і основоположних свобод від 04.11.1950 [70], Конвенцію Ради Європи про захист осіб у зв'язку з автоматизованою обробкою персональних даних від 28.01.1981 [71], Директиву 95/46/ЄС Європейського Парламенту і Ради ЄС «Про захист фізичних осіб при обробці персональних даних і про вільне переміщення таких даних», яка була прийнята 24 жовтня 1995 р. (надалі – Директива 95/46/ЄС) [32], яка замінена Регламентом (Євросоюзу) 2016/679

Європейського Парламенту та Ради від 27 квітня 2016 р. про захист фізичних осіб щодо обробки персональних даних та про вільне переміщення таких даних (Загальним регламентом про захист даних) [49]. Дослідження вказаних джерел обумовлене не тільки їх змістовним наповненням, але й тим впливом, який вони здійснили на зближення цивільно-правової охорони особистісної немайнової сфери фізичної особи в межах європейського правового простору на рівні Ради Європи та Європейського Союзу [13, с. 20].

Першим міжнародним актом, який спрямований на захист персональних даних, стала Конвенція Ради Європи про захист осіб у зв'язку з автоматизованою обробкою персональних даних від 28.01.1981 р.. Необхідність її прийняття пояснюється суперечністю, що виникла наприкінці 1970-х років між все більш активним впровадженням засобів автоматизованої обробки даних та їх поширенням у телекомунікаційних мережах, зловживання при використанні персональних даних, потреба у впорядкуванні експортно-імпортних операцій [72, с. 33]. Україна ратифікувала цю Конвенцію 6 липня 2010 р. [73]. Значення цієї конвенції для уніфікації правового регулювання відносин з приводу персональних даних можна розкрити за допомогою наступних тезисів.

Конвенція закріпила основоположні принципи обробки персональних даних, а саме: a) сумлінність та законність отримання та обробки персональних даних; b) зберігання персональних даних лише для визначених і законних цілей та недопущення їх використання в спосіб, не сумісний із цими цілями; c) адекватність, відповідність та ненадмірність персональних даних стосовно цілей, для яких вони зберігаються; d) точність персональних даних та їх оновлення в разі необхідності; e) зберігання персональних даних у формі, яка дозволяє ідентифікацію суб'єктів даних не довше, ніж це необхідно для мети, для якої такі дані зберігаються. Фактично ця конвенція випереджала розвиток міжнародного загального права у відповідній сфері та створила «модель»правового регулювання, яка потім втілювалася на міжнародному,

регіональному та національному рівнях [74, с. 55]. Також Конвенція створила правові умови, які забезпечують зростання транскордонного потоку персональних даних. При цьому, Конвенція була названа без прив'язки до слова «європейська» через необхідність осягнення цієї проблеми не тільки європейськими країнами, але й державами всього світу. Це також було спробою регулювання процесу обміну інформацією у міждержавному просторі [75**Error! Reference source not found.**, с. 42].

Актуальність дослідження стандартів захисту права на персональні дані відповідно до Директиви 95/46/ЄС [32] обумовлена наступним. По-перше, більш, ніж двадцятирічна історія застосування Директиви та її вплив на захист персональних даних за межами ЄС свідчить про дієвість закладених у ній принципів. По-друге, реформування правового захисту персональних даних, яке на сьогодні відбувається в Європі та обумовлене розвитком інформаційних технологій, фактично відбувається на базі тих самих принципів.

Захист персональних даних в ЄС вже неодноразово ставав предметом вітчизняних цивілістичних досліджень, серед яких слід назвати праці таких вчених як В. М. Брижко, О. А. Дмитренко, О. В Кохановської, О. О. Кулініч, О. А. Підопригори, С. О. Сліпченка, О. П. Радкевича, І. І. Романюк, О. О. Серебряник, Н. В. Устименко, В. С. Цимбалюка, С. В. Шевчука, Р. Б. Шишки та інших вчених. В процесі нашого наукового дослідження ми також вважаємо за необхідне акцентувати увагу на окремих питаннях формування системи захисту персональних даних в ЄС, чому були присвячені окремі наші публікації [77]

Директива 95/46/ЄС має на меті захист основоположних прав і свобод фізичних осіб та, зокрема, їхнє право на захист особистого життя від втручання при обробці персональних даних за допомогою встановлення загальних правил, як визначають законність такої обробки [77].

Для розуміння змісту положень Директиви 95/46/ЄС необхідним є з'ясування її зв'язку з іншими міжнародними документами про права людини,

насамперед, Конвенції про захист прав людини і основоположних свобод. Так, стверджується, що предметом національного законодавства щодо обробки персональних даних є захист фундаментальних прав і свобод людини, особливо права на особисте життя, яке закріплюється як у ст. 8 Європейської Конвенції про захист прав людини і основоположних свобод, так і загальними принципами законодавства Співтовариства; приймаючи до уваги, що з цією метою зближення таких законів не повинне викликати будь-якого зменшення меж захисту, що надається ними, але, навпаки, повинно прагнути забезпечити високий рівень захисту в Співтоваристві (п. 10 преамбули) [77]. Крім того, принципи захисту прав і свобод фізичних осіб, особливо права на приватне життя, що містяться в цій Директиві, закріплюють і посилюють принципи, що містяться в Конвенції Ради Європи від 28 січня 1981 р. про захист фізичних осіб стосовно автоматичної обробки персональних даних (п. 11 преамбули). Ці міжнародні акти вважаються першими міжнародно-правовими стандартами, що визначають умови гармонізації національних законодавств у сфері захисту персональних даних як для європейських, так й інших країн світу [76, с. 46].

Директива 95/46/ЄС спричинила розвиток законодавства ЄС через прийняття низки правових актів, що регулюють питання захисту персональних даних осіб, наприклад: 1) Директива 97/66/ЄС Європейського Парламенту і Ради «Стосовно обробки персональних даних і захисту права на невтручання в особисте життя в телекомунікаційному секторі» від 15 грудня 1997 р., яка в подальшому була замінена Директивою 2002/58/ЄС «Про обробку персональних даних та захист таємниці у секторі електронних комунікацій (Директива про секретність та електронні комунікації) від 12 липня 2002 р.; 2) Регламент (ЄС) № 45/2001 про захист фізичних осіб при обробці персональних даних інститутами і органами Співтовариства і про вільне переміщення таких даних (Регламент інститутів ЄС щодо захисту персональних даних) від 18 грудня 2000 р.; 3) Директива 2006/24/ЄС «Про збереження даних, створених або оброблених при наданні загальнодоступних послуг електронних

повідомлень або громадських мереж зв'язку та про внесення змін до Директиви 2002/58/ЄС (Директива про збереження даних) від 15 березня 2006 р., яка втратила чинність 8 квітня 2014 р [77].

Директива 95/46/ЄС зумовила також відповідні зміни на рівні національного законодавства членів Європейського Союзу. Більше того, зазначається вплив директиви на країни, що не входять до складу Європейського Союзу, оскільки ст. 25 забороняє передачу до іншої країни персональних даних, що проходять обробку чи призначені для проходження обробки після передачі, допоки в такій країні не буде гарантовано належний захист персональних даних [13, с. 28]. Приміром, екстериторіальна спрямованість цієї статті робила практично неможливою передачу персональних даних з країн-членів ЄС в США, оскільки вважається, що останні не надають належного рівня захисту такої інформації. Тобто, європейська система захисту персональних даних і приватності не відповідала інтересам американських компаній, що функціонували на підставі стандартів саморегулювання. У зв'язку з цим виникла необхідність узгодження позицій двох ключових суб'єктів в досліджуваній сфері. 21 липня 2000 р. у відповідь на Директиву 95/46/ЄС Міністерство торгівлі США прийняло Принципи відповідності вимогам інформаційної безпеки ЄС (International Safe Harbor Privacy Principles), запропонувавши компаніям дотримуватися їх [78]. У рішенні Європейської Комісії 2000/520/ЄС визнається, що ці принципи забезпечують необхідний захист [79]. Крім того, в цілях гармонізації був створений механізм затвердження міжнародними корпораціями спеціальних, єдиних корпоративних правил обробки персональних даних [80, с. 67].

Наближення українського законодавства до європейських стандартів, що визначають права фізичної особи при обробці персональних даних, обумовило прийняття Закону України «Про захист персональних даних» [3]. Попри те, що цей Закон майже повністю базується на положеннях Директиви 95/46/ЄС, у літературі зазначаються недоліки втілення її положень в національному

законодавстві, тому для правильного тлумачення вказаного закону доцільним є врахування відповідних положень Директиви 95/46/ЄС. Прикладом цього є норма Закону, яка підставою для обробки персональних даних визнає дозвіл на обробку персональних даних, наданий володільцем персональних даних відповідно до закону виключно для здійснення його повноважень (п. 2 ч. 1 ст. 11). Це кореспондує положенню Директиви 95/46/ЄС, відповідно до якого персональні дані можуть оброблятися тільки за умови, що обробка необхідна для виконання завдання, здійснюваного при виконанні офіційних повноважень, якими наділений контролер або третя сторона, якій надаються дані (п. е ч. 1 ст. 7) [77]. Практика застосування цієї норми демонструє, що положення Директиви було викладено таким чином, що призвело до неправильного тлумачення підстави для обробки персональних даних, відповідно до якого обробка персональних даних можлива лише тоді, якщо існує пряма норма закону, що безпосередньо закріплює дозвіл на таку обробку. Але це розуміння не відповідає зазначеному положенню Директиви 95/46/ЄС [81, с. 18].

У науці стандарти захисту права на персональні дані відповідно до Директиви 95/46/ЄС розглядають крізь призму принципів захисту персональних даних [77]. Зокрема, до основних принципів, на яких на сьогодні базується правовий захист персональних даних, відносять: 1) принцип персоноцентризму, що полягає в тому, що система захисту персональних даних створена, насамперед, для забезпечення прав людини; 2) принцип екстериторіальності, який вимагає, щоб володільці персональних даних (контролери) поважали основні права і свободи фізичних осіб, незалежно від їх національності чи місця проживання; 3) принцип субсидіарності, тобто будь-яка обробка персональних даних у ЄС повинна відбуватись відповідно до законодавства однієї з держав-членів; повноваження володільця персональних даних (контролера), створеного в державі-члені ЄС, повинні визначатися національними законодавствами; держави-члени за власним бажанням

визначають ризики для прав і свобод суб'єктів даних у своєму законодавств [82, с. 57].

Нормативне закріплення принципів захисту персональних даних здійснено в ч. 1 ст. 6 Директиви 95/46/ЄС, відповідно до котрої: обробка персональних даних повинна здійснюватися добросовісно і законно; збирання персональних даних повинно здійснюватися для встановлених, чітких і законних цілей, і надалі не допускається обробка таких даних будь-яким способом, несумісним із цими цілями. Подальша обробка даних для історичних, статистичних або наукових цілей не вважається несумісною з даними принципами за умови, що держави-учасники забезпечать відповідні гарантії; персональні дані повинні бути адекватними, такими, що стосуються справи і не надмірними відносно цілей, для яких вони збираються і надалі обробляються; персональні дані повинні бути точними і, якщо необхідно, актуальними; мають бути зроблені будь-які обґрунтовані кроки, щоб неточні або неповні дані, стосовно цілей, для яких вони збиралися або для яких вони згодом оброблялися, видалялися або уточнювалися; персональні дані повинні зберігатися у формі, що дозволяє ідентифікацію суб'єктів даних не довше, ніж це необхідно для цілей, для яких дані збиралися або згодом оброблялися. Держави-учасники встановлять необхідні гарантії для персональних даних, що зберігаються триваліші терміни в історичних, статистичних або наукових цілях [77].

Цей перелік принципів інколи доповнюють такими: 1) персональні дані повинні оброблятися з дотриманням прав фізичної особи, включаючи право на доступ до даних; 2) персональні дані повинні оброблятися з дотриманням вимог щодо захисту інформації; 3) персональні дані не повинні передаватися за межі країни без відповідного захисту. Інколи до вказаних принципів додають також принцип підзвітності, згідно з яким кожен володілець повинен вживати всіх необхідних заходів із метою дотримання стандартів захисту персональних даних в ході їх обробки, а також бути здатним у будь-який момент надати

наглядовому органу/суб'єкту персональних даних документи, що продемонструють, яких саме заходів було вжито [81, с. 31]. Слід зазначити, що вказані вище стандарти відповідають основним принципам захисту даних Конвенції про захист осіб у зв'язку з автоматизованою обробкою персональних даних (ст. 5) та відображені на рівні загальних вимог до обробки персональних даних Закону України «Про захист персональних даних» (ст. 6). Розглянемо їх детальніше [83].

Так, практика ЄСПЛ виробила критерії правомірного обмеження прав на персональні дані, які відповідають загальним принципам правомірного втручання в приватне життя: втручання відповідає закону; втручання обумовлюється легітимною метою; втручання є необхідним у демократичному суспільстві [77]. Принцип законності обробки персональних даних може бути розкритий за допомогою практики ЄСПЛ. Так, ЄСПЛ тлумачить поняття «згідно із законом» як таке, що не лише вимагає, щоб відповідні заходи мали певну підставу в «законі», але й ставить вимогу щодо якості такого «закону», вимагаючи, щоб він був доступним особі, якої стосується, та передбачуваним у частині наслідків його застосування [84]. Доступність закону вимагає щоб нормативно-правовий акт було оприлюднено [85]. Передбачуваність означає, що норма сформульована з чіткістю, достатньою для того, щоб особа мала змогу, користуючись в разі потреби відповідною допомогою, регулювати свою поведінку [85]. Переслідувана мета буде легітимною, якщо відповідатиме одному із перерахованих у ч. 2 ст. 8 Конвенції суспільних інтересів, або ж правами і свободами інших осіб [81, с. 71]. Втручання є необхідним у демократичному суспільстві, якщо відповідає нагальній суспільній потребі і, зокрема, є пропорційним переслідуваній законній меті. Наприклад, інтереси національної безпеки при здійсненні перевірки при прийнятті на важливу з точки зору національної безпеки посаду, переважають приватні інтереси суб'єкта персональних даних [86].

Принцип легітимної мети обробки персональних даних вимагає: 1) мета обробки персональних даних не повинна суперечити законодавству про захист персональних даних; 2) мета обробки персональних даних повинна мати нормативне закріплення на рівні законів, інших нормативно-правових актів, установчих або інших документів, котрими регулюють діяльність володільця персональних даних; 3) для заміни визначеної мети обробки персональних даних на нову мету, що є несумісною з попередньою, необхідно отримати згоду суб'єкта персональних даних на обробку даних згідно із зміненою метою [77].

Відповідно до принципу пропорційності обробки персональних даних склад та зміст персональних даних, що обробляються володільцем, а також спосіб їх обробки повинні відповідати легітимній меті їх обробки: 1) обробка персональних даних не повинна бути надмірною, тобто обробці підлягають тільки ті дані, які необхідні для досягнення визначеної мети; 2) обробка даних не повинна здійснюватися, якщо визначена мета може бути досягнута без такої обробки [81, с. 46]; 3) в системах з великим об'ємом даних, які підлягають обробці, доцільно використовувати технології підвищеної конфіденційності або псевдоніми, що сприятиме забезпеченню приватності [87, с. 78].

Принцип точності та достовірності персональних даних зобов'язання володільця: 1) передбачає, що суб'єкти відносин з приводу персональних даних будуть вживати розумні заходи, щоб підтримувати актуальний стан персональних даних; 2) кореспондує праву суб'єкта персональних даних пред'явити вимогу про виправлення його персональних даних, якщо вони не відповідають дійсності, або привести їх до актуального стану; 3) не поширюється на випадки, коли законом заборонено обновляти дані, наприклад, коли ціллю зберігання даних є документування подій; 4) у випадках, коли неточні чи неактуальні дані можуть завдати шкоди суб'єкту персональних даних, перевірка їх точності та достовірності повинна здійснюватися на регулярній основі [81, с. 79].

Принцип обмеженого строку зберігання персональних даних: 1) означає, що тривале зберігання персональних даних без достатніх на те підстав становить непропорційне втручання у право на повагу до приватного життя [88]; 2) поширюється тільки на випадки зберігання даних у формі, яка дозволяє встановити суб'єкта персональних даних; 3) не стосується неперсоніфікованих даних, тобто зберігання персональних даних упродовж визначеного строку можливе лише у разі їх знеособлення чи псевдонімізації; 4) виняток складає зберігання персональних даних з метою історичних, статистичних та наукових досліджень за умови дотримання спеціально встановлених законодавством гарантій [81, с. 81].

Принцип справедливості обробки персональних даних передбачає, що обробка персональних даних здійснюється відкрито і прозоро із застосуванням засобів та у спосіб, що відповідають визначеним цілям такої обробки. Вказаний принцип включає в себе такі права та обов'язки суб'єктів і володільців, як інформування суб'єкта персональних даних щодо обробки його персональних даних, право доступу суб'єкта персональних даних, право суб'єкта направляти заперечення проти обробки його персональних даних із посиланням на вагомі та легітимні особисті обставини, право суб'єкта заперечити проти автоматизованого індивідуального рішення щодо нього та проти обробки персональних даних із метою здійснення цільового маркетингу, повідомлення наглядового органу у визначених законом випадках про обробку персональних даних та оприлюднення останнім такої інформації [77].

Із часу прийняття Директиви 95/46/ЄС посилилась роль технологічного прогресу та процесу глобалізації в створенні нових викликів у сфері захисту персональних даних. Масове розповсюдження соціальних мереж, користувачами яких на сьогодні є більш ніж 300 млн європейців, так зване «хмарне зберігання даних» є новітніми прикладами незахищеності даних фізичних осіб. При даній моделі зберігання інформації використовуються великі віддалені в мережі сервери, що надаються в користування клієнтам

третьою особою. Інформація користувачів зберігається та обробляється, як правило, на одному віртуальному сервері. При цьому, маючи певні переваги, дана модель зберігання може нести в собі потенційну загрозу безпеці даних, особливо коли мова іде про конфіденційні дані про особу [89]. Це стало передумовою реформування захисту персональних даних в ЄС [77].

Так, 27 квітня 2016 р. прийнято Регламент (Євросоюз) 2016/679 Європейського Парламенту та Ради від 27 квітня 2016 р. про захист фізичних осіб стосовно обробки персональних даних та про вільне переміщення таких даних (Загальний регламент про захист даних) [49]. Згідно з положеннями Загального регламенту про захист даних (далі – Загальний регламент), скасовується Директива 95/46/ЄС Європейського Парламенту та Ради Європи від 24 жовтня 1995 р. про захист фізичних осіб стосовно обробки персональних даних та про вільне переміщення таких даних. Загальний регламент набирає чинності на 20-й день після його опублікування в «Офіційному віснику Європейського Союзу» та застосовується з 25 травня 2018 р. Положення цього Регламенту спрямовані на гармонізацію захисту основних прав і свобод фізичних осіб, щодо діяльності з переробки і на забезпечення вільного потоку персональних даних між державами-членами ЄС. Загальний регламент покликаний сприяти розбудові простору свободи, безпеки, справедливості і економічного союзу; економічного і соціального прогресу; зміцненню законності і зближення економік у рамках внутрішнього ринку, а також загальному добробуту фізичних осіб держав-членів ЄС. Цілі і принципи Директиви 95/46/ЄС залишаються співзвучними з положеннями нового міжнародного акту – Регламенту ЄС 2016/679. Разом із тим, економічна інтеграція і розвиток ринку ЄС в умовах активного застосування інформаційних технологій привели до значного збільшення трансграничних потоків персональних даних, зокрема завдяки можливостям Інтернету. Нові технології і глобалізація принесли з собою нові проблеми для захисту персональних даних. Масштаби їх збору і використання значно зросли.

Технології змінюють як економіку, так і соціальне життя. Тому виникла необхідність в подальшій фрагментації і уніфікації законодавства про захист персональних даних у всіх державах Союзу [90, с. 89]. Регламент значно розширює вже існуючі права фізичної особи як суб'єкта персональних даних та вводить нові, серед яких посилення права доступу до персональних даних, право на мобільність персональних даних, право бути забутим, право знати про випадки незаконного доступу до персональних даних.

Актуальність дослідження нових стандартів вказаного Регламенту для України обумовлена не тільки євроінтеграційними процесами та Угодою про асоціацію між Україною та ЄС, але й також тим, що, відповідно до Регламенту, транскордонна передача персональних даних за межами ЄС буде дозволена лише за умови достатнього рівня захисту персональних даних, що надається в юрисдикції, в яку здійснюється передача даних. Крім того, відповідно до п. 11 Плану заходів щодо імплементації Угоди про асоціацію між Україною та ЄС, що був затверджений 25 жовтня 2017 року, Україна мас удосконалити своє законодавства про захист персональних даних з метою приведення його у відповідність до Регламенту до 25 травня 2018 р. [91]. Однак, наразі це ще не реалізовано.

Основні принципи обробки персональних даних, наведені у Регламенті, визначають, що персональні дані повинні:

1) оброблятися законно, справедливо і в доступній формі щодо суб'єкта даних («законність, справедливість і прозорість»);

2) збиратися для певної, конкретної і законної мети і не піддаватися додатковій обробці, що несумісна з цією метою; подальша обробка для цілей архівації, з метою наукових, дослідницьких, історичних і статистичних цілей не може бути несумісною з початковою метою («цільове обмеження»);

3) бути адекватними і обмежуватися тими даними, які відповідають і необхідні для досягнення цілі, для яких вони обробляються («зведення до мінімуму даних»);

4) бути точними і, при необхідності, постійно підтримуватися в актуальному стані; неточні персональні дані, з урахуванням цілі, для якої вони обробляються, слід видаляти або виправляти без затримки («точність»);

5) зберігатися у формі, що дозволяє ідентифікувати суб'єкта даних не довше, ніж це необхідно для цілі, для якої вони обробляються; персональні дані можуть зберігатися протягом тривалішого періоду виключно для цілей архівації, інтересів наукових, дослідницьких, історичних і статистичних цілей («обмеження зберігання»);

6) оброблятися так, щоб забезпечити належний захист персональних даних, включаючи захист від несанкціонованої або незаконної обробки, випадкової втрати, знищення або пошкодження, з використанням відповідних технічних або організаційних заходів («цілісність і конфіденційність») [92, с. 42].

Приходимо до таких висновків:

1. Норми Загального регламенту про захист даних слід розглядати в їх взаємозв'язку із положеннями Конвенції про захист прав людини і основоположних свобод та Конвенції Ради Європи про захист фізичних осіб при автоматизованій обробці персональних даних, які доповнюють і конкретизують їх зміст щодо здійснення та захисту права на персональні дані.

2. Директива 95/46/ЄС не тільки спричинила імплементацію її положень в національне законодавство країн-членів ЄС, але й слугувала основою для регулювання на рівні ЄС обробки персональних даних в окремих сферах. Загальний регламент про захист даних натомість не потребує імплементації, оскільки містить норми прямої дії.

3. Норма Загального регламенту про захист даних (як і аналогічна норма Директиви 95/46/ЄС) щодо заборони передавати персональні дані до країни, в якій не забезпечується належний рівень захисту персональних даних, зумовила транскордонний, навіть трансатлантичний вплив на зближення законодавства про захист персональних даних.

4. Закон України «Про захист персональних даних» є, по факту, імплементацією стандартів Директиви 95/46/ЄС, а тому при тлумаченні його норм варто використовувати також і зміст відповідних норм Директиви. На сьогодні назріла необхідність приведення його положень до нововведень Загального регламенту про захист даних.

5. В основі стандартів захисту права на персональні дані лежать закріплені в Загальному регламенті про захист даних принципи, а саме законності, легітимної мети, пропорційності обробки персональних даних, актуальності персональних даних, обмеженого у часі зберігання персональних даних [77].

Право на персональні дані, попри те, що не згадується в Конвенції про захист прав людини і основоположних свобод (надалі – Конвенція), підпадає під її дію, що неодноразово підтверджувалось в практиці ЄСПЛ. Так, ще в 1987 р. рішенням ЄСПЛ у справі Leander v. Sweden [86] було визнано, що інформація з секретного поліцейського реєстру містила інформацію про приватне життя п. Леандера, а зберігання і повідомлення цієї інформації, а також відмова надати можливість п. Леандеру спростувати її, порушували його право на повагу до приватного життя, гарантоване п. 1 ст. 8 Конвенції. Термін «персональні дані» ЄСПЛ використовує відповідно до ст. 2 Конвенції про захист осіб у зв’язку з автоматизованою обробкою персональних даних та розуміє під ним будь-яку інформацію, що стосується конкретно визначеної особи або особи, що може бути конкретно визначеною [84].

При цьому поняття «персональні дані» охоплюють не тільки відомості про «приватне життя», яке не повинно тлумачитися вузько, оскільки повага до приватного життя включає право встановлювати і розвивати відносини з іншими людьми, а також відомості щодо діяльності професійного і ділового характеру [84]. Так, наприклад, справі «X та інші проти Росії» ЄСПЛ повторив, що поняття «приватне життя» є широким терміном, котрий не допускає вичерпного визначення, яке охоплює фізичну та психічну недоторканність

особи і тому може охоплювати декілька аспектів його або її ідентичності. Воно також охоплює особисту інформацію, яка, як вони могли законно очікувати, не буде опублікована без їх згоди [93]. Більше того, публічна інформація може охоплюватись поняттям «приватне життя», якщо вона систематично збирається та зберігається в базах даних, котрими володіють органи публічної влади [94].

Наступні приклади ілюструють широке коло видів персональних даних, що були предметом розгляду ЄСПЛ: офіційний перепис, в якому обов'язково збираються дані про стать, сімейний стан, місце народження, етнічну приналежність разом з іншою особистою інформацією; зняття поліцією відбитків пальців, знімків, зразків клітин, профілів ДНК та іншої особистої або публічної інформації, навіть якщо на неї поширюються умови таємності; збір і зберігання медичних даних і інших медичних записів; примус надавати детальну інформацію про особисті витрати з фіскальною метою (розкриття інтимних аспектів приватного життя); прослуховування, запис і зберігання телефонних розмов; система ідентифікації особи, розроблена для адміністративних і цивільних цілей, наприклад, бази даних в сфері охорони здоров'я, соціальної допомоги і податкових органів; знімки системи охоронного відеоспостереження, зроблені на вулиці; система перехоплення розмов між ув'язненими та їхніми родичами в кімнатах для побачень в місцях ув'язнення [95, с. 31–32].

Серед прав суб'єкта персональних даних в практиці ЄСПЛ на сьогодні можна виділити наступні:

1) Право на доступ до своїх персональних даних охоплюється, насамперед, негативним обов'язком держави не здійснювати свавільне втручання в приватне життя шляхом обмеження можливості особи ознайомитись з інформацією приватного змісту про неї, яка збирається, зберігається, використовується та поширюється органами держави [86]. Крім того, це право випливає з позитивних обов'язків держави забезпечити повагу до приватного життя через закріплення механізму доступу до персональних

даних [96]. При цьому право на доступ повинно бути ефективним, тобто не тільки надавати можливість ознайомитись з персональними даними та робити власноручні письмові витяги, але й можливість виготовлення копій документів з персональними даними [97], а також бути реалізованим у межах розумного строку [**Error! Reference source not found.**]. Право на доступ до персональних даних може бути обмежено в інтересах держави, наприклад, задля захисту національної безпеки [86], а також приватних інтересах, наприклад, захист конфіденційної інформації третіх осіб [99].

2) Забезпечення захисту персональних даних означає наявність позитивного зобов'язання держави щодо забезпечення поваги до її приватного життя за допомогою впровадження системи правил і гарантій щодо захисту даних, а саме практичного і ефективного механізму захисту, який би, насамперед, виключив саму можливість будь-якого несанкціонованого доступу до персональних даних [100].

3) Право на зміну або знищення своїх персональних даних. ЄСПЛ вважає, що відмова в наданні можливості спростувати персональні дані, які не відповідають дійсності, становить втручання в право на повагу приватного життя, гарантоване ст. 8 Конвенції [94]. Крім того, позитивний обов'язок держави забезпечувати повагу приватного життя охоплює собою передбачення процедури, яка б давала можливість вносити зміни в персональні дані, в тому числі – щодо етнічного походження [101]. ЄСПЛ також визнає так зване право на забуття, відповідно до якого тривале зберігання персональних даних без достатніх на те підстав становить непропорційне втручання у право на повагу до приватного життя [102].

Практика ЄСПЛ виробила критерії правомірного обмеження прав на персональні дані, що відповідають загальним принципам правомірного втручання в приватне життя: втручання відповідає закону; втручання переслідує легітимну мету; втручання є необхідним у демократичному суспільстві.

Таким чином, право на персональні дані отримує свій захист відповідно до практики ЄСПЛ в межах права на особисте життя. Персональними даними вважається будь-яка інформація, а не тільки інформація про особисте чи сімейне життя, за умови, що вони стосуються конкретно визначеної особи або особи, яка може бути конкретно визначена. За суб'єктом персональних даних визнається ціла низка прав, таких як право на доступ, на зміну, на знищення, на захист його персональних даних, здійснення яких може бути обмежено задля досягнення легітимної мети, за умови, що таке обмеження відповідає закону та є необхідним у демократичному суспільстві.

Висновки до Розділу 1

1. Персональні дані є нематеріальними благами, оскільки не належать до предметів матеріального світу, не мають матеріальної (фізичної) субстанції, не мають геометричних форм, розмірів, кольору тощо. Одночасно з нематеріальною природою персональні дані можуть бути збережені на матеріальних носіях (у формі картотек персональних даних) або відображені в електронному вигляді (база персональних даних в електронній формі). При цьому, персональні дані, будучи інформацією, одночасно виступають об'єктом особистих немайнових прав (особистим немайновим благом).

2. Персональні дані як особисте немайнове благо характеризуються немайновою природою, хоча, в силу сучасного рівня розвитку матеріальної та духовної культури, соціально-економічних відносин та інформаційного простору, об'єктивно можуть набувати майнової цінності. При цьому *відомості про фізичну особу самі по собі залишаються немайновими благами*, оскільки не створюються в процесі виробництва та не мають грошової вартості. А *майнова цінність персональних даних може бути обумовлена особистістю самої особи (наприклад, загальновідомої) або створюватись у процесі обробки персональних даних.*

3. Попри невіддільність персональних даних як особистого немайнового блага, *вони наділені відособленістю* завдяки об'єкту відомостей (інформація про конкретну фізичну особу), кількісного та якісного змісту відомостей (склад персональних даних, які обробляються), зовнішній формі (електронній формі та/або у формі картотек). Персональні дані належать до об'єктивованих нематеріальних благ, що виражені в доступній для сприйняття органами людських чуттів об'єктивній формі. Об'єктивованість вказує на зовнішній стосовно суб'єкта характер персональних даних. У свою чергу, об'єктивована форма персональних даних створює можливість їх використання у відриві від особи-носія (суб'єкта персональних даних), що свідчить про віддільність таких даних.

4. Персональні дані як особисте немайнове благо наділені такими ознаками: 1) відособленості; 2) об'єктивованості; 3) віддільності прав на персональні дані; 4) наділенність економічною цінністю; 5) мають властивості товару; 6) здатність брати участь в економічному обороті.

5. Зроблено висновок про те, що дефініція персональних даних у національному законодавстві в цілому відповідає європейським стандартам, закріпленим у вказаних міжнародних документах. При цьому, *визначення персональних даних у вітчизняному законі фактично запозичене з Директиви 95/46/ЄС.*

6. Визначення персональних даних структурно охоплює п'ять ознак: 1) відомості чи сукупність відомостей (включати 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.

При цьому *ознака ідентифікованості персональних даних є визначальною* при поширенні на відомості правового режиму персональних даних.

Перелік *ознак персональних даних* доповнено вказівкою на момент, з якого відомості про особу набувають правового режиму персональних даних; Такий момент пов'язаний із початком обробки персональних даних шляхом збирання, реєстрації, накопичення, зберігання, адаптування, зміни, поновлення, використання, поширення (розповсюдження, реалізація, передача), знеособлення, знищення персональних даних, у тому числі з використанням інформаційних (автоматизованих) систем.

7. *Поняття персональних даних* визначено як відомості або сукупність відомостей, що безпосередньо чи опосередковано стосуються фізичної особи, незалежно від її громадянства, постійного місця проживання чи іншого правового зв'язку з державою, яка 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 – з використанням інформаційних (автоматизованих) систем.

8. Поняття «персональних даних» потрібно відмежовувати від суміжних йому понять: «інформація про особу», «відомості про особисте життя фізичної особи», «ознаки, що індивідуалізують фізичну особу». *Усі ці поняття мають спільний обсяг*, тобто ті чи інші відомості можуть бути одночасно персональними даними та інформацію про особу, відомостями про особисте життя фізичної особи, ознаками, що індивідуалізують фізичну особу. Для *розмежування цих понять за змістом слід використовувати факт обробки*

відповідних відомостей. Тобто, відомості набувають правового режиму персональних даних внаслідок того, що стають предметом обробки.

9. *Поділ персональних даних на види відображає відмінності в їх правовому режимі.* Насамперед, необхідно розрізняти загальні та чутливі персональні дані, щодо яких законодавство встановлює особливі вимоги до обробки. Персональні дані також можуть бути поділені на ті, що належать, та ті, що не належать до інформації з обмеженим законодавством доступом, у тому числі тих, які забороняється відносити до інформації з обмеженим доступом. За правовим режимом також слід окремо виділяти персональні дані, що містяться в публічній інформації.

10. Проведено порівняльний наліз *бази персональних даних як об'єкта захисту персональних даних та бази даних як об'єкта авторського права*. Внаслідок проведеного аналізу Закону України «Про авторське право та суміжні права» та Директиви 96/9/ЄС Європейського Парламенту та Ради «Про правовий захист баз даних» від 11 березня 1996 р. було зроблено висновок про те, що база персональних даних буде одночасно відповідати умовам охороноздатності бази даних як об'єкта авторського права. Це означає, що *одна й та ж база персональних даних може підпадати під захист персональних даних та захист права авторства*.

11. Запропоновано поділ цивільних правовідносин 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 із приводу обробки персональних даних; 4) відносні відносини володільця, розпорядника персональних даних та третіх осіб між собою, які виникають з приводу обробки персональних даних. При цьому треті та четверті види відносин можуть мати як самостійний характер, так і бути додатковими щодо основних.

12. *Суб'єктом персональних даних може бути лише фізична особа*, тобто людина як учасник цивільних відносин, персональні дані якої обробляються, та яка наділена особистими немайновими правами на персональні дані, а тому виступає у правовідносинах щодо персональних даних управомоченою особою, правам якої кореспондують обов'язки інших учасників. *Здатність фізичної особи бути суб'єктом персональних даних виникає з моменту народження при здійсненні процедури її ідентифікації.*

13. З-поміж інших учасників відносин з приводу персональних даних їх *суб'єкт вирізняється такими ознаками*: 1) суб'єкт персональних даних є обов'язковим учасником таких відносин, без якого вони не виникають; 2) суб'єкт персональних даних виступає управомоченою особою, правам якої кореспондують обов'язки інших учасників, оскільки він наділений особистими немайновими правами щодо них.

14. Здатність фізичної особи своїми діями набувати та здійснювати права суб'єкта персональних даних залежить від їх обсягу дієздатності.

Щодо неповнолітніх осіб може мати місце два випадки: 1) коли обробка персональних даних неповнолітніх осіб здійснюється у зв'язку із правовідносинами, які охоплюються обсягом їх дієздатності; *2)* коли обробка персональних даних неповнолітніх осіб здійснюється у зв'язку із правовідносинами, які знаходяться за межами обсягу їх дієздатності. *У першому випадку* неповнолітня особа може самостійно здійснювати права суб'єкта персональних даних; *у другому* – ці права здійснюються за згодою батьків (усиновлювачів) або піклувальників.

Визначено особливості правового режиму відомостей про зачату, але ще не народжену дитину, та відомостей про померлу особу. Зроблено висновок про те, що відомості чи сукупність відомостей про зачату, але ще не народжену дитину, яка ідентифікована або може бути конкретно ідентифікована, *становлять персональні відомості такої особи після її народження живою*. При цьому, необхідно враховувати два моменти: 1) часові межі таких відомостей не обмежуються строком вагітності матері, особливо у випадках коли така дитина народжена за допомогою допоміжних репродуктивних технологій; 2) такі відомості будуть складати персональні дані як народженої дитини, так і матері (й батька). У разі *виникнення протиріччя прав на персональні дані народженої дитини та матері (й батька), таке питання слід вирішувати при дотриманні справедливого балансу та забезпечення розумного співвідношення між інтересами, що зачіпаються, як це має місце в практиці ЄСПЛ.*

15. Наголошується на *необхідності захисту персональних даних після смерті їх суб'єкта («посттанативні права»).* Проаналізовано два підходи європейських країн щодо регулювання обробки персональних даних померлої особи. *Перший («негативний»)* полягає у виключені відносин з приводу відомостей про померлу особу зі сфери дії законодавства про захист персональних даних (закони про захист персональних даних Великобританії, Швеції та ін.). *Другий (позитивний)* представлений країнами, де поширюється дія законодавства про захист персональних даних на відносини щодо обробки відомостей про померлу особу (закони про захист персональних даних: Болгарії – права суб'єкта персональних даних можуть здійснювати її спадкоємці; Франції – спадкоємцям померлої особи надається право вимагати від розпорядника оновити персональні дані щодо померлої особи та встановлюється презумпція згоди фізичної особи на обробку її персональних даних після її смерті; Словенії – передбачено окрему статтю, присвячену правилам обробки персональних даних померлої особи та ін.).

16. Охарактеризовано *окрему категорію суб'єктів персональних даних, зокрема, здобувача освіти, працівника, пацієнта.* Зроблено висновок про необхідність розробки галузевого механізму захисту персональних даних таких осіб.

17. Актуальність дослідження європейських стандартів захисту права на персональні дані відповідно до Директиви 95/46/ЄС обумовлена наступним. По-перше, більш ніж двадцятирічна історія застосування Директиви та її вплив на захист персональних даних за межами ЄС свідчить про дієвість закладених у ній принципів. По-друге, реформування правового захисту персональних даних, яке сьогодні відбувається в Європі та обумовлене розвитком інформаційних технологій, фактично відбувається на базі тих самих принципів.

Зроблено висновок про те, що *з часу прийняття Директиви 95/46/ЄС посилилась роль технологічного прогресу та процесу глобалізації в створенні нових викликів у сфері захисту персональних даних.* Наприклад, масове розповсюдження соціальних мереж, так зване «хмарне зберігання даних», віддалені в мережі сервери, що надаються в користування клієнтам третьою особою, створюють потенційну загрозу безпеці даних. Це стало передумовою реформування захисту персональних даних в ЄС шляхом прийняття 27 квітня 2016 р. Регламенту (Євросоюз) 2016/679 Європейського Парламенту та Ради про захист фізичних осіб стосовно обробки персональних даних та про вільне переміщення таких даних (Загальний регламент про захист даних), який застосовується з 25 травня 2018 р.

Положення цього Регламенту спрямовані на гармонізацію захисту основних прав і свобод фізичних осіб, щодо діяльності з переробки і на забезпечення вільного потоку персональних даних між державами-членами ЄС. Регламент значно розширює вже існуючі права фізичної особи як суб'єкта персональних даних та вводить нові, серед яких *посилення права доступу до персональних даних, право на мобільність персональних даних, право бути забутим, право знати про випадки незаконного доступу до персональних даних*.

18. Європейські стандарти найбільш повно відображені в Загальному регламенті про захист даних, норми якого слід розглядати у їх взаємозв'язку із положеннями Конвенції про захист прав людини і основоположних свобод і Конвенції Ради Європи про захист фізичних осіб при автоматизованій обробці персональних даних, які доповнюють і конкретизують їх зміст щодо здійснення та захисту права на персональні дані. *В основі європейських стандартів захисту права на персональні дані покладено принципи, закріплені в Загальному регламенті про захист даних*, а саме: законності, легітимної мети, пропорційності обробки персональних даних, актуальності персональних даних, обмеженого у часі зберігання персональних даних.

Директива 95/46/ЄС не лише обумовила імплементацію її положень в національне законодавство країн-членів ЄС, але й слугувала основою для регулювання на рівні ЄС обробки персональних даних в окремих сферах. Норма Загального регламенту про захист даних (як і аналогічна норма Директиви 95/46/ЄС) щодо заборони передавати персональні дані до країни, в якій не забезпечується належний рівень захисту персональних даних, зумовила транскордонний, навіть трансатлантичний вплив на зближення законодавства про захист персональних даних. Закон України «Про захист персональних даних» є по факту імплементацією стандартів Директиви 95/46/ЄС, а тому при тлумаченні його норм варто використовувати також і зміст відповідних норм Директиви. Обґрунтовано необхідність приведення змісту Закону України «Про захист персональних даних» у відповідність до Загального регламенту про захист даних Європейського Парламенту та Ради, який застосовується з 25 травня 2018 р.;

19. *Практика ЄСПЛ виробила критерії правомірного обмеження прав на персональні дані*, які відповідають загальним принципам правомірного втручання в приватне життя: втручання відповідає закону; втручання переслідує легітимну мету; втручання є необхідним у демократичному суспільстві.

РОЗДІЛ 2
ПРОБЛЕМИ СТАТИКИ ЦИВІЛЬНИХ ПРАВОВІДНОСИН ЩОДО ПЕРСОНАЛЬНИХ ДАНИХ

2.1 Поняття та правова природа цивільних прав суб'єкта персональних даних

Перш за все, спробуємо з'ясувати місце прав суб'єкта персональних даних у системі суб'єктивних цивільних прав. Із цього приводу потребує тлумачення ч. 1 ст. 1 Закону України «Про захист персональних даних» [3], яка визначає сферу дії цього закону та встановлює його спрямування «на захист основоположних прав і свобод людини і громадянина, зокрема права на невтручання в особисте життя, у зв'язку з обробкою персональних даних». Аналогічна норма міститься також в ч. 2 ст. 1 Загального регламенту про захист даних [49] («Відповідно до цього Регламенту, держави-члени захищають основні права і свободи фізичних осіб і, особливо, їхнє право на невтручання в особисте життя при обробці персональних даних») та ст. 1 Конвенції Ради Європи про захист осіб у зв'язку з автоматизованою обробкою персональних даних [71] («Метою цієї Конвенції є забезпечення на території кожної Сторони для кожної особи, незалежно від її громадянства або місця проживання, дотримання її прав й основоположних свобод, зокрема її права на недоторканість приватного життя, у зв'язку з автоматизованою обробкою персональних даних, що її стосуються»). Постає питання про співвідношення прав суб'єкта персональних даних з основоположними (основними чи фундаментальними) правами людини.

Як нами вище було встановлено, право на персональні дані знаходить свій прояв на рівні міжнародних документів про права людини, зокрема: ст. 8 ЄКПЛ тлумачиться ЄСПЛ як така, що охоплює право на персональні дані; ст. 8Хартії основних прав Європейського Союзу [103] безпосередньо закріплює

право на захист персональних даних. При встановленні співвідношення прав суб'єкта персональних даних з відповідними правами людини слід виходити із того, що останні не обмежують свою дію відносинами в системі координат «людина – держава», тобто охоплюють як публічно-правову, так і приватно-правову сфери. З доктринальної точки зору це пояснюється домінуючою в європейській правовій науці концепцією горизонтального застосування прав людини [104, с. 98]. Горизонтальна дія прав людини поділяється на: 1) безпосередню горизонтальну дію – міжнародні нормативно-правові акти з прав людини, належним чином ратифіковані, вважаються нормами прямої дії; 2) сильну опосередковану дію – основоположні права людини до приватних правовідносин застосовуються опосередковано, через вплив на судову правозастосовну практику в межах тлумачення норм приватного права та усунення прогалин у праві; 3) слабку опосередковану дію – вплив на правозастосовну практику таким чином, щоб вона була сумісною з основоположними правами. Екстраполювання цих концепції на право України, дозволяє науковцям стверджувати про безпосередню дію прав людини [105, с. 113–114].

Віднесення права на персональні дані до основоположних прав людини має, принаймі, два важливих значення. По-перше, це повинно враховуватись при так званих колізіях (зіткненнях) суб'єктивних цивільних прав, під якими слід розуміти нетипові правові ситуації, що полягають в неможливості паралельного здійснення в повному обсязі суб'єктивних цивільних прав, які належать різним особам: реалізація будь-якого одного з прав у повному обсязі перешкоджає повністю / частково здійсненню іншого (інших) чи призводить до його припинення [106, с. 5]. Зокрема, Р. О. Стефанчук пропонує у разі зіткнення суб'єктивних цивільних прав виходити із такої їх ієрархії: 1) суб'єктивні цивільні права, що мають немайновий характер та об'єктами яких є особисті немайнові блага, які визнаються найвищими соціальним цінностями; 2) решта особистих немайнових прав; 3) інші суб'єктивні цивільні права [6, с. 169].

Посикалюк О. О. уточнює дану ієрархію, зазначаючи, що схематично вона матиме такий вигляд: особисті немайнові права, що входять до системи фундаментальних (основних) прав людини та об'єктом яких є особисті немайнові блага, які визнаються найвищими соціальними цінностями – інші особисті немайнові права, що входять до системи фундаментальних (основних) прав людини – решта особистих немайнових прав – інші суб'єктивні цивільні права [107, с. 126].

По-друге, віднесення права на персональні дані до основоположних зіграло визначальну роль у процесі зближення правового регулювання та охорони персональних даних в різних країнах. Це може бути продемонстровано на прикладі ЄС. Так, відповідно до ст. 16 Договору про функціонування Європейського Союзу [108] кожен має право на захист своїх персональних даних. При цьому Європейський Парламент та Рада, діючи згідно зі звичайною законодавчою процедурою, встановлюють правила захисту фізичних осіб під час обробки їхніх персональних даних установами, органами, службами та агенціями Союзу та державами-членами у ході провадження діяльності в межах, охоплених законодавством Союзу, а також правила щодо вільного руху таких даних. Також ст. 39 Договору про Європейський Союз [108] установи ЄС можуть ухвалювати рішення, що встановлює правила, пов'язані із захистом фізичних осіб з огляду на обробку персональних даних державами-членами при виконанні заходів, які підпадають під сферу застосування положень про спільну зовнішню та безпекову політику, а також правила, пов'язані з вільним рухом такої інформації. Ці норми лягли в основу Директиви 95/46/ЄС та Загального регламенту про захист даних, вплив яких на гармонізацію законодавства щодо персональних даних нами вже був досліджений [109].

Також слід брати до уваги, що право на персональні дані не є абсолютним. Можливість встановлення випадків правомірного втручання, винятків зі змісту та обмежень при здійсненні права на персональні дані нормативно закріплена в ч. 2 ст. 8 ЄКПЛ, ч. 1, 3 ст. 52 Хартії основних прав

Європейського Союзу, ч. 1, 2 ст. 9 Конвенції про захист осіб у зв'язку з автоматизованою обробкою персональних даних, ст. 9 та ч. 1 ст. 13 Директиви 95/46/ЄС, ч. 1 ст. 25 Закону України «Про захист персональних даних». Якщо узагальнити ці норми, то можна стверджувати, що будь-яке обмеженняправа на персональні дані має бути передбачене законом і відповідати основному змісту цього права. Обмеження можуть застосовуватися лише при дотриманні принципу пропорційності і тільки у тому разі, якщо вони необхідні в демократичному суспільстві, спрямовані на досягнення легальних цілей, або потрібні для захисту прав і свобод інших людей. Яскравим прикладом у цьому контексті є Рішення КСУ, яким КСУ визнав такими, що не відповідають Конституції України (є неконституційними), окремі положення абзацу першого пункту 40 розділу VI «Прикінцеві та перехідні положення» Бюджетного кодексу України (далі – Кодекс) щодо права Міністерства фінансів України (далі – Міністерство) отримувати інформацію, що містить персональні дані через те, що втручання у конституційне право особи на приватне і сімейне життя вважатиметься законним у разі наявності підстав в національному законі, а також за умови, що такий закон відповідатиме конституційному принципу верховенства права. Конституційний принцип верховенства права вимагає законодавчого закріплення механізму запобігання свавільному втручанню органів публічної влади при здійсненні ними дискреційних повноважень у права і свободи особи. Конституційний Суд України вважає, що повноваження Міністерства на безоплатне отримання інформації, що містить персональні дані, є дискреційними, а тому вкрай необхідно, щоб оспорювані положення Кодексу, які є підставою для здійснення відповідних повноважень Міністерством, узгоджувалися з конституційним принципом верховенства права, зокрема такими його елементами, як юридична визначеність та заборона свавілля [110].

Розглянемо загальні особливості встановлення балансу між правом на персональні дані та таким правами як: правом на свободу вираження поглядів;

правом на свободу літературної, художньої, наукової і технічної творчості; правом на доступ до публічної інформації.

Вирішення колізії при зіткненні права на персональні дані та правом на свободу вираження поглядів можна продемонструвати на прикладі рішення ЄСПЛ у справі Satakunnan Markkinapörssi Oy and Satamedia Oy v. Finland [111]. У цій справі ЄСПЛ встановив: оприлюднені заявниками відомості про фінських платників податків безпосередньо зачіпали приватне життя громадян; рішення фінської влади обмежили право заявників на вільне поширення інформації; це обмеження було засноване на законі, інтерпретація якого фінськими судами не була довільною або непередбачуваною; метою такого обмеження був захист законних прав і інтересів третіх осіб. ЄСПЛ визнав, що обидва права є рівноцінні і повинні, в принципі, користуватися однаковим захистом. Тому в кожному випадку належить оцінювати усі обставини справи в сукупності, приділяючи особливу увагу пропорційності прийнятих державою заходів переслідуваним цілям. При цьому ЄСПЛ використав такі критерії встановлення балансу свободи слова та права на персональні дані: вклад журналіста (автора) в суспільно значущу дискусію, міра публічності особи, що торкнулася інформацією, форма поширення відомостей і його наслідку, добросовісність в отриманні та інтерпретації фактів, характер і тяжкість застосованих до журналіста санкцій та ін. ЄСПЛ відмітив, що дана справа стосувалася збору і публікації даних, які були відкриті для загального доступу і мали відношення до великого числа фінських громадян. І хоча ЄСПЛ погодився з тим, що податкові відносини в державі представляють певний публічний інтерес, він не знайшов, що дії заявників вносили який-небудь вклад в суспільні дебати на актуальну для громадян Фінляндії тему. На думку суду, журналістська діяльність припускає якусь (хоч би мінімальну) аналітичну обробку отриманих даних, чого не було в даній справі. ЗМІ можуть претендувати на привілеї при роботі з персональними даними лише в тих випадках, коли їх метою є донесення до суспільства інформації, ідей або думок. Просте копіювання

величезних баз даних і їх дослівна публікація не можуть вважатися зробленими з журналістськими цілями. Швидше вони були призначені для задоволення простої людської цікавості щодо окремих аспектів чужого приватного життя.

Подоланню колізії між правом на персональні дані та правом на доступ до публічної інформації в національному законодавстві присвячена ч. 3 ст. 10^1 Закону України «Про доступ до публічної інформації» [39], яка передбачає, що публічна інформація, що містить персональні дані фізичної особи, оприлюднюється та надається на запит у формі відкритих даних у разі додержання однієї з таких умов: 1) персональні дані знеособлені та захищені; 2) фізичні особи (суб'єкти даних), персональні дані яких містяться в інформації у формі відкритих даних, надали свою згоду на поширення таких даних; 3) надання чи оприлюднення такої інформації передбачено законом; 4) обмеження доступу до такої інформації (віднесення її до інформації з обмеженим доступом) заборонено законом.

Також у справі Társaság a Szabadságjogokért v. Hungary [112] ЄСПЛ визнав, що громадськість має право на одержання інформації, яка представляє суспільний інтерес. У цьому рішенні ЄСПЛ визнав такий публічний інтерес, відповідно і порушення права на доступ до публічної інформації у разі відмови у її наданні, щодо інформації про парламентську скаргу, що перебувала на розгляді Конституційного суду, як елемент законного збору інформації з питань суспільної значимості.Створивши адміністративну перешкоду і відмовивши в наданні доступу до змісту подібного звернення заявникові, який брав участь у правомірному зборі інформації у справах громадської значущості, влада втрутилася в підготовчу частину цього процесу. Більше того, монополія конституційного суду на володіння інформацією в подібних справах була рівносильна цензурі. Крім того, скарга члена парламенту не містила ніяких посилань на його приватне життя. Було б згубним для свободи висловлювання думок у сфері політики, якби публічні особи могли обмежувати пресу і громадські дискусії, посилаючись на захист своїх персональних даних. Нарешті

Суд дійшов висновку, що перешкоди, створені для того, щоб не допустити до відомостей, що представляють суспільний інтерес, можуть стати стримувальним чинником для тих, хто працює в засобах масової інформації або в суміжних областях, виконуючи надзвичайно важливу роль «сторожового пса», і вплинути таким чином на їх можливість забезпечувати точне і достовірне інформування. Або справа «Breyer v. Germany», котра стосувалась того, чи порушують право на приватність (ст. 8 Конвенції) законодавчі положення, які зобов'язують операторів мобільного зв'язку витребовувати у потенційних абонентів інформацію, що містить персональні дані про особу (ім'я, номер телефону, адресу проживання, дату народження) при оформленні наперед оплачених сім-карток. ЄСПЛ прийняв рішення, згідно з яким, такі законодавчі вимоги не суперечать ст. 8 Конвенції [113].

Отже, законодавство повинно забезпечувати пропорційність між правом на персональні дані та правом на свободу висловлювання думок і інформації, у тому числі щодо обробки персональних даних для журналістських цілей і цілей академічної, художньої або літературної свободи. Винятки та обмеження прав суб'єкта персональних даних у випадках їх обробки для цілей журналістики або в цілях академічної, художньої чи літературної свободи повинні бути закріплені в законі та застосовуватись із дотриманням балансу між правом на персональні дані та відповідними колідуючими правами.

Поряд із цим, цивільно-правова природа права на персональні дані, на наш погляд, не викликає сумнівів, оскільки відносини, що виникають з приводу персональних даних, сповна відповідають ознакам, закріпленим в ч. 1 ст. 1 ЦК України. У той же час, місце права на персональні дані в системі суб'єктивних цивільних прав видається не таким вже й однозначним. Насамперед в літературі піднімається питання про можливість розглядати право на персональні дані як право власності.

Так, з огляду на положення цивільно-правового інституту права власності досліджує права учасників відносин із приводу персональних даних

М.М. Мікуліна, яка стверджує, що: володільцем персональних даних можна вважати особу, яка має юридичну можливість фактичного впливу на ці дані; розпорядником – особу, яка має юридичну можливість визначати фактичну та юридичну долю цих даних, тобто такі повноваження особам-розпорядникам може надати лише власник персональних даних; лише власник персональних даних акумулює всю сукупність повноважень на свої персональні дані [114, с. 38]. Л. В. Борисова та В. В. Тулупов використовують поняття «виключне право власності на персональні дані», тобто можливість законодавчого обмеження прав особи на персональні дані з точки зору інтересів інших фізичних осіб, суспільства і держави, а право власності надає особі монопольні права володіння, користування і розпорядження своїми персональними даними [115, с. 98]. В. І. Бобрик пропонує наділити фізичну особу-носія персональних даних лише первісним правом власності на свої персональні дані. Це право є непорушним і невідчужуваним, але ж персональні дані можуть бути за бажанням особи повідомлені стороннім фізичним чи юридичним особам, які в такому випадку, за думкою науковця, повинні набувати також права власності на ці персональні дані, точніше на їх накопичення, банки, бази таких даних. Дане право власності по відношенню до права власності на персональні дані їх носіїв буде вторинним. Але з метою захисту прав первісних власників, вторинне право власності на персональні дані має бути обмеженим, неповним, для чого в законодавстві необхідно встановити ряд обмежень стосовно використання і розпорядження такою власністю [116, с. 117].

Пояснення такого підходу криється в тому, що інформація визнається товаром і має певний економічний зміст, що повною мірою стосується і персональних даних, економічний зміст яких виражається в тому, що зі становленням і функціонуванням ринку, котрий передбачає рух товарів, послуг і капіталів, виникає необхідність у русі персональних даних. Персональні дані вказують на споживача, і відповідно на сферу й обсяги товарів та послуг, якими він користується. Персональні дані – це інформація, що представляє певний

економічний інтерес і може бути товаром незалежно від волі особи, якої вона торкається [116, с. 115]. Напевно саме це зумовило намагання законодавця на початку 90-х ввести інформацію в цивільне правове поле за допомогою поширення на неї речево-правового режиму. Так, перша редакція Закону України «Про інформацію» [2] закріплювала право власності на інформацію як врегульовані законом суспільні відносини щодо володіння, користування і розпорядження інформацією (наразі законодавець відмовився від поняття «права власності на інформацію» – уточнено мною – Ю. Б.) [109].

Вважаємо, що на сьогодні речево-правовий підхід щодо розуміння права на інформацію, загалом, та права на персональні дані, зокрема, не може бути сприйнятим. Тому ми підтримуємо висловлену в літературі позицію щодо наукової необґрунтованості пропозицій розгляду права на персональні дані як права власності [28, с. 14]. Така позиція відповідає аргументованому О. В. Кохановською положенню про те, що поняття «право власності на інформацію», яке безпідставно набуло за часів розробки національного законодавства широкого використання, не може застосовуватися до нематеріального блага особливого роду, яким є інформація: інформація і матеріальна об’єктивна форма, в якій вона може втілюватись, не можуть ототожнюватись [5, с. 9]. Разом із, тим таке положення потребує уточнення щодо прав володільців та розпорядників персональних даних. Наприклад, суб’єкт підприємницької діяльності, який правомірно обробляє персональні дані споживачів, зібрані під час реалізації товарів, робіт та послуг, може ставитись до таких персональних даних як до майна, компілюючи їх та досить часто продаючи такі компіляції персональних даних іншим суб’єктам [117, с. 517]. Отже, права на персональні дані можуть набувати ознак нематеріальних активів. Тому важливо розмежовувати права на персональні дані та права інтелектуальної власності, які можуть бути з ними пов’язані [109].

Оскільки персональні дані є одним із видів інформації, а остання як об’єкт цивільних відносин може проявлятися не тільки як інформаційний

продукт, але й як результат творчої інтелектуальної діяльності, тобто як об’єкт виключних прав [5 с. 6], постає питання про співвідношення правового режиму «бази персональних даних» як сукупності упорядкованих персональних даних та «бази даних» як об’єкта авторського права. З цього приводу підтримаємо позицію, відповідно до якої база персональних даних є різновидом бази даних (компіляції даних), що може бути як оригінальною (містить творчий вклад автору), так і неоригінальною (проста систематизована інформація про персональні данні людини) [118, с. 433]. Така відмінність випливає зі ст. 1, 8, 10 Закону України «Про авторське право і суміжні права» [40] та полягає в тому, що база персональних даних, підбір і розташування складових частин якої та її упорядкування є результатом творчої праці, визнається об’єктом авторського права, тоді як база персональних даних, що не відповідає критеріям оригінальності, не є об’єктом авторського права, але на неї поширюється право sui-generis (своєрідне право, право особливого роду). Під останнім розуміють право виробника бази даних стати на заваді вилученню чи повторному використанню всієї або значної, визначеної кількісно або якісно, частини змісту даної бази, коли одержання, перевірка або представлення цього змісту свідчать про істотне інвестування з точки зору якості і кількості (Директива 96/9/ЄС від 11 березня 1996 року про правову охорону баз даних [119]).

Для розмежування правового режиму бази персональних даних як об’єкта права інтелектуальної власності та об’єкту захисту у зв’язку із обробкою персональних даних необхідно враховувати наступне. По-перше, самі собою ні матеріальний носій бази персональних даних, ні її внутрішнє інформаційне наповнення не є об’єктом права інтелектуальної власності автора (творця, розробника) бази. Такими об’єктами виступають тільки індивідуальна система обігу інформації та/або особливий алгоритм оброблення інформаційного наповнення бази [120, с. 17]. По-друге, ні визнання бази персональних даних об’єктом авторського права, ні встановлення щодо неї права особливого роду,

не виключають застосування законодавства стосовно охорони персональних даних та не можуть йому суперечити.

Природа особистих немайнових прав суб'єкта персональних даних на сьогодні не викликає сумнівів, оскільки теоретично обґрунтована відповідність конструкції права на персональні дані усім ознакам особистого немайнового права [12, с. 234] та законодавчо закріплена (ч. 1 ст. 8 Закону України «Про захист персональних даних»). Натомість питання про місце права на персональні дані в системі особистих немайнових прав фізичних осіб та їх співвідношення між собою є питанням наукової дискусії. З цього приводу можна виділити три підходи.

Відповідно до першого з них, право на персональні дані розглядається як складова права на приватність. Так, практика Європейського суду з прав людини тлумачить ст. 8, що передбачає право на повагу до свого приватного і сімейного життя, до свого житла і кореспонденції, як таку, яка охоплює право на захист персональних даних. Так, у справі Леандер проти Швеції суд зазначив, що немає сумнівів, що інформація з секретного поліцейського реєстру містила інформацію про приватне життя заявника, а її зберігання, повідомлення, а також відмова надати можливість спростувати її, становили втручання в право на повагу до приватного життя, гарантоване пунктом 1 статті 8 Конвенції [86]. У подальшому цей підхід було підтверджено і щодо персональних даних, обробка яких здійснюється автоматизованими засобами (справа С. і Марпер проти Сполученого Королівства [121]). Пояснення цього підходу криється в самій ґенезі інституту захисту персональних даних. Розвиток інформаційних технологій поступово трансформувало розуміння поняття приватності у бік застосування заходів захисту права на інформаційний суверенітет особи, зокрема, права людини визначати ким, коли, з якою метою та яким чином інформація про неї буде використовуватися іншими особами [122, с. 8]. Іншими словами, право на персональні дані історично походить від права на приватність.

Другий підхід закріплений в Хартії основних прав Європейського Союзу [103], з буквального тлумачення якої право на повагу до особистого та сімейного життя, житла та кореспонденції (ст. 7) та право на захист персональних даних (ст. 8) розглядаються як два відокремлених права. Тобто, право на персональні дані розглядається як самостійне особисте немайнове право. У науковій літературі це обґрунтовують тим, що право на захист персональних даних забезпечує ефективніший контроль над ширшим колом персональних даних, ніж право на приватність. При цьому вказують на два ключових моменти права на захист персональних даних: по-перше, воно сприяє інформаційній самовизначеності особи, по-друге, зменшує негативний інформаційний вплив на вільний розвиток особистості [123, с. 597].

Відповідно до третього підходу право особи на власні персональні дані розглядається як комплексне утворення у системі особистих немайнових прав, що забезпечують соціальне буття фізичної особи, і, фактично, об'єднує в собі такі, передбачені в ЦК України, особисті немайнові права як право на особисте життя (а саме – його «інформаційну» складову – право на таємницю особистого життя), право на таємницю, право на ім'я, право на власне зображення та право на індивідуальність [12, с. 237].

Попри те, що кожен із вказаних підходів має свою наукову цінність та методологічне обґрунтування, вважаємо за можливе підтримати позицію, відповідно до якої право на персональні дані слід розглядати як самостійне особисте немайнове право. Додатковим аргументом цього є специфіка персональних даних як об'єкта цивільних правовідносин. Мається на увазі те, що персональні дані є за своєю суттю інформацією про фізичну особу, в тому числі – її особисті немайнові блага та ознаки, котрі її індивідуалізують. При цьому особисті немайнові блага, як і права на них, існують незалежно від того, чи відомості про ці блага обробляються як персональні дані. Таким чином, персональні дані не можуть бути повноцінно охоплені змістом права на приватність чи окремо іншим особистим немайновим правом [109].

У зв’язку із цим постає питання про співвідношення права на персональні дані та інших особистих немайнових прав. Це питання вже стало предметом наукового дослідження. Зокрема, І. І. Романюк, встановлюючи зв’язок права на персональні дані та інших особистих немайнових прав, використовує як критерій розмежування ознаку їх об’єкта. Це дало можливість автору прийти до таких висновків. Персональні дані фактично охоплюють: інформацію про особисте життя; таємницю тих чи інших відомостей про особу; охоплюється змістом права особи на власні персональні дані; ім’я; зображення; індивідуальність особи як певну її інформаційну характеристику, що містить дані про зовнішність, звички, манеру одягу, ходи, поведінки людини тощо [12, с. 235–236].

Цілковито погоджуючись із вказаними судженнями, зауважимо, що взаємозв’язок права на персональні дані з іншими особистими немайновими правами проявляється не тільки в їх об’єктах, але й в їх змісті та здійсненні. При цьому необхідно враховувати, що цілеспрямування права на персональні дані є захист особистих немайнових прав фізичної особи, зокрема права на приватність та інших, у зв’язку з обробкою персональних даних. Від так вважаємо вірним твердження, що право на персональні дані не може суперечити праву на приватність та іншим особистим немайновим правам, на захист яких воно спрямовано, звужувати їх зміст та межі здійснення.

Ми підтримуємо позицію, відповідно до якої, особисті немайнові права, що забезпечують індивідуалізацію та приватність фізичної особи, визнаються матеріальними правами (призначеними для забезпечення охорони благ та інтересів, задоволення та захист яких вважається пріоритетним для людини та суспільства), тоді як право на захист персональних даних належить до процедурних прав (діють на різних рівнях, встановлюючи правила, способи та умови ефективного здійснення та захисту відповідних матеріальних прав) [124, с. 66–67].

В основі такого розмежування лежить традиційний для юридичної науки і практики правозастосування поділ галузей права на матеріальні і процесуальні, доповнений вченням про існування процедурних норм, які займають проміжне місце між матеріальними та процесуальними нормами [125, с. 466].Такий підхід підкріплений практикою ЄСПЛ, відповідно до котрої права, закріплені в ЄКПЛ, поділяються на дві групи: субстантивні (матеріальні або «*substantive rights*») і процедурні (процесуальні або «*proceduralrights*») [126, с. 189]. Так, ЄСПЛ визнає, що права, передбачені в національному праві можуть бути матеріальними, процедурними, або як альтернатива, їх поєднанням. Найчастіше питання про співвідношення таких видів прав виникає при застосуванні ст. 6 ЄКПЛ, змістом якої охоплюються випадки, коли матеріальне право, визнане на національному рівні, супроводжується процедурним правом забезпечити здійснення такого права за рішенням суду [127]. Також до процедурних ЄСПЛ відносить право подавати індивідуальні заяви, передбачене ст. 34 ЄКПЛ та, відповідно, зобов'язання держави не перешкоджати жодним чином ефективному здійсненню цього права. Більше того, таке процедурне право може бути пов'язане зі здійсненням матеріального права, викладеного у ст. 6 ЄКПЛ [128].

Значення поділу прав на матеріальні та процедурні є багатоаспектним: 1) Різниця між матеріальними і процедурними правами визначає застосовність і, в деяких випадках, обсяг гарантій, передбачених ст. 6 ЄКПЛ, яка може, в принципі, не мати застосування до матеріальних обмежень права, чинних у національному законодавстві [129]; 2) ЄСПЛ зауважує, що ст. 8 ЄКПЛ може гарантувати право на судовий контроль навіть у випадках, коли дане матеріальне право ще слід було встановити (наприклад, у справі Кох проти Німеччини ЄСПЛ визнав, що рішення інституту про відмову у видачі дозволу на придбання наркотичної речовини, а також відмову адміністративних судів розглянути по суті позов заявника складали втручання в право на повагу його особистого життя, гарантовану ст. 8 ЄКПЛ) [130]; 3) відмінність матеріальних

та процедурних прав впливає також на також на спосіб та розмір компенсації моральної шкоди, зокрема, при встановленні факту порушення процедурного права за відсутності порушення матеріального права, ЄСПЛ визнає, беручи до уваги природу порушення, що визнання судом права порушеним само по собі є достатньою компенсацією завданої моральної шкоди [131].

Додатковим аргументом може слугувати і те, що право на персональні дані не єдине особисте немайнове право, котре в літературі пропонується розглядати як процедурне. Аналогію можна провести: із визнанням права на здоров'я матеріальним правом, а прав пацієнтів процедурними правами [132, с. 230–233]; із розумінням права на здорове довкілля одночасно як матеріального права, самостійного права та процедурного права, котре необхідне для забезпечення інших особистих немайнових прав [133, с 159]. Отже, якщо вчення про поділ прав на матеріальні та процедурні екстраполювати на наш предмет дослідження, то приходимо до висновку, що власне захист персональних даних не спрямований безпосередньо на якесь благо або інтерес, а встановлює механізм здійснення та захисту благ, втілених в інших правах, серед яких права, що забезпечують індивідуалізацію та приватність фізичної особи.

В теорії цивільного права немає єдності щодо кількісного складу прав суб'єкта персональних даних. На цьому тлі можна виділити два підходи. Відповідно до першого із них, права суб'єкта персональних даних розглядають як сукупність суб'єктивних прав, закріплених у законодавстві. Такий підхід отримав нормативне закріплення як на рівні національного законодавства, так і на рівні актів ЄС [32]. Так, ст. 8 Закону України «Про захист персональних даних» відносить права на персональні дані до особистих немайнових, що належать кожній фізичній особі та є невід'ємними і непорушними. До таких прав Закон відносить право:

1) знати про джерела збирання, місцезнаходження своїх персональних даних, мету їх обробки, місцезнаходження або місце проживання (перебування)

володільця чи розпорядника персональних даних або дати відповідне доручення щодо отримання цієї інформації уповноваженим ним особам, крім випадків, встановлених законом;

2) отримувати інформацію про умови надання доступу до персональних даних, зокрема інформацію про третіх осіб, яким передаються його персональні дані;

3) на доступ до своїх персональних даних;

4) отримувати не пізніш як за тридцять календарних днів із дня надходження запиту, крім випадків, передбачених законом, відповідь про те, чи обробляються його персональні дані, а також отримувати зміст таких персональних даних;

5) пред'являти вмотивовану вимогу володільцю персональних даних із запереченням проти обробки своїх персональних даних;

6) 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;

7) 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;

8) звертатися зі скаргами на обробку своїх персональних даних до Уповноваженого або до суду;

9) застосовувати засоби правового захисту в разі порушення законодавства про захист персональних даних;

10) вносити застереження стосовно обмеження права на обробку своїх персональних даних під час надання згоди;

11) відкликати згоду на обробку персональних даних;

12) знати механізм автоматичної обробки персональних даних;

13) на захист від автоматизованого рішення, яке має для нього правові наслідки.

Представники другого підходу розглядають право на персональні дані як єдине комплексне суб'єктивне цивільне право, що об'єднує закріплені в законодавстві правомочності. Так, Дмитренко О. А. вважає, що зміст права на персональні дані можна розглядати як єдність трьох елементів: права на власні дії, права на чужі дії та права на захист. На основі сучасних наукових досліджень під змістом права на персональні дані запропоновано розуміти сукупність позитивних правомочностей особи юридично визнаватись володільцем персональних даних як особистого немайнового блага («благообладання») та використовувати його («благо використання») у межах, передбачених законом, вимагати від усіх інших учасників правовідносин не порушувати дане право, в тому числі правомочність захисту [28, с. 11–12]. Далі вчений обґрунтовує, що правомочність «благообладання» включає в себе пасивну правомочність бути повідомленим з ініціативи суб'єкта, який бажає використовувати персональні дані, перед початком використання про зміст цих даних та засади їх використання (право на повідомлення); а також активну правомочність суб'єкта права у будь-який час, безкоштовно або за розумну плату вимагати доступу до власних персональних даних та інформації про засади їх використання (право на доступ). Під правомочністю «благовикористання» персональних даних автор розуміє юридично забезпечену можливість фізичної особи приймати рішення щодо використання власних персональних даних у суспільних відносинах, що включає в себе право на погодження використання персональних даних до його початку, на безпеку даних та заперечення проти використання, яке відбувається [28, с. 11–12]. Вважаємо такий підхід більш теоретично обґрунтованим, оскільки в ньому враховано, що усі вказані вище правові можливості належать одному і тому ж суб'єкту (суб'єкту персональних даних), їх об'єктом виступає одне і те ж благо

(персональні дані), мають спільне спрямування на захист права на невтручання в особисте життя, у зв’язку з обробкою персональних даних.

У доповнення до цього вважаємо, що правомочності суб’єкта персональних даних доцільно поділяти на дві групи: ті, які реалізуються в абсолютних правовідносинах, тобто коли суб’єкту персональних даних як уповноваженій особі протистоїть невизначене коло зобов’язаних осіб; ті, які реалізуються у відносних правовідносинах, тобто коли суб’єкту персональних даних як уповноваженій особі протистоїть володілець та (або) розпорядник персональних даних. До таких правомочностей, які реалізуються у відносних правовідносинах належать: 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; відкликати згоду на обробку персональних даних. Виокремлення правомочностей, які реалізуються у відносних правовідносинах, має важливе практичне значення, яке полягає в тому, що вимогу про їх здійснення чи захист можна пред’явити тільки до конкретної зобов’язаної особи, володільця та (або) розпорядника відповідно.

Пояснити сказане можна на прикладах судової практики. Зокрема, Вищий Господарський Суд України у справі за позовом фізичної особи-підприємця ОСОБА_2 до Публічного акціонерного товариства «Комерційний банк «ПриватБанк», ґрунтуючись на встановлених обставинах та враховуючи приписи ст. 8, 15 Закону України «Про захист персональних даних», прийшов до висновку про наявність підстав для знищення всіх персональних даних позивача, отриманих відповідачем при відкритті рахунка, підставою для чого є розірвання договору банківського рахунку [134]. В іншій справі Апеляційний суд Львівської області встановив, що в заяві абітурієнта ОСОБА_2 повідомив про себе всі необхідні персональні дані, дав згоду на оприлюднення результатів вступних випробувань та викреслив пункт яким передбачено надання згоди на

використання його персональних даних в Єдиній державній базі з питань освіти та підтвердив це особистим підписом, а також навів мотиви свого непогодження щодо надання такої згоди. Задовольняючи вимогу про захист персональних даних, суд виходив з того, що відповідач не виконав свій обов'язок, який випливає з абз. 1 п. 2 ст. 8 Закону України «Про захист персональних даних». Оскільки в матеріалах справи відсутні будь-які докази на підтвердження того, що ОСОБА_2 були роз'яснені його права, передбачені ст. 8 цього Закону, в тому числі щодо мети отримання згоди на обробку його персональних даних, на отримання інформації про умови надання доступу до персональних даних, зокрема про третіх осіб, яким передаються його персональні дані, механізм автоматичної обробки його персональних даних та інші [135].

Отже, право на персональні дані є особистим немайновим правом, специфіка якого полягає в його: об'єкті – персональні дані; цілеспрямуванні – захист права на приватність та інших особистих немайнових прав у зв'язку з обробкою персональних даних; змісті – активні та пасивні правомочності, а також правомочність захисту, які можуть бути реалізовані як в абсолютних, так і відносних правовідносинах [109].

2.2 Запровадження нових прав суб'єкта персональних даних в контексті гармонізаційних процесів

Враховуючи мету та завдання нашого дослідження, вимоги до обсягу такого виду робіт, а також, те, що значна частина змісту прав суб'єкта персональних даних знайшла належне розкриття на рівні наукової літератури [28; **Error! Reference source not found.**], ми зупинимо свою увагу виключно на тих правомочностях, які потребують нормативного закріплення у зв'язку із реформуванням захисту персональних даних в ЄС, а саме праві на мобільність персональних даних та праві на забуття. Проблематика права на мобільність

взагалі тривалий час залишається поза увагою сучасних дослідників. У процесі підготовки нашого дослідження ми приділяли увагу питанням праву на мобільність персональних даних у окремих публікаціях [136].

Так, право на мобільність персональних даних (*righttodataportability*) закріплено в ст. 20 Загального регламенту про захист даних [49]. Під мобільністю персональних даних розуміється здатність їх перенесення між різними володільцями. Введення цього права обумовлене широким поширенням обробки персональних даних в мережі Інтернет та покликане забезпечити можливість вільного переміщення персональних даних від одного володільця (провайдера, соціальної мережі) до іншого. Це, в свою чергу, сприятиме вільній конкуренції шляхом створення рівних можливостей для існуючих компаній та появи нових компаній на ринку [136].

Зв'язок права на мобільність персональних даних та правових засад захисту економічної конкуренції може бути продемонстрований двома шляхами. По-перше, право на мобільність покликане запобігати зловживанню монопольного становища на ринку шляхом обмеження виробництва, ринків товарів, техніко-технологічного розвитку, інвестицій або встановлення контролю над ними. По-друге, право на мобільність персональних даних надасть споживачам можливість вільного вибору виконавця та перевагу в отримані додаткових послуг від останнього [137]. Проаналізуємо зміст вказаного права відповідно до Загального регламенту про захист даних.

Право особи на мобільність персональних даних охоплює три аспекти. По-перше, суб'єкт має право отримати персональні дані у структурованому форматі, який зазвичай використовується, та у формі придатній для введення в комп'ютер, зберігати їх для подальшого використання на особистих пристроях без передачі іншому володільцю. Вимоги до формату даних встановлюються з метою забезпечення їх подальшого використання, в тому числі шляхом передачі іншому володільцю. Поняття «структурованого формату» законодавчо не визначено, однак, під ним потрібно розуміти формат даних, що мають певну

структуру, відповідно до якої вони можуть бути оброблені. Наприклад, до структурованих можна віднести файли XML-документів [138]. Крім того, формат даних повинен бути таким, що зазвичай використовується, тобто бути достатньо поширеним. У той же час, персональні дані повинні бути надані у формі, яка дозволяє їх автоматичне розпізнавання за допомогою комп'ютерних програм. Зауважимо, що усі вказані вимоги до формату даних не достатньо конкретизовані. Це, з одного боку, зумовить необхідність встановлення відповідності формату даних цим вимогам у кожному окремому випадку, а з іншого, робить основним критерієм відповідності формату даних досягнення ними мобільності, тобто чи можуть вони у відповідному форматі бути перенесені до іншого володільця. Таким чином, Загальний регламент про захист даних сприяє розробці володільцями взаємних форматів даних, які б забезпечували право на мобільність, хоча і не покладає обов'язку використовувати сумісне програмне забезпечення [136].

По-друге, суб'єкт має право безперешкодно перенести отримані у структурованому форматі, який звичайно використовується, та у формі придатній для введення в комп'ютер персональні дані до іншого володільця. Цьому праву кореспондує обов'язок володільця даних не створювати технічних перешкод, які унеможливлюють або ускладнюють перенесення персональних даних. З технічної точки зору володілець персональних даних може запропонувати різні варіанти імплементації права на мобільність. У літературі також можна зустріти широке тлумачення такого обов'язку, яке полягає в необхідності розробки програмного забезпечення, яке б дозволяло експортувати та імпортувати користувачем свої персональні дані [139, с. 344].

По-третє, суб'єкт має право вимагати безпосереднього перенесення персональних даних від одного володільця до іншого, коли це технічно можливо. Відмінність цього права від попередніх полягає в тому, що суб'єкту персональних даних не потрібно самостійно копіювати та завантажувати дані, достатньо тільки звернутися з такою вимогою до володільця персональних

даних. При цьому, це право не обумовлене форматом персональних даних, однак може бути здійснене лише за наявності технічної можливості. Знову ж таки, розуміння «технічної можливості» не розкривається, що є предметом справедливої критики в науковій літературі [140, с. 61], оскільки залишає на розсуд володільця персональних даних запровадження чи незапровадження такої технічної можливості.

Право на мобільність не охоплює весь обсяг персональних даних, які перебувають у володільця, а лише ті з них, котрі були надані (створені) самим суб'єктом персональних даних. До таких належать безпосередньо завантажені чи опубліковані суб'єктом фотографії, статуси, контактна інформація, резюме тощо. Наприклад, поштовий сервіс може дозволяти суб'єкту створювати директорії контактів, друзів, родичів та ширше коло оточення. Оскільки такі дані стосуються суб'єкта, безпосередньо ним створені, то він повинен мати можливість перенести їх до іншого поштового сервісу [141]. Однак, очевидним є те, що персональні дані, що знаходяться у володільця не обмежуються тільки тими, що надані їх суб'єктом. Так, володілець може зберігати статистику використання сайту, створювати дані для аналітичних цілей тощо. Зрозуміло, що такі персональні дані виходять за межі права на мобільність. Однак чітка демаркаційна лінія між двома видами даних (ті, що надаються суб'єктом, та ті, що створюються володільцем) відсутня. Значна частина даних будуть мати, так би мовити, комбіноване походження, особливо це стосується створення персональних даних із використанням програмного забезпечення володільця, (наприклад, графічне відображення користувача (аватарка)).

Більше того, термін «дані, створені суб'єктом» може охоплювати дві категорії: дані безпосередньо та свідомо створені суб'єктом персональних даних (наприклад, поштова адреса, ім'я користувача, вік тощо); дані, створені внаслідок фіксування використання суб'єктом сервісом або пристроєм (наприклад, історія пошуку, дані трафіку тощо). Натомість персональні дані,

створені володільцем, є похідними та базуються на даних, створених самим суб'єктом [142].

Крім того, право на мобільність може бути реалізоване лише за наявності двох умов.

По-перше, право на мобільність персональних даних має місце лише у випадках, коли їх обробка здійснюється на підставі вільного волевиявлення суб'єкта даних, тобто коли: суб'єкт даних недвозначно дав свою згоду; обробка необхідна для виконання контракту, стороною якого є суб'єкт даних, чи для вживання заходів на прохання суб'єкта даних до підписання контракту.

По-друге, право на мобільність персональних даних можливе лише тоді, коли їх обробка здійснюється повністю із застосуванням автоматизованих засобів, тобто включає такі операції, що здійснюються за допомогою автоматизованих засобів: зберігання даних, виконання логічних та (або) арифметичних операцій із цими даними, їхню зміну, знищення, вибірку або поширення [136].

Загальний регламент також визначає межі здійснення права на мобільність персональних даних. Так, здійснення права на мобільність не може перешкоджати реалізації права бути забутим («*right to be forgotten*»), закріпленого в ст. 17 вказаного Регламенту. Тобто, право на мобільність не може бути використано як аргумент для відстрочки чи відмови в задоволені права бути забутим [142]. Під правом бути забутим розуміють право суб'єкта даних вимагати видалення персональних даних, які його стосуються, і відповідний обов'язок видалити ці дані з боку володільця даних у випадку, якщо суб'єкт даних заперечує проти обробки даних і відсутні легітимні підстави для такої обробки, які переважають інтереси, права та свободи суб'єкта даних. Так само здійснення права на мобільність не повинно обмежувати реалізацію інших прав суб'єкта персональних даних та не звільняє володільця від покладених на нього обов'язків.

Також право на мобільність не застосовується, якщо обробка персональних даних необхідна для виконання завдання, здійснюваного в суспільних інтересах, чи при виконанні офіційних повноважень, якими наділений контролер або третя сторона, якій надаються дані. Тобто, право на мобільність персональних даних не повинно перешкоджати володільцям, які обробляють персональні дані, виконуючи свої публічно-правові обов'язки.

Крім того, забороняється здійснювати право на мобільність персональних даних, якщо це може завдати шкоди правам та свободам третіх осіб. Отже, якщо конкретні дані будуть концентрувати персональні дані двох і більше суб'єктів, то права кожного з них повинні бути дотримані.Так само це право не повинне негативно впливати на комерційну таємницю чи інтелектуальну власність і, зокрема, на авторське право, що захищає програмне забезпечення; водночас, врахування цих факторів не повинно призвести до відмови суб'єкта даних у наданні всієї інформації.

Тепер спробуємо з'ясувати правову природу права на мобільність персональних даних шляхом встановлення співвідношення з іншими суб'єктивними цивільними правами. Насамперед, визначимо місце цього права в системі прав, якими наділений суб'єкт персональних даних. Запровадження права на мобільність, перш за все, посилює контроль суб'єкта над своїми персональними даними, які знаходяться у володільця. За своїм змістом право на мобільність найбільш дотичне до права на доступ до своїх персональних даних. Справедливим є твердження, що право на мобільність частково базується на праві суб'єкта персональних даних одержувати будь-які відомості про себе у будь-якого суб'єкта відносин, пов'язаних із персональними даними [143, с. 315]. Однак системний аналіз свідчить, що це різні права, що відрізняються рядом ознак. По-перше, обсяг права на доступ не обмежується лише персональними даними, наданими суб'єктом даним. Доступ реалізується шляхом подання запиту, обов'язковим реквізитом якого є перелік персональних даних, що запитуються. Тобто, суб'єкту даних надається можливість або

вимагати надання усіх персональних даних, які знаходяться у володільця, або конкретизувати їх певним чином. По-друге, реалізація права на доступ до персональних даних не обтяжена вказаними вище вимогами до формату даних [136]. Так, у відповідь на запит щодо доступу до персональних даних фактично надається паперова чи електронна копія персональних даних, які знаходяться у володільця. Тому, навпаки, така копія повинна надаватися у форматі, призначеному для подальшого використання людиною (human-readable), а не для їх автоматичного розпізнавання за допомогою комп'ютерних програм.

Право на мобільність тісно пов'язано із правом 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. Зокрема, володілець персональних даних повинен здійснювати відповідні технічні й організаційні заходи для захисту персональних даних від випадкового або незаконного знищення чи випадкової втрати, зміни, несанкціонованого розкриття чи доступу, зокрема, якщо обробка включає передачу даних через мережу, і від усіх інших незаконних форм обробки. Такі заходи, із врахуванням нинішнього стану речей і вартості їхнього здійснення, повинні забезпечувати рівень безпеки, співвідносний із ризиком, що супроводжує обробку, і з природою даних, що захищаються. Вказані запобіжні заходи повинні бути аналогічними тим, котрі застосовуються при наданні особі доступу до її персональних даних. Наприклад, це може бути вимога вказувати прізвище, ім'я та по батькові, місце проживання (місце перебування) і реквізити документа, що посвідчує фізичну особу, яка виявила бажання реалізувати своє право на мобільність персональних даних. Таким чином, реалізація права на мобільність персональних даних повинна бути узгоджена із забезпеченням права на захист своїх персональних даних [136].

Право на мобільність персональних даних як один із елементів механізму захисту персональних даних спрямоване на захист основоположних прав і свобод людини і громадянина, зокрема права на невтручання в особисте життя, у зв'язку з обробкою персональних даних. Отже, право на мобільність персональних даних може бути охарактеризоване таким чином:

1. Зміст права на мобільність персональних даних включає в себе можливість суб'єкта персональних даних: отримати від володільця персональні дані у форматі, придатному для подальшого використання; передати такі персональні дані іншому володільцю; вимагати від володільця безпосередньої передачі таких персональних даних іншому володільцю при технічній можливості.

2. Межі права на мобільність персональних даних обумовлені: предметом (мобільності підлягають лише персональні дані, створені самим суб'єктом); умовами (мобільність персональних даних можлива лише, якщо персональні дані обробляються на підставі вільного волевиявлення суб'єкта даних із застосуванням автоматизованих засобів); межами здійснення (право на мобільність не може здійснюватися на шкоду іншим правам суб'єкта персональних даних, правам інших суб'єктів персональних даних, правам та свободам третіх осіб).

3. Право на мобільність слід розглядати як окреме право в системі прав суб'єкта персональних даних, відмінне від права на доступ, права на забуття, та тісно пов'язане з правом на захист персональних даних [136].

Наступним правом суб'єкта персональних даних, яке вводиться Загальним регламентом про захист даних [49], є так зване право на забуття. Це право ще не має усталеної традиції терміновживання. Так, для його позначення інколи використовують конструкції: «право бути забутим», «право на стирання», «право на видалення інформації», «право забувати»; або англомовні варіанти: «right to be forgotten», «right to erasure», «right to oblivion» тощо. Спробуємо дослідити правову природу вказаного права.

Для розуміння правової природи права на забуття необхідно дослідити ґенезу його нормативного закріплення. Право на забуття походить від французького «droit à l'oubli», під яким розуміють цивільно-правовий спосіб захисту особистих немайнових прав публічної особи, спрямований на захист таємниці минулого і життєвого спокою того, хто вирішив не присвячувати себе публічним справам. Цей спосіб захисту передбачає, що стосовно особи, яка набула статусу публічної особи не звласної ініціативи, умова корисності інформації, в першу чергу, означає заборону розголошення поточних подій життя особи, яка була предметом інформаційних сюжетів у минулому. Французькі суди досить стримано підходять до задоволення вимоги про забуття, оскільки в багатьох випадках застосовують принцип, відповідно до якого особа не може вимагати заборони публікації фактів щодо колишнього злочину, що викликав обурення у суспільстві. Разом із тим, даний підхід піддається критиці, обґрунтованій таким чином: якщо особа не перебуває більше в центрі суспільної уваги, таке нагадування про колишній злочин погіршить можливості реінтеграції у суспільство [144, с. 45]. У 2010 р. у Франції була прийнята Хартія про право на забуття (Charte du droit à l'oubli dans les site collaboratifs et les moteurs derecherche), що стала першою спробою уряду Франції «вбудувати» концепцію «права на забуття» в Інтернеті в національну систему права [145, с. 162]. Таким чином, при застосуванні такого способу захисту, як право на забуття, важливим є врахування низки факторів: суб'єктивного – наявність підтвердженої поведінкою волі самої фізичної особи, що виражає небажання бути в центрі суспільної уваги, та об'єктивного – пов'язаного із відсутністю (зникненням) виправданого суспільного інтересу, а відтак – легітимності та корисності втручання в особисте життя публічної особи [146, с. 199].

У свою чергу, право на забуття визнається і на рівні інших національних правових систем. Так, в Італії «право на забуття» («diritto all'oblio») розглядається судовою практикою, передусім, із точки зору права кожного

громадянина на видалення з архіву новин певних біографічних фактів, здатних завдати шкоди його честі або репутації, якщо ці факти більше не є актуальними чи не становлять громадського інтересу, або на нерозповсюдження (без певних причин) інформації про свої минулі судові процеси [145, с. 162]. У Німеччині право на забуття інтерпретується як один із елементів змісту загального особистого немайнового права («Allgemeine Persönlichkeitsrecht») [147], який найчастіше стосується засуджених за вчинення злочину, ресоціалізація яких переважає право суспільства знати біографію злочинця [148, с. 23]. Основа такого підходу була закладена рішенням Федерального Конституційного Суду, в якому було визнано існування часових рамок, коли повідомлення про поточні події, яке в принципі є допустимим, стає згодом неприйнятним [149]. При встановленні таких часових рамок Суд враховував наступні положення. По-перше, звичайно, такі часові рамки не можуть бути встановлені в місяцях і роках для того, щоб підходити для усіх випадків. По-друге, вирішальним критерієм повинно бути те, чи відповідне повідомлення ймовірно заподіє засудженому значну нову або додаткову шкоду, порівняно з інформацією, яка вже є доступною.

У Сполучених Штатах «право на забуття» в основному розглядається як таке, що суперечить Конституції США і судова практика виходить із того, що вимогу про видалення інформації можна відхилити, ґрунтуючись на Першій поправці до Конституції США [150]. Однак в окремих штатах закріплені одиничні прояви права на забуття. Так, загалом у США забезпечується право неповнолітніх злочинців подати до суду заяву про вилучення обвинувального вироку суду у справах неповнолітніх [151, с. 379–380]. Також у вересні 2013 року в Каліфорнії прийняли закон, який наділяє неповнолітніх правом видаляти або вимагати видалення контенту або інформації, викладеної ними на інтернет веб-сайті, інтернет-порталі чи застосунках, окрім випадків, коли контент або інформація викладені третьою особою, інші положення закону вимагають

збереження цього контенту чи інформації, контент або інформація були знеособлені [152].

Підґрунтя права на забуття отримало своє нормативне закріплення на міжнародному рівні. Прикладом цього є окремі положення, що містяться в Конвенції про захист осіб у зв'язку з автоматизованою обробкою персональних даних [71], зокрема: 1) персональні дані, що піддаються автоматизованій обробці, повинні зберігатись у формі, що дозволяє ідентифікацію суб'єктів даних не довше, ніж це необхідно для мети, для якої такі дані зберігаються (п. е ч. 1 ст. 5); 2) будь-якій особі надається можливість вимагати у відповідних випадках виправлення або знищення таких даних, якщо вони оброблялися всупереч положенням внутрішнього законодавства, що запроваджують основоположні принципи, визначені у статтях 5 і 6 цієї Конвенції (п. с ч. 1 ст. 8).

Право на забуття знаходить своє визнання також в практиці ЄСПЛ, яка відображає наступні правові позиції:

1) публічна інформація може відноситися до сфери приватного життя у разі, коли вона систематично збирається і зберігається в досьє, що знаходяться у розпорядженні влади. Це ще вірніше у разі, коли йдеться про інформацію, що зачіпає віддалене минуле фізичної особи (Rotaru v. Romania [85]) – тривале зберігання персональних даних підпадає під дію ст. 8 ЄКПЛ та охоплюється змістом права на приватне життя;

2) слід враховувати характер і давність персональних даних при визначенні того, чи їх тривале зберігання підкріплене підставами, доречними і достатніми з точки зору захисту національної безпеки (Segerstedt-Wiberg and others v. Sweden [88]) – тривале зберігання персональних даних повинно мати додаткові підстави;

3) тривале зберігання інформації, згідно якої фізична особа в 1969 році відстоювала ідею насильницького опору поліції під час проведення демонстрацій, мало під собою підстави, які хоча і мають відношення до

справжньої справи, але не можуть вважатися достатніми після закінчення тридцяти років(Segerstedt-Wiberg and others v. Sweden [88]) – тривале зберігання інформації може спричинити непропорційне втручання держави в реалізацію права на приватне життя;

4) необмежене у часі зберігання даних криміналістичного обліку навряд чи відповідає вимогам ст. 8 ЄКПЛ, за відсутності зрозумілого та детального регулювання, серед іншого, тривалості зберігання персональних даних та умов, при яких вони можуть бути знищені (M.M. v. The United Kingdom [153]) – строк зберігання персональних даних та умови їх дострокового знищення повинні бути чітко визначені;

5) при вирішенні питання щодо заборони публікації фотографії засудженої особи після її умовно-дострокового звільнення, має бути врахований не лише час, який минув з моменту засудження і звільнення, але й характер злочину, зв'язок між змістом повідомлення і показаної фотографії, а також повнота і коректність тексту, що супроводжується (Österreichischer Rundfunk v. Austria [154]) – темпоральні рамки є лише однією з умов, які враховуються при встановленні балансу між захистом персональних даних та правом на свободу слова.

Крім того, окремі елементи права на забуття були закріплені в Директиві 95/46/ЄС, серед яких: 1) персональні дані повинні бути точними і, якщо необхідно, оновлюватися; слід вжити всіх розумних заходів, щоб гарантувати, що дані, які є неточними чи неповними, з урахуванням цілей, заради яких вони були зібрані чи заради яких вони надалі обробляються, стиралися чи виправлялися (п. d ст. 6); 2) персональні дані повинні зберігатися у формі, що дозволяє встановлювати особу суб'єктів даних не довше, ніж це необхідно для цілей, заради яких дані були зібрані чи заради яких вони надалі обробляються. Держави-члени встановлюють відповідні гарантії для персональних даних, що зберігаються упродовж більш тривалих періодів із метою історичного, статистичного чи наукового використання (п. e ст. 6);

3) кожен суб'єкт персональних даних має право вимагати від володільця стирання персональних даних, обробка яких не відповідає положенням даної Директиви, зокрема, через неповноту чи неточність даних (п. b ст. 12); 4) кожен суб'єкт персональних даних має право вимагати від володільця повідомлення третім сторонам, яким були надані дані, про будь-яке виправлення, стирання чи блокування, якщо це можливо чи не вимагає непропорційних зусиль (п. c ст. 12); 5) суб'єкт персональних даних має право заперечувати в будь-який час на безсумнівних законних підставах, пов'язаних із його конкретною ситуацією, проти обробки даних, які його стосуються, за винятком випадків, коли інше передбачено національним законодавством. За наявності обґрунтованого заперечення в розпочатій контролером обробці більше не можуть використовуватися такі дані (п. a ст. 14).

Таким чином, право на забуття знаходить своє обґрунтування на рівні принципів, що стосуються якості даних, а його окремі елементи розкриваються через зміст прав суб'єкта персональних даних на доступ та на заперечення. Аналіз вказаних положень, а особливо меж їх застосування, дає можливість прийти до висновку, що повноцінного права на забуття Директива 95/46/ЄС не закріплювала. По-перше, обумовлення права на забуття темпоральними рамками існування цілей обробки персональних даних (п. e ст. 6) є малозастосовним на практиці, оскільки постійний розвиток сфери електронної комерції зумовлює збирання та використання персональних даних для цілей, не обмежених у часі [155, с. 319]. По-друге, «неповнота» та «неточність» персональних даних як умови видалення персональних даних (п. d ст. 6; п. b ст. 12) є оціночними поняттями, що робить здійснення права на забуття залежним від кожного окремого випадку. По-третє, обґрунтоване заперечення проти обробки персональних даних (п. a ст. 14) обмежено випадками, коли обробка необхідна для виконання завдання, здійснюваного в суспільнихінтересах,чи при виконанні офіційних повноважень, котрими наділений контролер або третя

сторона, або в цілях законних інтересів, переслідуваних контролером чи третьою стороною або сторонами, для яких надаються дані.

Подібно до Директиви 95/46/ЄС Закон України «Про захист персональних даних» також частково визнає право на забуття. Так, в Законі закріплюється: право суб'єкта персональних даних пред'являти вмотивовану вимогу щодо знищення своїх персональних даних будь-яким володільцем та розпорядником персональних даних, якщо ці дані обробляються незаконно чи є недостовірними (п. 6 ч. 2 ст. 8); підстави та умови видалення або знищення персональних даних (ч. 2, 3 ст. 15).

Вказані положення Директиви 95/46/ЄС в подальшому лягли в основу рішення Суду Європейського Союзу від 13 травня 2014 року у справі Google Spain SL, Google Inc. v. Agencia Española de Protección de Datos (AEPD), Mario Costeja González [156], яке стало чи не першим судовим рішенням, що визнало право на забуття в контексті персональних даних. Відповідно до обставин справи, громадянин Іспанії вимагав, щоб компанія Google видалила посилання на оголошення 1998 р. в іспанській газеті про продаж його будинку на аукціоні в рахунок сплати боргу, котрий був згодом ним погашений, як результат при пошуку його імені, і щоб газета видалила саме оголошення зі свого веб-сайту. У підсумку Суд Європейського Союзу ухвалив, що пошукові системи контролювали персональні дані відповідно до Директиви 95/46/ЄС; що Директива 95/46/ЄС застосовується у разі операцій, що здійснюються пошуковою системою на території країн-членів ЄС; і що люди мають право за певних умов просити видалити з пошукових систем посилання з особистою інформацією про них. Суд Європейського Союзу зобов'язав Google видалити посилання на інформацію в результатах пошуку, як просив громадянин, але ухвалив, що контент основного новинного архіву на веб-сайті газети міняти немає необхідності. Таким чином, громадяни Євросоюзу отримали право звернутися при певних обставинах до будь-якої пошукової системи із запитом про видалення неадекватної, невідповідної дійсності або застарілої інформації,

що містить їх імена або інші персональні дані, а вказана справа стала першим судовим прецедентом у цьому питанні. Важливо, що Суд також ухвалив, що ця справа не є універсальною, а право на забуття – абсолютним: рішення в аналогічних справах виноситимуться на основі конкретних обставин, щоб виключити їх протиріччя з фундаментальними правами людини (свободи слова і преси) [145, с. 164].

Значення вказаного рішення Суду Європейського Союзу можна продемонструвати тими триваючими наслідками загального характеру, які воно спричинило. У результаті рішення Суду Європейського Союзу користувачі Інтернету країн ЄС на підставі вказаного судового прецеденту отримали можливість звернутися до пошукових сервісів із запитом про видалення з пошукових результатів невідповідної реаліям, застарілої або такої, що містить персональні відомості інформації у вигляді інтернет-посилань [157, с. 107]. Наприклад, Google 29 травня 2014 р. запровадив електронну форму запиту на видалення контенту, проіндексованого в Google Пошуку, на основі закону ЄС про захист даних. Вказаний запит повинен містити: ім’я, що використовується при пошуку; розкриття того, яким чином ця сторінка стосується змісту запиту; пояснення того, чому зміст цієї сторінки є незаконним, неточним або неактуальним. До запиту додається розбірлива електронна копія документу, що посвідчує особу, персональні дані якої підлягають видаленню. Станом на 23 липня 2017 р. за результатами розгляду таких запитів було видалено 780 485 URL-адрес, що складає 43,2 % від загальної кількості адрес, що були предметом таких запитів [158]. Крім того, зазначається, що рішення Суду ЄС матиме наслідки не лише в межах ЄС, але і за його межами, зокрема стосовно компаній, які здійснюють обробку персональних даних цих громадян Європейського Союзу за його межами [159, с. 97].

Таким чином, проаналізоване рішення Суду ЄС закріпило право фізичних осіб вимагати видалення їх персональних даних із результатів пошуку, що здійснюються за їх ім’ям. Однак, навряд чи мова може йти про визнання

повноцінного права на забуття, якщо брати до уваги межі, встановлені в самому рішенні: 1) за об'єктом – видаленню підлягають лише результати, які формуються пошуковою системою інтернету, тобто лише посилання на відповідні сайти, де знаходяться персональні дані; 2) за суб'єктом – вказане рішення поширюється лише на пошукові системи Інтернету і не може бути застосоване до інших володільців персональних даних.

Наступним кроком ґенези права на забуття стало його закріплення в ст. 17 Загального регламенту про захист даних [49]. Право на забуття розглядається як одна з гарантій того, що персональні дані не будуть зберігатися довше, ніж необхідно. Із цією метою повинні бути встановлені часові рамки, поза якими персональні дані підлягають видаленню чи перегляду. Так само суб'єкт персональних даних повинен мати право на забуття, у випадках, коли збереження таких даних порушує європейські стандарти захисту персональних даних. Зокрема, суб'єкт персональних даних повинен мати право на те, щоб його чи її персональні дані були видалені й більше не оброблялися у випадках, коли персональні дані більше не потрібні для цілей, для яких вони були зібрані або оброблені іншим чином; коли суб'єкт персональних даних відкликав свою згоду або заперечує щодо обробки персональних даних, що стосуються його, або там, де відповідна обробка його персональних даних не відповідає європейським стандартам захисту персональних даних. Це право застосовується також, коли суб'єкт персональних даних дав свою згоду, як неповнолітній, і не повною мірою усвідомлював ризики від обробки, і надалі хоче видалити особисті дані, особливо в Інтернеті. Суб'єкт даних повинен мати можливість здійснювати це право, навіть і після досягнення повноліття. Проте подальше збереження персональних даних має бути законним, де це необхідно, для здійснення права на свободу слова та інформації, для цілей виконання володільцем персональних даних передбаченого законом обов'язку, для архівних цілей, наукових та історичних досліджень або статистичних цілей або для цілей судового захисту. Праву на забуття кореспондує обов'язок володільця

персональних даних, який зробив персональні дані загальнодоступними, інформувати інших осіб, які обробляють такі персональні дані, про видалення будь-яких посилань, копій або реплікацій цих персональних даних. При цьому, володілець повинен вжити розумних заходів, із урахуванням наявних технологій і засобів, наявних в розпорядженні володільця, включаючи технічні заходи, щоб сповістити інших осіб, які здійснюють обробку персональних даних, що є предметом запиту суб'єкта даних.

Розкриваючи далі правову природу права на забуття, потрібно вказати, що необхідність його закріплення обумовлена власне сучасним рівнем розвитку інформаційних технологій. Зокрема, Кірон О'Хара порівнює право на забуття з діловодством минулого. У дні, коли Інтернет не був повсюди доступний людям як результат розвитку технологій, багато відомостей зберігалися на друкованих носіях, але також були доступні, хоча доступ до них не завжди можна було отримати з різних причин, наприклад, через територіальну віддаленість від місця, де зберігалися ті або інші архіви. Проводячи паралелі з минулим, вона стверджує про логічність та історичну необхідність права на забуття [160, с. 74]. Інші автори йдуть ще далі й навіть розглядають право на забуття як відповідь на розповсюдження електронних засобів масової інформації в нашому житті з їх настільки широким впливом, що можна говорити про схрещування нашого офлайн та онлайн існування. Таке схрещене існування нашого біологічного та цифрового життя починає впливати на взаємодію та кореспондування наших прав та обов'язків, що не проявляються там, де наше цифрове, онлайн життя є незначним [161, с. 19].

Важливо також визначити місце права на забуття в системі суб'єктивних цивільних прав. Складність та неоднозначність цього питання випливає вже із термінології, котра вжита у Загальному регламенті про захист даних [49]. Так, у ст. 17 використовується два терміни: право на знищення («right to erasure») та право на забуття («right to be forgotten»). Така подвійна термінологія критикується в наукових дослідженнях. Аргументується це тим, що фактично

нове право на забуття є по суті уточненням та посиленням існуючого права на знищення персональних даних, а тому відсутня необхідність створювати нове право під новим ім'ям. В силу цього висувається припущення, що переваги нових положень можуть бути досягнені, залишаючись під заголовком «права на знищення» без додаткового посилання на «право на забуття» [162, с. 210]. Однак, цьому є просте пояснення, яке полягає в тому, що право на забуття проявляється на зрізі двох площин: особистих немайнових прав та законодавства про захист персональних даних [163, с. 180]. Таким чином, досліджуване право може ґрунтуватись на особистих немайнових правах фізичної особи, і в цьому контексті його слід розглядати як «право на забуття», або воно може ґрунтуватись на механізмі захисту персональних даних, і в такому разі розглядатись як «право на знищення персональних даних».

Таке неоднозначне нормативне закріплення та багатогранність правової природи призвели до наукової дискусії щодо встановлення співвідношення права на забуття з іншими особистими немайновими правами. З цього приводу можна виділити кілька основних підходів. Перший, найбільш традиційний із них, полягає в тому, що право на забуття розглядається як правомочність права на приватність. Обґрунтовується це тим, що кінцевою метою захисту персональних даних є забезпечення дотримання права на недоторканість приватного життя. Останнє твердження навіть знаходить своє легальне закріплення в ст. 1 Конвенції про захист осіб у зв'язку з автоматизованою обробкою персональних даних [71]. Другий підхід розглядає право на забуття як елемент права на захист персональних даних, при цьому останнє виокремлюється у самостійне право, поряд із правом на недоторканність приватного життя. Аргументується це тим, що значення права на забуття не вичерпується життєвою необхідністю і тісним зв'язком захисту персональних даних із захистом приватності. Право на захист персональних даних у різних обставинах також необхідне і для забезпечення низки інших основних прав, таких як право на честь і гідність, свободу зібрань, свободу пересування,

свободу думки, свободу вираження поглядів, захист від дискримінації, трудові та економічні права [164, с. 92]. Як аргумент на користь цього тезису можна привести Хартію основних прав Європейського Союзу [103], що закріплює два окремих права: повагу до приватного та сімейного життя (ст. 7) та захист персональних даних (ст. 8). Третій, найбільш радикальний підхід, визнає право на забуття незалежним правовим механізмом або особистим немайновим правом sui generis [165, с. 35].

Наше бачення місця права на забуття в системі особистих немайнових прав базується на двох вихідних положеннях. Ми відштовхуємося від того, що в системі особистих немайнових прав виділяють серед інших дві групи прав: особисті немайнові права, що забезпечують індивідуалізацію фізичних осіб у суспільстві, та особисті немайнові права, що забезпечують приватність фізичної особи [6, с. 410–446, 474–479]. Взаємозв'язок права на забуття та права на приватність найбільш чітко простежується у випадках, коли інформація про особисте життя фізичної особи була правомірно публічно оприлюднена, а згодом підстава такого оприлюднення знівелювалася [163, с. 181]. Крім того, сам факт обробки персональних даних відповідним володільцем може охоплюватись змістом права на приватність суб'єкта таких даних. У той же час, право на забуття вдосконалює та розширює розуміння прав, що забезпечують індивідуалізацію фізичних осіб. Так, право на забуття надає особливого значення не тільки праву відрізнятись від інших, але також праву бути іншим стосовно свого минулого. Таким чином, право на забуття відіграє важливу роль у забезпеченні можливості змінити свою індивідуальність [124, с. 69].

Зміст права на забуття полягає у можливості суб'єкта персональних даних вимагати від володільця видалення даних, що його стосуються. Цьому праву кореспондує обов'язок володільця видалити персональні дані без надмірної затримки. Крім того, у випадках, коли володілець зробив персональні дані загальнодоступними, він зобов'язаний, з урахуванням наявних технологій і вартості здійснення, вжити розумних заходів, включаючи технічні заходи, щоб

проінформувати інших осіб, які здійснюють обробку таких персональних даних, що суб'єкт персональних даних запросив видалити будь-які посилання на використання або копіювання або тиражування цих персональних даних. Для реалізації права на забуття необхідна одна із підстав, передбачених в ч. 3 ст. 17 Загального регламенту про захист даних:

1) персональні дані більше не потрібні для цілей, для яких вони були зібрані або оброблялися іншим чином;

2) суб'єкт персональних даних відкликає згоду, що була підставою для їх обробки, за умови відсутності інших законних підстав для обробки таких даних;

3) суб'єкт персональних даних заперечує проти їх подальшої обробки, за умови відсутності інших законних підстав для обробки таких даних, котрі є більш значимими, ніж інтереси суб'єкта персональних даних;

4) персональні дані оброблялися незаконно;

5) персональні дані підлягають видаленню відповідно до обов'язку володільця, передбаченого законодавством;

6) персональні дані, були зібрані відповідно до згоди, наданої неповнолітнім.

При цьому слід враховувати, що право на забуття не є абсолютним, а його здійснення фактично щоразу призводить до зіткнення охоронюваних законом інтересів. Так, право на забуття, як було встановлено, спрямоване на захист не тільки приватності та індивідуальності фізичної особи, але й її права на самовизначення, права на честь, гідність та репутацію тощо. З іншого боку, здійснення права на забуття повинно бути обмеженим у випадках, коли обробка персональних даних здійснюється: для реалізації права на свободу думки і слова, на вільне вираження своїх поглядів і переконань; для здійснення повноважень володільця персональних даних, наданих йому відповідно до закону; для виконання володільцем персональних даних передбаченого законом обов'язку; для цілей охорони здоров'я, встановлення медичного діагнозу, для

забезпечення піклування чи лікування або надання медичних послуг за умови, що такі дані обробляються медичним працівником або іншою особою закладу охорони здоров'я, на якого покладено обов'язки щодо забезпечення захисту персональних даних та на якого поширюється законодавство про лікарську таємницю; для цілей архівної справи, в тому числі щодо доступу до архівів репресивних органів комуністичного тоталітарного режиму 1917-1991 років; для цілей наукових або історичних досліджень; для статистичної діяльності; для обґрунтування, задоволення або захисту правової вимоги (ч. 3 ст. 17 Загального регламенту про захист даних).

Таким чином, при здійсненні права на забуття необхідно завжди встановлювати баланс між колідуючими правами та приймати рішення з урахуванням конкретних обставин кожної окремої справи, дотримуючись при цьому принципу пропорційності. Рекомендується використовувати такі критерії при встановлені такого балансу [166]:

1) Чи належить суб'єкт персональних даних до публічних осіб, тобто осіб, які обіймають державні посади і (або) користуються державними ресурсами, а також усі ті, хто відіграє певну роль у суспільному житті (у галузі політики, економіки, мистецтва, соціальній сфері, спорті чи в будь-якій іншій галузі) [167]. У зв'язку з цим, межа правомірної обробки персональних даних щодо політичного діяча чи іншої публічної особи є значно ширшою, ніж окремої пересічної особи;

2) Чи є суб'єкт персональних даних неповнолітнім, чи був неповнолітнім на момент первинної обробки персональних даних. Важливість цього критерію випливає з ч. 2 ст. 24 Хартії основних прав Європейського Союзу [103], відповідно до якої, при здійсненні будь-яких дій відносно дітей як публічною владою, так і приватними установами вищі інтереси дитини повинні розглядатися як пріоритетні;

3) Чи є персональні дані повними, точними та достовірними. Цей критерій обумовлений загальними вимогами до обробки персональних даних,

однак, якщо має місце спір про достовірність персональних даних, наприклад, у випадках пред'явлення позову про спростування недостовірної інформації, право на забуття не може бути здійснено до вирішення такої справи по суті.

4) Чи є персональні дані адекватними та ненадмірними. При цьому слід враховувати давність персональних даних, оскільки чим більше часу минуло з моменту збирання персональних даних, тим менше вони є релевантними теперішньому стану речей. Також слід брати до уваги те, чи стосуються персональні дані особистого життя суб'єкта або його участі в суспільному житті. Так, персональні дані, що стосуються здійснення особою, яка займає посаду, пов'язану з виконанням функцій держави або органів місцевого самоврядування, посадових або службових повноважень, не можуть вважатися надмірними. Крім того, важливим є те, чи містяться персональні дані в інформації, яка за своїм характером є фактичним твердженням чи оціночним судженням. Оціночні судження, за винятком наклепу та оціночних суджень, що принижують гідність, честь чи ділову репутацію, а також інші особисті немайнові права фізичної особи, не можуть вважатися надмірними;

5) Чи належать персональні дані до так званих чутливих категорій даних. Такі персональні дані користуються підвищеним захистом, а їх обробка повинна відповідати особливим вимогам (ст. 7 Закону України «Про захист персональних даних»);

6) Чи заподіює обробка персональних даних шкоду їх суб'єкту, чи створює загрозу заподіяння такої шкоди. Хоча шкода не є умовою здійснення права на забуття, її наявність значно впливає на встановлення балансу між колідуючими інтересами;

7) Чи давав суб'єкт персональних даних згоду на їх обробку, чи обробка здійснювалась на інших підставах. Якщо єдиною підставою обробки персональних даних була згода їх суб'єкта, яка згодом була відкликана, така обробка повинна бути припинена, а персональні дані підлягають видаленню.

Перелік таких критеріїв не може вважатися вичерпним, а тому повинні бути враховані й інші обставини, що мають значення для встановлення балансу між правом на забуття та колідуючими йому правами.

Завершуючи, наголосимо, що прогрес сучасних технологічних систем активно впливає на формування нових правових можливостей суб'єктів цивільно-правових відносин. Особливо широко таке коло правових інтересів виникає у інтернет-користувачів. Яскравим прикладом, може бути справа за позовом групи мешканців штату Іліной (США) до компанії Facebook, яка погодилась на укладення мирової угоди та виплати значної суми відшкодування через неправомірне збирання таких персональних даних користувачів, як біометричне зображення їх обличчя на фотографіях [168].

Динаміка розвитку правового регулювання інтернет-відносин лише підтверджує необхідність формування у національній цивільно-правовій доктрині теоретичних та прикладних засад запровадження категорії «цифрові права», органічною частиною яких ми бачимо «цифрові» засоби забезпечення права на приватність та права на персональні дані. Фактично, відбувається маштабне «перетікання» персональних даних у технологічну сферу інформаційних інтернет-відносин. Яскравим прикладом цього процесу стають багаточисельні реєстри та бази даних із доступом через мережу Інтернет.

Під такими «цифровими правами» ми пропонуємо розуміти відображені у інтернет-середовищі правові можливості інтернет-користувачів реалізовувати свої права та інтереси, закріплені у національному законодавстві та міжнародно-правових актах, із врахуванням особливостей породжених технологічними можливостями Інтернет-мережі.

Однією з таких сучасних правомочностей виступає право суб'єкта персональних даних на визначення порядку використання її «цифрових» активів та персональних даних, які у них містяться у випадку відкриття спадщини. При цьому вирішення даного питання може відбуватися і шляхом

включення відповідної вказівки до змісту письмової вказівки як частини заповіту.

2.3 Участь у відносинах щодо персональних даних осіб, які їх обробляють

Центральним серед суб'єктів, які обробляють персональні дані, є володілець персональних даних. При термінологічному аналізі, насамперед, звертають увагу на те, що Конвенція про захист осіб у зв'язку з автоматизованою обробкою персональних даних та Загальний регламент про захист даних використовують інший термін – «контролер» («controller»). У науковій літературі стверджується, що термін «контролер» є точнішим, ніж просто «володілець бази персональних даних», і в якості аргумента наводиться міркування про те, що «питання права власності на інформацію зараз фактично опинилися за межами правового поля» [169, с. 193–194]. Загалом погоджуючись із таким твердженням, зазначимо, що використання терміна «володілець», в принципі, узгоджується з «пропієтарною» концепцією змісту особистих немайнових прав [6 с. 139–141], однак не повинно тлумачитись як закріплення речового права «володіти» персональними даними.

Поняття «володілець» отримало своє легальне визначення на різних рівнях: Конвенція про захист осіб у зв'язку з автоматизованою обробкою персональних даних – фізична або юридична особа, державний орган, установа чи будь-який інший орган, що уповноважений відповідно до національного законодавства вирішувати, яким повинно бути призначення файлу даних для автоматизованої обробки, які категорії персональних даних повинні зберігатися та які операції повинні здійснюватися з ними (п. d ч. 1 ст. 2); Загальний регламент про захист даних – фізична чи юридична особа, орган публічної влади, агентство чи інший орган, котрий самостійно чи спільно з іншими визначає цілі та засоби опрацювання персональних даних; якщо цілі та засоби

такого опрацювання визначаються законодавством Союзу чи держави-члена, власне контролер або спеціальні критерії його призначення можуть бути передбачені законодавством Союзу чи держави-члена (п. 7 ст. 4); Закон України «Про захист персональних даних» – фізична або юридична особа, яка визначає мету обробки персональних даних, встановлює склад цих даних та процедури їх обробки, якщо інше не визначено законом (абзац третій ч. 1 ст. 2). Якщо синтезувати ці дефініції, то можна виокремити три ознаки володільця персональних даних: 1) власна правосуб'єктність; 2) можливість діяти самостійно чи разом з іншими суб'єктами; 3) можливість визначати мету та інші умови обробки персональних даних. Розглянемо ці ознаки більш детально.

Значення такої ознаки як наявність у володільця власної правосуб'єктності полягає у визначенні суб'єкта, відповідального за дотримання законодавства про захист персональних даних, на якого покладаються обов'язки, що кореспондуються правам суб'єкта персональних даних [170]. Володільцями можуть бути як фізичні, так і юридичні особи. Звертає на себе увагу ч. 2 ст. 4 Закону України «Про захист персональних даних», котра обмежує коло володільців (так само як і розпорядників) лише фізичними особами-підприємцями. Враховуючи правила обмеження дії вказаного Закону, відповідно до якого дозволяється обробка персональних даних без застосування його положень, якщо така обробка здійснюється фізичною особою виключно для особистих чи побутових потреб, вважаємо, що ч. 2 ст. 4 підлягає поширювальному тлумаченню. Так, до володільців персональних даних також слід включити: фізичну особу, яка провадить незалежну професійну діяльність, тобто бере участь у науковій, літературній, артистичній, художній, освітній або викладацькій діяльності, діяльність лікарів, приватних нотаріусів, приватних виконавців, адвокатів, арбітражних керуючих (розпорядників майна, керуючих санацією, ліквідаторів), аудиторів, бухгалтерів, оцінщиків, інженерів чи архітекторів, осіб, зайнятих релігійною (місіонерською) діяльністю, іншою подібною діяльністю; фізичну особу, яка

обробляє персональні дані не для особистих чи побутових потреб. Коло юридичних осіб, які можуть бути володільцями, також сформульовано досить широко та включає підприємства, установи і організації усіх форм власності, органи державної влади чи органи місцевого самоврядування.

Друга ознака вказує на можливість існування множинності осіб на стороні володільця. Ця ознака відсутня в національному законодавстві про захист персональних даних, але не суперечить йому. Тобто, у разі, коли два і більше суб'єкти визначають цілі та засоби обробки персональних даних, такі суб'єкти є співволодільцями. Участь співволодільців у спільному визначенні цілей та засобів обробки персональних даних може набувати різних форм та не обов'язково повинна бути рівною. Наприклад, можна виділити такі випадки: 1) ті самі дані окремо зберігаються у декількох суб'єктів; 2) рівним доступом до однієї бази даних користуються два суб'єкти і кожен може приймати на свій розсуд рішення щодо обробки наявних у ній даних; 3) двоє чи більше суб'єктів мають різні рівні доступу до однієї бази даних і кожен може приймати рішення щодо обробки наявних у ній даних, до яких він має доступ [81, с. 27–28]. У цих та інших випадках співволодільці за взаємною згодою можуть розподілити між собою права та обов'язки при обробці персональних даних, а також відповідальність за порушення прав суб'єкта персональних даних. При цьому суб'єкт персональних даних може здійснювати та захищати свої права відносно кожного зі співволодільців.

Третя ознака, а саме можливість визначати мету та інші умови обробки персональних даних, є конститутивною ознакою володільця персональних даних. Така можливість може бути прямо передбачена в законодавстві, випливати зі звичаїв ділового обороту або обумовлюватися фактичними обставинами справи. При цьому, аналіз визначення поняття «володілець» свідчить, що воно охоплює випадки як правомірної обробки персональних даних, так і обробку персональних даних за відсутності правової підстави, а також обробку, котру здійснюють у протиправний спосіб. Використавши це

твердження як критерій, можна виділити види володільців: 1) титульний володілець – особа, яка набула статусу володільця безпосередньо чи опосередковано на підставі норм права; 2) фактичний законний володілець – особа, яка набула статусу володільця в силу фактичних обставин за умови дотримання принципів обробки персональних даних; 3) фактичний незаконний володілець – особа, яка набула статусу володільця за відсутності правомірної підстави для обробки персональних даних. Такий поділ має не тільки теоретичне значення, але й може бути врахований при визначенні відповідальності володільця за порушення прав суб'єкта персональних даних.

Важливою особливістю поняття «володілець» є його автономність у тому розумінні, що, хоча інші норми права, в тому числі цивільно-правових інститутів, можуть допомогти ідентифікувати володільця, його правовий статус у відносинах з приводу персональних даних слід тлумачити згідно із законодавством про захист персональних даних. Тобто, поняття володілець не повинно звужуватись іншими дотичними чи перехресними поняттями з різних галузей права, як наприклад, автор або суб'єкт майнових прав інтелектуальної власності. Іншими словами, статус суб'єкта майнових прав інтелектуальної власності не виключає можливості одночасної кваліфікації такого суб'єкта як «володілець» та покладання на нього обов'язків по захисту персональних даних [170].

Наступним суб'єктом, який обробляє персональні дані, є розпорядник. Як і у разі тлумачення поняття «володілець», термінологія щодо розпорядника персональних даних, котра використовується в національному законодавстві, відрізняється від тієї, що міститься у актах ЄС, де цього суб'єкта називають «оператор обробки даних» («processor»). Під розпорядником персональних даних розуміють фізичну чи юридичну особу, якій володільцем персональних даних або законом надано право обробляти ці дані від імені володільця (абзац одинадцятий ст. 2 Закону України «Про захист персональних даних»). Отже, розпорядник є факультативним (додатковим) суб'єктом правовідносин із

приводу персональних даних, наявність якого в приватних правовідносинах залежить від волі володільця. Так, володілець, якщо інше не встановлено законом, може прийняти рішення обробляти персональні дані самостійно або доручити обробляти персональні дані повністю або частково іншій особі. Вбачається, що наявність розпорядника персональних даних обумовлена такими чинниками: 1) відносно володільця – юридичної особи така необхідність викликана структурними особливостями підприємств, установ та організацій, що використовують персональні дані фізичних осіб. Наприклад, відсутність у структурі підприємства кадрової служби обумовлює потребу залучити до процесу обробки персональних даних розпорядника; 2) відносно володільця – фізичної особи основною причиною укладання договору з розпорядником може бути обмеженість ресурсів та фондів для здійснення якісної обробки персональних даних, а також малий штат працівників [43, с. 174].

Розпорядника персональних даних характеризує дві ознаки: 1) власна правосуб'єктність; 2) можливість обробляти персональні дані від імені володільця. Так, розпорядником, як і володільцем, може бути фізична чи юридична особа. З цього приводу не може бути розпорядником підрозділ юридичної особи або працівник організації – володільця персональних даних. Ним може бути лише окрема юридична особа або окрема фізична особа. Однак, якщо володільцем персональних даних є орган державної влади чи орган місцевого самоврядування, то розпорядником, крім цих органів, може бути лише підприємство державної або комунальної форми власності, що належить до сфери управління цього органу (ч. 3 ст. 4 Закону України «Про захист персональних даних»). Розмежувальною ознакою розпорядника є те, що він обробляє персональні дані від імені володільця. Розпорядник не встановлює самостійно мету обробки персональних даних, не визначає їх склад та процедури обробки. Розпорядник діє від імені володільця, який визначив мету

обробки персональних даних розпорядником, установив склад персональних даних та встановив розпоряднику процедури обробки [171, с. 60].

Із розвитком інформаційних технологій дедалі частіше трапляються випадки, коли володільці доручають обробку персональних даних кільком розпорядникам. Така множинність розпорядників не суперечить законодавству про захист персональних даних. При цьому, можливими є два випадки. По-перше, той самий володілець доручає різним розпорядникам обробляти однакові персональні дані з різними цілями та/або обсягом такої обробки. По-друге, розпорядник, за погодженням із володільцем, залучає іншу особу («суброзпорядника») для обробки персональних даних у межах мети та обсягів, визначених володільцем.

Відносини між володільцем та розпорядником персональних даних повинні регулюватися відповідним договором. Наприклад, на практиці інколи зустрічається договір про передачу права обробки персональних даних, котрий, як правило, укладають як додаток на виконання іншого основного договору. Правова природа договору між володільцем та розпорядником мало висвітлюється в науковій літературі та повинна бути предметом окремого дослідження. Вважаємо, що такий договір має цивільно-правову природу, оскільки він є домовленістю володільця та розпорядника, спрямованою на встановлення, зміну або припинення цивільних прав та обов’язків, відповідно до якої володілець персональних даних доручає обробку персональних даних розпоряднику персональних даних. Тому ми критично оцінюємо віднесення договору між володільцем та розпорядником до рівнів адміністративно-правового регулювання сфери персональних даних [172, с. 518–519]. Не заперечуючи міжгалузевий характер відносин з приводу персональних даних та охоплення частини з них предметом адміністративного права, зауважимо, що у випадках, коли ні володілець, ні розпорядник не виступають як суб’єкт владних повноважень, договір між ними повинен підпадати під цивільно-правове регулювання. Договір між володільцем та розпорядником персональних даних

можна віднести до непоіменованих цивільно-правових договорів, до яких за аналогією закону можуть застосовуватись положення про договір доручення та загальні положення про послуги.

Необхідно вказати, що з норм як національного законодавства, так і Загального регламенту про захист даних, випливає обов'язковість укладання договору між володільцем та розпорядником (ч. 4, 5 ст. 4 Закону України «Про захист персональних даних» та ч. 3 ст. 28 Загального регламенту про захист даних). Більше того, встановлюється обов'язкова проста письмова форма такого договору. У літературі ці положення тлумачаться таким чином, що у разі відсутності договору, яким організація, володілець, доручає обробляти персональних дані з визначеною володільцем метою та у визначених володільцем обсягах іншій організації, то ця інша організація не може бути розпорядником [171, с. 61]. Вважаємо, що це твердження є занадто категоричним та може бути уточнено з урахуванням двох випадків. По-перше, якщо сторони як володілець та розпорядник досягли між собою згоди щодо обробки персональних даних, однак не зафіксували її зміст в одному або кількох документах (у тому числі електронних), то у цьому випадку необхідно застосовувати загальні правові наслідки недодержання вимоги щодо письмової форми правочину (ст. 218 ЦК України). Тобто, недодержання володільцем та розпорядником письмової форми договору не має наслідком його недійсність, оскільки це прямо не встановлено законом. А у разі спору факт вчинення такого договору або зміст окремих його частин може доводитися письмовими доказами, засобами аудіо-, відеозапису та іншими доказами. По-друге, якщо така домовленість між володільцем персональних даних та іншою особою не була досягнута, то остання не може набути статусу розпорядника. У випадках, коли така особа все ж отримала персональні дані її слід розглядати як фактичного володільця, законного або незаконного, залежно від конкретних обставин.

Закон України «Про захист персональних даних»фактично не містить положень, котрі би визначали зміст договору між володільцем та розпорядником, за винятком ч. 5 ст. 4, з якої випливає, що у такому договорі повинна бути визначена мета та обсяг обробки персональних даних. Натомість, Загальний регламент про захист даних встановлює, що такий договір повинен передбачати: предмет і тривалість обробки, специфіку і цілі обробки, тип персональних даних і категорії суб'єктів даних, обов'язки і права контролера (ч. 3 ст. 28).

Зрозуміло, що конкретний зміст досліджуваного договору буде значною мірою залежати від тих правовідносин, які склалися між суб'єктом персональних даних, їх володільцем і розпорядником, та зумовили необхідність обробки персональних даних. У той же час, слушною вважаємо пропозицію щодо визначення загальних вимог до договору між володільцем та розпорядником, зміст якого повинен охоплювати: предмет та строк дії договору; мету обробки персональних даних; склад персональних даних та категорії суб'єктів персональних даних, що обробляються розпорядником; вимоги до технічних та організаційних заходів захисту в ході обробки цих даних розпорядником; відповідальність володільця перед суб'єктом персональних даних, зокрема за дії розпорядника під час обробки його даних. Саме володілець несе відповідальність перед суб'єктом, доки не доведе, що порушення прав суб'єкта сталося з вини розпорядника; можливість (право) розпорядника залучати субпідрядників до процесу обробки персональних даних; процедуру видалення та знищення персональних даних розпорядником, у тому числі внаслідок закінчення строку дії договору (чи через певний час після цього), та повернення володільцю носіїв персональних даних [81, с. 164].

Поряд із взаємними правами та обов'язками, встановленими договором між володільцем та розпорядником, їм також належать сукупність прав та обов'язків щодо обробки та захисту персональних даних. Такі права та обв'язки прийнято групувати наступним чином.

1. Права та обов’язки щодо отримання та збирання персональних даних: а) права і обов’язки щодо встановлення мети обробки персональних даних у базах; б) права і обов’язки щодо підбору відомостей про особу, які мають увійти до бази персональних даних; в) права і обов’язки щодо впорядкування відомостей про фізичну особу.

2. Права та обов’язки щодо обробки персональних даних: а) права і обов’язки щодо накопичення персональних даних; б) права і обов’язки щодо використання персональних даних; в) права і обов’язки щодо поширення персональних даних; г) права і обов’язки щодо знеособлення, видалення та знищення персональних даних.

3. Права і обов’язки щодо захисту персональних даних: а) права і обов’язки щодо надання доступу до персональних даних; б) обов’язки щодо повідомлення про обробку та інші дії з персональними даними; в) обов’язки щодо поточного захисту персональної інформації; г) право на судовий захист інтересів суб’єкта персональних даних – володільця та розпорядника [173, с. 210–203].

До учасників, які обробляють персональні данні, слід віднести також третіх осіб. Закон України «Про захист персональних даних» [3] під третіми особами розуміє будь-яку особу, 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. Загалом поняття «третьої особи» використовується в Законі відповідно до цивілістичної традиції його вживання. Так, визначають наступні сутнісні риси участі третіх осіб у цивільних правовідносинах. Ними є: (1) множинність правовідносин. Адже фігура третьої особи з’являється там, де виникає декілька цивільних правовідносин. При чому, стороною первісного, вихідного правовідношення третя особа не виступає; (2) характер правовідносин. За характером усі правовідносини є відносними. Відносні правовідносини, до яких третя особа

вступає як сторона, іншою стороною мають сторону первісних правовідносин. Без первісного правовідношення дані відносини існувати не можуть; (3) динаміка первісного правовідношення. У встановленні (виникненні) первісного правовідношення третя особа участі не приймає, однак не виключається ситуація, коли на наступних етапах його динаміки третя особа може набути прав сторони первісного правовідношення; (4) юридична заінтересованість третьої особи, яка має багатогранний характер. Інтереси сторони первісних правовідносин та третьої особи можуть співпадати або ні, але юридична заінтересованість третьої особи не може бути ідентичною інтересу сторін [174, с. 7–8].

Однак, на відміну від загальних положень, 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 [170]. 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.

У літературі підкреслюється, що становище третьої особи у відносинах, пов'язаних із персональними даними, має дві істотні особливості, які визначають індивідуальність цього суб'єкта. По-перше, третя особа отримує

відомості про фізичну особу не від самого суб'єкта персональних даних, а від володільця або розпорядника. При цьому ми критично ставимось до твердження, що третя особа – єдиний суб'єкт, який може використовувати персональні дані навіть без згоди самої фізичної особи [43, с. 175], оскільки відповідно до чинної редакції ч. 1 ст. 16 Закону України «Про захист персональних даних» умовами згоди суб'єкта персональних даних, наданої володільцю персональних даних на обробку цих даних, визначається крім іншого і порядок доступу до персональних даних третіх осіб. Крім того, як вже було встановлено, згода є далеко не єдиною підставою для обробки персональних даних. По-друге, мета обробки персональних даних третьою особою не співпадає із метою обробки таких даних володільцем чи розпорядником, які їх надають[43, с. 175]. Саме це наочно демонструє різницю між розпорядником і третьою особою, котра полягає в тому, що розпорядник бази обробляє персональні дані в інтересах володільця, а третій особі дані (або частина даних) надаються для цілей третьої особи, визначених законом або для цілей статутної діяльності третьої особи за згодою суб'єкта персональних даних [169, с. 193].

Висловимо свою солідарність з М. В. Різак, який запропонував визначити такі права та обов'язки третіх осіб у відносинах обігу та обробки персональних даних:

– право на отримання персональних даних від володільців та розпорядників персональних даних у межах, визначених умовами згоди суб'єктів цих персональних даних;

– право на обіг та/або обробку персональних даних у межах конкретно визначеної мети та/або правової підстави, задля яких вони були отримані;

– право на формування власних баз персональних даних;

– обов'язок розкривати чітко визначені мету та цілі отримання персональних даних від їх володільців та/або розпорядників;

– обов’язок корегувати межі обігу та/або обробки персональних даних залежно від змін згоди суб’єкта персональних даних, зокрема, припинити обіг та/або обробку персональних даних у разі отримання інформації про відкликання згоди суб’єкта персональних даних або її заміни на таку, що не дозволяє третім особам продовжувати обіг та/або обробку цих даних;

– обов’язок видаляти або знищувати персональні дані у випадках, передбачених законодавством;

– обов’язок набути в порядку, визначеному законом, правового статусу володільця та/або розпорядника персональних даних після отримання персональних даних від їх володільця та/або розпорядника [169, с. 23].

Поряд із третіми особами виділяють ще одного учасника відносин із приводу персональних даних – одержувача. Поняття «одержувач» має легальне визначення як на рівні Загального регламенту про захист даних («одержувач» означає фізичну чи юридичну особу, державний орган, агентство чи будь-який інший орган, якому надаються дані, незалежно від того, третя це особа чи ні; однак, органи, що можуть одержувати дані в рамках окремого запиту, не розглядаються як одержувачі»), так і на рівні Закону України «Про захист персональних даних» [3] («одержувач – фізична чи юридична особа, якій надаються персональні дані, у тому числі третя особа»). Аналіз цих двох визначень свідчить, що вони не цілком співпадають за своїм змістом та обсягом. Так, національний законодавець не відніс до одержувачів такий суб’єкт, як державний орган, та не виключив із числа одержувачів такі державні органи, до повноважень котрих належить отримання персональних даних у межах спеціального запиту.

Важливо розмежувати поняття «третіх осіб» та «одержувачів». У навчальній літературі різниця між цими двома категоріями фізичних або юридичних осіб, полягає у тому, як саме визначається їх зв’язок із володільцем і, як результат, їхнім правом на доступ до персональних даних володільця [87, с. 59]. Більше того, стверджується, що поняття «одержувач» є ширшим та

включає поняття третьої особи [81, с. 29]. Вважаємо, що така позиція не враховує важливу розмежувальну ознаку, а саме: одержувачем визнається тільки особа, якій передаються персональні дані, тоді як для третьої особи така ознака не обов'язкова. Тому, в контексті законодавства про захист персональних даних, доцільно розглядати одержувача та третіх осіб як різні за змістом поняття, які частково мають спільний обсяг.

Відмінність між одержувачами і третіми особами є важливою лише у зв'язку з умовами законного оприлюднення персональних даних. Співробітники володільця або розпорядника можуть без будь-яких законних вимог бути одержувачами персональних даних, якщо беруть участь у їхніх операціях з обробки. Такі співробітники володільця або розпорядника, 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 (п. 3.7 Типового порядку обробки персональних даних, затвердженого Наказом Уповноваженого Верховної Ради України з прав людини від 08.01.2014 № 1/02-14 [175]). З іншого боку, третя особа, яка є юридично самостійною по відношенню доволодільця або розпорядника, не має права використовувати оброблені володільцем персональні дані, за винятком, коли це передбачено спеціальним законом у кожному конкретному випадку. Тому для того, щоб отримати персональні дані у законний спосіб, у «одержувачів-третьої особи» завжди повиннібути правові підстави [87 с. 60].

Інші науковці висловлюють думку, що закріплення поняття «одержувач» є недоцільним і таким, що створює можливості неоднозначності розуміння правового статусу цього суб'єкта правовідносин з обігу та обробки персональних даних. У зв'язку із цим, пропонують виключити поняття «одержувач» із законодавства про захист персональних даних [176, с. 22–23]. Однак, із такою позицією не можна погодитись, виходячи з таких аргументів: по-перше, виключення поняття «одержувач» буде суперечити європейським

стандартам, оскільки і Директива 95/46/ЄС [32], і Загальний регламент про захист даних [49] передбачають такого учасника відносин з приводу персональних даних як одержувач. По-друге, виключення поняття «одержувач» звузить зміст прав суб'єкта персональних даних, принаймні, таких, як право на інформацію та право на доступ.

Висновки до Розділу 2

1. Право на персональні дані належить до основоположних прав людини, прояв якого в цивільних правовідносинах обґрунтований теорією горизонтальної дії прав людини.

2. Обґрунтовано неможливість визнання абсолютним права на персональні дані. Це зумовлено встановленням обмежень та випадків правомірного втручання при здійсненні цього права (ч. 2 ст. 8 ЄКПЛ, ч. 1, 3 ст. 52 Хартії основних прав Європейського Союзу, ч. 1, 2 ст. 9 Конвенції про захист осіб у зв'язку з автоматизованою обробкою персональних даних, ст. 9 та ч. 1 ст. 13 Директиви 95/46/ЄС, ч. 1 ст. 25 Закону України «Про захист персональних даних»). При цьому, обмеження можуть застосовуватися лише при дотриманні принципу пропорційності та у випадку, якщо вони необхідні в демократичному суспільстві, спрямовані на досягнення легальних цілей або для захисту прав і свобод інших людей.

Законодавство повинно забезпечувати *пропорційність між правом на персональні дані та правом на свободу висловлювання думок та інформації,* у тому числі – щодо обробки персональних даних для журналістських цілей та академічної, художньої і літературної свободи.

3. Право на персональні дані є цивільно-правовим за своєю природою, оскільки відносини, що виникають із приводу персональних даних, цілком відповідають ознакам, закріпленим в ч. 1 ст. 1 ЦК України.

4. Обґрунтовано *неможливість розглядати право на персональні дані та право на інформацію загалом як право власності* (заперечується речево-правовий підхід), оскільки не можна ототожнювати персональні дані як інформацію та матеріальний носій їх закріплення. Водночас, в окремих випадках права на персональні дані можуть набувати ознак матеріальних активів. Наприклад, суб'єкт підприємницької діяльності, який правомірно обробляє персональні дані споживачів, може продавати компіляцію таких персональних даних іншим особам.

5. У зв'язку із обробкою персональних даних, необхідно *розмежовувати правовий режим бази персональних даних як об'єкта права інтелектуальної власності та об'єкта захисту*. Потрібно враховувати наступне. *По-перше*, ні матеріальний носій бази персональних даних, ні її внутрішнє інформаційне наповнення не є об'єктом права інтелектуальної власності автора бази (творця, розробника). *По-друге*, ні визнання бази персональних даних об'єктом авторського права, ні встановлення щодо неї права особливого роду, не виключають застосування законодавства стосовно охорони персональних даних та не можуть йому суперечити.

6. *Право на персональні дані є самостійним особистим немайновим правом*, що обумовлено специфікою персональних даних як об'єкта цивільних правовідносин. Так, *персональні дані є власне інформацією про фізичну особу*, в тому числі – про її особисті немайнові блага та ознаки, що її індивідуалізують.

Право на персональні дані - це особисте немайнове право, специфіка якого полягає в його: об'єкті – персональні дані; меті – захист права на приватність та інших особистих немайнових прав у зв'язку з обробкою персональних даних; змісті – активні та пасивні правомочності, а також правомочність захисту, котрі можуть бути реалізовані як в абсолютних, так і відносних правовідносинах.

Запропоновано проект статті 302^1 Цивільного кодексу України. Стаття 302-1**.** *Право фізичної особи на персональні дані*

«1. Фізична особа має право на персональні дані, у тому числі на зміну або знищення своїх персональних даних.

2. Фізична особа має право на доступ до своїх персональних даних, що включає в себе її можливість ознайомитись з персональними даними та робити власноручні письмові витяги, а також можливість виготовлення копій документів з персональними даними у розумний строк.

3. Право на доступ до персональних даних може бути обмежено в інтересах захисту національної безпеки, а також з метою захисту конфіденційної інформації третіх осіб.

4. Держава гарантує практичний і ефективний механізм захисту прав на персональні дані, який виключає можливість будь-якого несанкціонованого доступу до персональних даних фізичної особи».

7. Охарактеризовано два підходи до кількісного складу прав суб'єкта персональних даних: 1) нормативний – права суб'єкта персональних даних закріплено в законодавстві (України та актах ЄС); 2) права суб'єкта персональних даних залежать від змісту права на персональні дані як єдність трьох елементів: права на власні дії, права на чужі дії та права на захист. Обґрунтовано правильність другого підходу, оскільки він відображає зміст права на персональні дані як об'єкта цивільного правовідношення, що залежить від конкретного суб'єкта, має конкретний об'єкт та спрямований на захист права на невтручання в особисте життя, у зв'язку з обробкою персональних даних.

8. Зміст права на персональні дані сьогодні потребує доповнення новими правомочностями. До таких правомочностей віднесено право на мобільність та право на забуття.

Право на мобільність персональних даних закріплено в ст. 20 Загального регламенту про захист даних. Причиною його запровадження є поширення обробки персональних даних в мережі Інтернет та необхідність забезпечити можливість вільного переміщення персональних даних від одного володільця

(провайдера, соціальної мережі) до іншого. Це сприятиме вільній конкуренції шляхом створення рівних можливостей для існуючих компаній та появи нових на ринку.

Право на мобільність не охоплює весь обсяг персональних даних, які перебувають у володільця, а тільки ті з них, котрі були надані (створені) самим суб'єктом персональних даних. До таких слід віднести дані безпосередньо завантажені чи опубліковані суб'єктом, наприклад, фотографії, статуси, контактна інформація, резюме тощо.

Зміст права на мобільність персональних даних включає в себе можливість суб'єкта персональних даних: отримати від володільця персональні дані у форматі, придатному для подальшого використання; передати такі персональні дані іншому володільцю; вимагати від володільця безпосередньої передачі таких персональних даних іншому володільцю при технічній можливості.

Межі права на мобільність персональних даних обумовлені: предметом (мобільності підлягають лише персональні дані, створені самим суб'єктом); умовами (мобільність персональних даних можлива лише, якщо персональні дані обробляються на підставі вільного волевиявлення суб'єкта даних із застосуванням автоматизованих засобів); межами здійснення (право на мобільність не може здійснюватися на шкоду іншим правам суб'єкта персональних даних, правам інших суб'єктів персональних даних, правам та свободам третіх осіб).

Право на мобільність слід розглядати як окреме право в системі прав суб'єкта персональних даних, відмінне від права на доступ, права на забуття, та тісно пов'язане з правом на захист персональних даних.

Наступним є *право на забуття*, зміст якого полягає у можливості суб'єкта персональних даних вимагати від володільця видалення даних, які його стосуються.

Право на забуття одержало нормативне закріплення в окремих

зарубіжних країнах. У Франції була прийнята Хартія про право на забуття (2010 р.), де ним позначається цивільно-правовий спосіб захисту особистих немайнових прав публічної особи щодо таємниці минулого і життєвий спокій того, хто вирішив не присвячувати себе публічним справам надалі. В Італії право на забуття розглядається судовою практикою як право кожного громадянина на видалення з архіву новин певних біографічних фактів, здатних завдати шкоди його честі або репутації, якщо ці факти більше не є актуальними або не становлять громадський інтерес. У Німеччині право на забуття інтерпретується як один із елементів змісту загального особистого немайнового права, як правило, засуджених за вчинення злочину. У США встановлено право неповнолітніх злочинців подати до суду заяву про вилучення обвинувального вироку суду у справах неповнолітніх. Крім того, в Каліфорнії з 2013 р. діє закон, який наділяє неповнолітніх осіб правом видаляти або вимагати видалення контенту чи інформації, викладеної ними на веб-сайті чи Інтернет-порталі.

Право на забуття знаходить своє визнання також в практиці ЄСПЛ, де відображено наступні правові позиції: 1) тривале зберігання персональних даних підпадає під дію ст. 8 ЄКПЛ та охоплюється змістом права на приватне життя; 2) тривале зберігання персональних даних повинно мати додаткові підстави; 3) тривале зберігання інформації може спричинити непропорційне втручання держави в реалізацію права на приватне життя; 4) строк зберігання персональних даних та умови їх дострокового знищення повинні бути чітко визначені; 5) темпоральні рамки є лише однією з умов, які враховуються при встановленні балансу між захистом персональних даних та правом на свободу слова.

Окремі елементи права на забуття закріплені в Директиві 95/46/ЄС, серед яких: 1) персональні дані повинні бути точними і, якщо необхідно, оновлюватися (п. d ст. 6); 2) персональні дані повинні зберігатися у певній формі (п. e ст. 6); 3) суб'єкт персональних даних має право вимагати від

володільця стирання персональних даних, обробка яких не відповідає положенням цієї Директиви (п. b ст. 12); 4) суб'єкт персональних даних має право вимагати від володільця повідомлення третім сторонам про будь-яке виправлення, стирання чи блокування (п. c ст. 12); 5) суб'єкт персональних даних має право заперечувати проти обробки даних, які його стосуються (п. a ст. 14).

Закон України «Про захист персональних даних» частково визнає право на забуття. Так, у Законі закріплюється: право суб'єкта персональних даних пред'являти вмотивовану вимогу щодо знищення своїх персональних даних будь-яким володільцем та розпорядником персональних даних, якщо ці дані обробляються незаконно чи є недостовірними (п. 6 ч. 2 ст. 8); підстави та умови видалення або знищення персональних даних (ч. 2, 3 ст. 15).

Одним із перших рішень Європейського Суду про визнання права на забуття персональних даних було рішення у справі Google Spain SL, Google Inc. v. Agencia Española de Protección de Datos (AEPD), Mario Costeja González (2014 р.). Суд зазначив, що люди мають право за певних умов просити видалити із пошукових систем посилання з особистою інформацією про них.

У Загальному регламенті про захист даних використовується два терміни: право на знищення («right to erasure») та право на забуття («right to be forgotten») (17). У роботі це пояснюється так: якщо досліджуване право ґрунтується на особистих немайнових правах фізичної особи, то це – «право на забуття», а якщо на механізмі захисту персональних даних, то це – «право на знищення персональних даних». У цьому документі закріплено підстави для реалізації права на забуття (ч. 3 ст. 17).

Запропоновано критерії при встановлені балансу між колідуючими правами та правом на забуття із дотриманням при цьому принципу пропорційності: 1) чи належить суб'єкт персональних даних до публічних осіб, оскільки межа правомірної обробки персональних даних щодо політичного діяча чи іншої публічної особи є значно ширшою, ніж непублічної особи; 2) чи

суб'єкт персональних даних є неповнолітнім, і чи була особа неповнолітньою на момент первинної обробки персональних даних, оскільки інтереси дитини повинні розглядатися як пріоритетні; 3) чи персональні дані є повними, точними та достовірними; 4) чи персональні дані є адекватними та не надмірними; 5) чи належать персональні дані до так званих чутливих категорій даних, оскільки останні користуються підвищеним захистом, а їх обробка повинна відповідати особливим вимогам; 6) чи заподіює обробка персональних даних шкоду їх суб'єкту або створює загрозу заподіяння такої шкоди; 7) чи давав суб'єкт персональних даних згоду на їх обробку або обробка здійснювалась на інших підставах. При цьому зазначається, що перелік таких критеріїв не може бути визнаний вичерпним, а тому повинні враховуватися й інші обставини, що мають значення для встановлення балансу між правом на забуття та колідуючими йому правами.

9. До осіб, які беруть участь у відносинах щодо персональних даних, віднесено володільця персональних даних і розпорядника ними. *Володілець характеризується такими ознаками*: 1) володіє власною правосуб'єктністю, тому є відповідальним за дотримання законодавства про захист персональних даних та носієм обов'язків, що кореспондують правам суб'єкта персональних даних; 2) можливість діяти самостійно чи разом з іншими суб'єктами, коли два і більше суб'єкти визначають мету та засоби обробки персональних даних (співволодільці); 3) можливість визначати мету та інші умови обробки персональних даних.

10. Залежно від підстави обробки персональних даних виділено види їх володільців: 1) титульний – особа, яка набула статусу володільця безпосередньо чи опосередковано на підставі норм права; 2) фактичний законний – особа, яка набула статусу володільця в силу фактичних обставин за умови дотримання принципів обробки персональних даних; 3) фактичний незаконний – особа, яка набула статусу володільця за відсутності правомірної підстави для обробки персональних даних. Такий поділ має значення при

визначенні відповідальності володільця за порушення прав суб'єкта персональних даних.

11. *Розпорядник персональних даних* є факультативним (додатковим) суб'єктом правовідносин щодо персональних даних, який є володільцем персональних даних або за законом йому надано право обробляти такі дані від імені володільця. Розпорядника персональних даних характеризують такі ознаки: 1) власна правосуб'єктність; 2) можливість обробляти персональні дані від імені володільця.

12. Правовідносини між володільцем і розпорядником персональних даних повинні регулюватися відповідним *договором*. Укладення такого договору є обов'язковою умовою для залучення розпорядника. Такий договір має цивільно-правову природу, оскільки означає домовленість володільця та розпорядника, спрямовану на встановлення, зміну або припинення цивільних прав та обов'язків, відповідно до якої володілець персональних даних доручає їх обробку розпоряднику персональних даних.

13. У відносинах обробки персональних даних беруть участь також *треті особи,* які: 1) не є стороною відносних правовідносин між суб'єктом даних та їх володільцем (розпорядником); 2) мають охоронюваний законом інтерес щодо персональних даних; 3) перебвають у правовідносинах із володільцем (розпорядником) щодо передачі даних; 4) об'єктом таких відносин виступають персональні дані того самого суб'єкта персональних даних; 5) із моменту отримання персональних даних набувають статусу їх володільця чи розпорядника. Поряд із третіми особами виділяють ще одного учасника відносин з приводу персональних даних – *одержувача*. Ним визнається лише особа, якій передають персональні дані, тоді як для третьої особи така ознака не обов'язкова. Тому, в контексті законодавства про захист персональних даних, доцільно розглядати «одержувача» та «третіх осіб» як різних учасників правовідносин щодо персональних даних, які мають частково спільний обсяг прав.

РОЗДІЛ 3
ДИНАМІКА ЦИВІЛЬНИХ ПРАВОВІДНОСИН ЩОДО ПЕРСОНАЛЬНИХ ДАНИХ

3.1 Підстави виникнення цивільних правовідносин щодо персональних даних

Поняття «згода» має загальноцивілістичне значення та знаходить свій прояв у різних інститутах цивільного права, фактично усіх його підгалузей, зокрема: загальні положення про фізичну особу – згода батьків (усиновлювачів), піклувальника на вчинення правочину; загальні положення про юридичну особу – згода учасників товариства; особисті немайнові права фізичної особи – згода фізичної особи на втручання в її особисті немайнові права (проведення медичних, наукових та інших дослідів; надання медичної допомоги; донорство органів та інших анатомічних матеріалів, у тому числі на випадок смерті фізичної особи; використання імені фізичної особи; розголошення обставин особистого життя фізичної особи; збирання, зберігання, використання і поширення інформації про особисте життя фізичної особи; ознайомлення з особистими паперами фізичної особи та їх використання; знімання фізичної особи на фото-, кіно-, теле- чи відеоплівку); право власності та інші речові права – згода співвласників; право інтелектуальної власності – згода автора; зобов'язальне право – згода сторони договору, згода кредитора, згода боржника, згода поручителя, згода заставодержателя, згода третьої особи, згода учасників спільної діяльності; спадкове право – згода спадкоємців, виконавця заповіту.

Очевидно, що найбільша питома вага використання поняття «згода» припадає на особисті немайнові права фізичної особи, що власне і розкриває її значення у відносинах з приводу персональних даних. Перш за все, розглянемо нормативне закріплення згоди суб'єкта персональних даних на європейському

рівні. Конвенція про захист осіб у зв'язку з автоматизованою обробкою персональних даних [71], попри те, що встановлює вимогу законності обробки персональних даних, не містить переліку легітимних підстав для такої обробки. Згода суб'єкта персональних даних згадується у цій Конвенції лише з приводу допомоги особам, які проживають закордоном (ст. 14, 15). Однак, навряд чи це можна використати як аргумент для ствердження, що згода не відіграє важливої ролі відповідно до вказаної Конвенції. Натомість Хартія основних прав Європейського Союзу [103] визнає згоду як правомірну підставу використання персональних даних (ст. 8). Найбільш повно концепція згоди розкрита в Загальному регламенті про захист даних [49], в якому дається визначення поняття «згода суб'єкта даних» (ст. 4), така згода визнається підставою законної обробки персональних даних (ст. 6), виокремлюється згода на обробку чутливих категорій даних (ст. 9).Такий же підхід рецепійовано національним законодавством ще з Директиви 95/46/ЄС «Про захист фізичних осіб при обробці персональних даних і про вільне переміщення таких даних» [32].

Ні міжнародні акти, ні національне законодавство не визначають правову природу згоди суб'єкта персональних даних, залишивши це питання предметом наукових досліджень. Згода суб'єкта персональних даних має щонайменше три іпостасі: 1) можливість фізичної особи діяти певним чином; 2) юридичний факт; 3) об'єктивована форма. Згоду як можливість суб'єкта персональних даних слід розглядати у трьох зрізох. По-перше, така згода є важливим елементом права кожної людини на вільний розвиток своєї особистості. Так, концепція згоди базується на ліберальній доктрині свободи людини, її гідності та недоторканості, ґрунтується на теорії фундаментальних прав людини, тісно переплітаючись із правом на приватність [177]. Іншими словами, інститут згоди суб'єкта персональних даних є одним із проявів свободи людини у відносинах з приводу таких даних. Свобода суб'єкта персональних даних є одночасно і передумовою, і наслідком згоди та, в кінцевому результаті, забезпечує вплив суб'єкта персональних даних на їх обробку. Однак свобода суб'єкта

персональних даних надавати чи не надавати згоду на їх обробку не є абсолютною, що підтверджується тим, що згода є далеко не єдиною підставою для їх обробки.

По-друге, згода суб'єкта персональних даних відображає таку загальну засаду цивільного законодавства як неприпустимість свавільного втручання у сферу особистого життя людини. У цьому контексті наявність чи відсутність згоди суб'єкта персональних даних вказує на правомірність чи неправомірність обробки персональних даних. Тобто, більш узагальнено, згода виконує функцію трансформації поведінки з такої, що суперечить моральним засадам суспільства, в таку, що їм відповідає [178, с. 123]. Так, змінюються очікування особи, яка надає згоду (вона розуміє чого очікувати відповідно до наданої згоди), особи, яка запитує згоди (вона розуміє, що її поведінка вважається дозволеною), суспільства в цілому (відбувається визнання впливу згоди на відносини між особою, яка надає згоду, та особою, яка її запитує) [179, с. 172]. У нашому випадку втручання в особисте життя шляхом збирання, зберігання, використання і поширення відомостей про фізичну особу при наявності згоди такої особи трансформується у відносини між суб'єктом, володільцем та розпорядником персональних даних з приводу їх обробки.При цьому, для того, щоб згода суб'єкта персональних даних виконувала таку функцію, вона повинна відповідати встановленим в законі вимогам щодо її змісту та форми, котрі будуть досліджені нами нижче.

По-третє, згоду суб'єкта персональних даних слід розглядати в контексті можливості фізичної особи вільно, на власний розсуд визначати свою поведінку у сфері васного приватного життя, тобто, як елемент змісту особистого немайнового права. Оскільки персональні дані становлять невідчужуване особисте немайнове благо, юридичний зв'язок між суб'єктом права та його об'єктом існує протягом усього життя і не може вважатися розірваним через те, що індивід дозволив третій особі збирати, поширювати чи іншим чином використовувати такі дані [180, с. 103]. У цій площині поняття згоди тісно

пов’язане з ідеєю контролю суб’єкта персональних даних над тим хто, відповідно до якої мети та для яких цілей оброблятиме його персональні дані. Очевидно, що згода не єдиний прояв контролю суб’єкта персональних даних. Цьому, серед іншого, також слугує вимога суб’єкта персональних даних із запереченням проти обробки персональних даних, вимога щодо зміни чи знищення своїх персональних даних, а також відкликання згоди на обробку персональних даних. Проте, усе це різні механізми забезпечення контролю суб’єкта персональних даних на різних стадіях обробки персональних даних.

Таким чином, згоду суб’єкта персональних даних слід розглядати як прояв можливості вільно визначати свою поведінку в сфері особистого життя, яка, з одного боку, спрямована уповноважити володільця персональних даних на їх подальшу обробку, а з іншого, – забезпечує контроль суб’єкта персональних даних за їх обробкою. Таке розуміння згоди відображає концепцію «автономного дозволу» («*autonomous authorisation*»), запропоновану Р. Фаденомі Т. Бошампом, котра розглядає згоду як свідому, розумну поведінку, позбавлену контролюючого впливу [181, с. 277].

Згода суб’єкта персональних даних як юридичний факт слугує підставою для обробки таких даних. При цьому виникає, як мінімум, два питання, на які немає однозначної відповіді ні в законодавстві, ні в правозастосовній практиці, ні в доктрині: чи є згода суб’єкта персональних даних правочином; чи застосовуються до згоди суб’єкта персональних даних вимоги про дійсність правочинів. Якщо трактувати ці питання ширше, хоча б на рівні згоди фізичної особи на втручання в її особисті немайнові права, то стає очевидним, що відповіді будуть різними залежно від ситуації. Так, в літературі зазначається, що згода особи, яка виражає дозвіл на використання ознак індивідуальності, повинна вважатися правочином та може бути вчинена у вигляді як одностороннього, так і двостороннього правочину, на відміну від згоди пацієнта на здійснення медичного втручання, котра не визнається правочином [13, с. 144]. Буквальне тлумачення законодавства свідчить, що

згода суб'єкта персональних даних має усі ознаки правочину: є дією особи (добровільним волевиявленням фізичної особи), спрямованою на набуття, зміну або припинення цивільних прав та обов'язків (щодо надання дозволу на обробку її персональних даних). Таким чином, згоду суб'єкта персональних даних слід віднести до односторонніх правочинів.

Поряд із цим, згода суб'єкта персональних даних має ще одне, неочевидне на перший погляд, значення. Розвиток інформаційних технологій та спричинена ним поява й поширення адресного маркетингу надали персональним даним комерційної цінності для суб'єктів підприємницької діяльності. У такій ситуації згода суб'єкта персональних даних не тільки виражає вибір фізичної особи щодо використання персональних даних іншою особою, але й, крім того, забезпечує оборотоздатність економічної цінності персональних даних [182, с. 11]. Підтвердження цьому знаходимо навіть у преамбулі Загального регламенту про захист даних [49], яка вказує на дедалі частіше застосування обробки персональних даних у різних сферах соціальної та економічної діяльності, неминуче істотне збільшення транскордонних потоків персональних даних між усіма тими, хто бере участь в економічному і соціальному житті, необхідність розвитку обміну персональними даними між різними підприємствами (пп. 4, 5). У науковій літературі це пояснюється тим, що після надання суб'єктом згоди на обробку інформації про особу (в тому числі персональних даних – уточнено мною – Ю. Б.) виникає віддільність інформації від фізичної особи, оскільки факт згоди суб'єкта на використання інформації про себе надає можливість виокремити інформацію від суб'єкта-носія, а це є умовою для визнання такого об'єкта оборотоздатним. Разом із тим, якщо особа надала згоду на обробку інформації про себе, то інформація отримує стан виокремленості від особи, однак використання отриманої інформації можливо у межах, які дозволені особою. Отже, інформація про особу за наявності її волевиявлення може розглядатися як оборотоздатний об'єкт, оскільки цей вид інформації може мати економічний зміст, здатність до

об’єктивного існування та віддільності від особи [24, с. 40]. Загалом підтримуючи такий підхід, зауважимо, що згоду не слід розглядати як єдиний чинник відокремленості персональних даних від суб’єкта, оскільки обробка персональних даних можлива й з інших підстав. Із цього приводу необхідним є співвідношення згоди з іншими підставами обробки персональних даних.

Закон України «Про захист персональних даних» та Загальний регламент про захист даних [49] називають по шість підстав для обробки персональних даних. Цей перелік підстав є вичерпним та не потребує поширювального тлумачення. Крім того, передбачаються спеціальні підстави для обробки чутливих категорій даних: 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 (ч. 2 ст. 7 Закону та ч. 6–9 Загального регламенту про захист даних [49]). Загалом, вказані в законі підстави відповідають нормам Регламенту попри те, що їх дослівне формулювання, а подекуди і тлумачення, при застосуванні відрізняються. Дослідимо їх детальніше.

Традиційно, підстави обробки персональних даних можна поділити на дві групи: незалежно від згоди особи та за згодою особи [183, с. 215]. Однак такий дихотомічний поділ не розкриває усієї специфіки підстав. Пропонуємо при поділі підстав на види використовувати як критерій не тільки наявність чи відсутність згоди, але й також суб’єкта інтересів здійснення обробки персональних даних. Це дає змогу виділити чотири види підстав: 1) обробка персональних даних здійснюється за згодою суб’єкта персональних даних; 2) обробка персональних даних здійснюється в інтересах суб’єкта персональних даних, але не залежно від згоди останнього (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; захист життєво

важливих інтересів суб'єкта персональних даних); 3) обробка персональних даних здійснюється незалежно від згоди суб'єкта персональних даних для задоволення публічних інтересів (дозвіл на обробку персональних даних, наданий володільцю персональних даних відповідно до закону виключно для здійснення його повноважень; необхідність виконання обов'язку володільця персональних даних, який передбачений законом); 4) обробка персональних даних здійснюється в інтересах третіх осіб незалежно від згоди суб'єкта персональних даних за умови пропорційності такого втручання в його особисте життя (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).

При цьому, ми критично ставимось до висловленого в літературі твердження, що деякі з цих підстав, закріплених в ст. 11 Закону України «Про захист персональних даних», встановлюють умови обробки персональних даних, а деякі мають характер принципів, тобто, вихідних положень. Цим твердженням аргументується потреба розмежування на законодавчому рівні категорії «підстава», «умова» та «принцип» [184, с. 143]. Вважаємо, що вказана позиція не може бути підтримана, оскільки ґрунтується виключно на буквальному тлумаченні зазначеної норми, та не зовсім враховує системне тлумачення, а саме взаємозв'язок із загальними правилами законності обробки персональних даних, тобто, загальними та особливими вимогами до їх обробки. Більше того, вона вступає в протиріччя з європейськими стандартами захисту персональних даних (Загальний регламент про захист даних [49]).

Розкриваючи співвідношення згоди та інших підстав обробки персональних даних, слід зазначити наступне. Попри те, що згода міститься в переліку підстав на першому місці, це не означає, що згода має переважаюче значення порівняно з іншими підставами. Більше того кількість альтернативних згоді підстав обробки персональних даних дає можливість стверджувати, що

значення згоди як прояву інформаційного самовизначення фізичної особи у відносинах із приводу персональних даних дещо перебільшено [185, с. 241]. Для прикладу, з урахуванням мети, забезпечення інтересів, за наявності яких допускається вчинення діянь з персональними даними без згоди особи, можна виділити наступні випадки: 1) захист інтересів держави, безпеки громадян під час введення воєнного чи надзвичайного стану; 2) забезпечення сплати податків, зборів, інших обов'язкових платежів; 3) забезпечення інтересів судочинства; 4) інтереси забезпечення виконавчого провадження; 5) мета – забезпечення цивільного обороту; 6) реалізація конституційних, цивільних прав громадян; 7) розслідування злочинів; 8) мета – доступ до публічної інформації та суспільно-необхідної інформації (інформації, що містить суспільний інтерес) [183 с. 217–221].

Однак, якщо вести мову про цивільні правовідносини, то згода займає чільне місце серед підстав обробки персональних даних поряд із правочином та випадками, коли приватні інтереси володільця персональних даних або третьої особи, якій передаються персональні дані, переважають потреби захисту основоположних прав і свобод суб'єкта персональних даних.

Поряд із цим, згода має ще одну відмінність від інших підстав обробки персональних даних. Усі інші підстави обробки персональних даних, крім згоди, обтяжені додатковою умовою – так званим тестом на необхідність. Тобто, обробка персональних даних буде вважатися правомірною, якщо вона є необхідною для досягнення цілей, обумовлених у відповідній підставі. Якщо ж обробка персональних даних виходить за межі такої необхідності, то для її здійснення вже потрібна згода суб'єкта персональних даних.

Те, що згода як підстава обробки персональних даних не вимагає застосування тесту на необхідність, не означає, що згода надає володільцю персональних даних ширші можливості. Так, отримання згоди суб'єкта персональних даних не звільняє їх володільця від обов'язку дотримуватись загальних та особливих вимог до обробки персональних даних. Більше того,

згода фізичної особи на обробку персональних даних не тягне за собою її відмову від прав суб'єкта персональних даних чи звуження їх змісту. Так само згода на обробку персональних даних не позбавляє та не обмежує можливості захисту персональних даних. На жаль, вітчизняний законодавець вказав на необхідність як умову обробки персональних даних лише щодо виконання передбаченого законом обов'язку володільця персональних даних та захисту законних інтересів володільця персональних даних або третьої особи, якій передаються персональні дані (п. 5, 6 ч. 1 ст. 11). З цього приводу вважаємо, що п. 2, 3 та 4 ч. 1 ст. 11 потребують змін шляхом закріплення необхідності як умови обробки персональних даних, а до внесення змін ці норми закону слід тлумачити обмежувально, із застосуванням тесту на необхідність обробки.

Від згоди як підстави для обробки персональних даних слід відрізняти випадки необхідності такої обробки, що виникає на стадії, котра передує укладанню правочину, під час укладання або виконання правочину, стороною або третьою особою, на користь якої укладено цей правочин, є суб'єкт персональних даних. Спільним для цих підстав є те, що вони ґрунтуються на вільному волевиявленні суб'єкта персональних даних. Більше того, як було встановлено вище, згода є різновидом одностороннього правочину. При цьому є дві принципові відмінності. По-перше, правочин є сам по собі підставою для обробки персональних даних, не залежно від того чи передбачає він дозвіл суб'єкта персональних даних на таку обробку. По-друге, обробка персональних даних на підставі правочину обмежена необхідність, яка виникає у зв'язку із укладанням або виконанням відповідного правочину. Також правомірність обробки персональних даних у цьому разі залежить від правомірності самого правочину, від того, чи був він укладений, від його дійсності на момент такої обробки.

Необхідність обробки персональних даних в інтересах третіх осіб незалежно від згоди суб'єкта персональних даних за умови пропорційності такого втручання в його особисте життя (п. 6 ч. 1 ст. 11) є єдиною підставою,

яка, відповідно до законодавства, вимагає дотримання балансу між колідуючими інтересами. Тобто, вимагається одночасна наявність двох умов: необхідність захисту законних інтересів володільця персональних даних або третьої особи, якій передаються персональні дані; такі інтереси переважають потреби захисту основоположних прав і свобод суб'єкта персональних даних у зв'язку з обробкою його даних. Прикладом вказаного законного інтересу у сфері захисту персональних даних може бути адресний (прямий) маркетинг, а саме: просування товарів шляхом направлення комерційного повідомлення потенційним споживачам не є правом, гарантованим законом, як і не є ним заборонено [81, с. 68].

Розуміння балансу колідуючих інтересів в контексті даної підстави обробки персональних даних було розкрито Судом ЄС у справі «Національна асоціація кредитних фінансових установ (ASNEF) і Федерація електронної комерції і прямого маркетингу (FECEMD) проти Державної адміністрації» (Asociacion Nacional de Establecimientos Financieros deCredito (ASNEF) and Federacion de Comercio Electronico y Marketing Directo (FECEMD) v. Administracion del Estado) від 24 листопада 2011 року [186]. Так, слід брати до уваги, що баланс вказаних інтересів залежить, в принципі, від індивідуальних особливостей конкретної справи, враховуючи те, що права суб'єкта персональних даних тісно пов'язані з фундаментальним правом на приватність. При цьому слід враховувати, що серйозність втручання в фундаментальні права суб'єкта персональних даних внаслідок їх обробки може відрізнятися залежно від того, чи отримали такі дані оприлюднення в загальнодоступних джерелах, чи ні. Однак, за винятком чутливих даних, жодні інші персональні дані не можуть мати наперед визначеної переваги перед інтересами володільця персональних даних.

Співвідношення згоди з іншими підставами обробки персональних даних не завжди є простим та очевидним. Наприклад, якщо володілець персональних даних обробляє їх у зв'язку із вчиненням та виконанням правочину, то для

обробки цих даних для цілей не пов’язаних із вчиненням та виконанням правочину необхідна буде окрема згода суб’єкта персональних даних. Це демонструє необхідність деталізації умов правочину. На практиці це означає, що для окремих етапів обробки персональних даних необхідно отримати згоду як додаткову підставу для такої обробки. У деяких випадках кілька підстав обробки персональних даних можуть застосовуватись одночасно. Іншими словами, будь-який етап обробки персональних даних повинен у будь-який час відповідати одній або кільком підставам для такої обробки [187].

Для того, щоб згода фізичної особи була правомірною підставою для обробки персональних даних, вона повинна відповідати умовам дійсності такої згоди. Аналіз законодавства та практики його застосування дозволяє виділити такі чотири умови: добровільність, поінформованість, конкретність, однозначність. Вказані умови застосовуються у сукупності, тобто, відсутність однієї з них свідчить про недійсність згоди на обробку персональних даних. Розглянемо умови дійсності згоди більш детально [188].

Добровільність як умова дійсності згоди означає, що волевиявлення суб’єкта персональних даних має бути вільним і відповідати його внутрішній волі. Таке волевиявлення не може вважатися вільним, якщо вчинено під впливом помилки, обману, насильства, тяжкої обставини. Тобто, згода є добровільною, якщо суб’єкт персональних даних самостійно обирає надавати таку згоду чи ні. Відсутність контролю з боку інших осіб у контексті згоди є ознакою такого вибору [188]. Тобто, якщо відмова надати згоду є практично нездійсненою в силу того, що вона є або неможливою, або буде мати дуже негативні наслідки для особи, яка надає таку згоду, тоді справжній вибір, як власне і згода відсутні [179, с. 173]. З цього приводу Л. Бігрейв та Д. Счартум пояснюють, що велика кількість позаюридичних факторів можуть зменшувати ефективність захисту приватності за допомогою механізму надання згоди, оскільки той рівень вибору, який цей механізм передбачає, не завжди присутній, особливо, якщо володілець персональних даних займає монопольне

(домінуюче) становище на ринку [189, с. 159]. У більшості випадків такий вибір зводиться до альтернативи «прийми це або залиш це» («take it or leave it»). Тобто, якщо споживач хоче отримати товар, роботу чи послугу, він може бути змушений або поступитись приватністю, або шукати цю продукцію в іншому місці. Такий підхід по суті не відповідає вимогам, що пред'являються до добровільної згоди, оскільки не надає суб'єкту свободу вибору щодо обробки його персональних даних.

Також О. В. Кохановська зазначає, що згода буде ефективною тільки за чітко визначених умов, які мають бути передбачені для такої згоди і за реальної можливості самої фізичної особи вносити зміни у зміст договору, оскільки так звані «договори про приєднання» в цій сфері, на думку вченої, можуть спричинити багато зловживань [33, с. 32]. Названі приклади демонструють ситуації дисбалансу між суб'єктом персональних даних та їх володільцем. Більше того, складність деяких бізнес-моделей, відносин між споживачем та суб'єктами господарювання, засобів та способів обробки персональних даних, технологічних застосунків можуть зробити майже неможливим для споживача зрозуміння або вільне вирішення щодо прийняти умов обробки персональних даних [190, с. 123]. Вирівнюванню вказаного дисбалансу служать закріплені в цивільному законодавстві гарантії захисту слабкої сторони. «Слабкою» в даному випадку виступає суб'єкт персональних даних, оскільки не має в розпорядженні ніяких фактичних можливостей впливати на володільця персональних даних щодо здійснення обробки персональних даних. «Сильна» сторона – володілець персональних даних, – навпаки, має в розпорядженні всі реальні можливості, в змозі диктувати суб'єкту персональних даних свою волю [191, с. 64].

Поінформованість як умова дійсності згоди знаходить свій прояв при нормативному закріпленні на рівні прав суб'єкта персональних даних (п. 1, 2, 12 ч. 2 ст. 8 Закону України «Про захист персональних даних») та обов'язків володільця персональних даних (ч. 2 ст. 12 Закону України «Про захист

персональних даних»). Хоча законодавство безпосередньо не визначає вимоги до інформації, яка має бути надана суб'єкту персональних даних, вважаємо, що вона повинна бути необхідною, доступною, достовірною та своєчасною. Необхідною інформацію щодо обробки персональних даних слід вважати тоді, коли вона містить відомості про: 1) суб'єктів (володільця чи розпорядника персональних, їх місцезнаходження або місце проживання (перебування); третіх осіб, яким передаються його персональні дані); 2) об'єкт (склад та зміст зібраних персональних даних); 3) суб'єктивні умови (права, визначені законом, мету збору персональних даних); 4) об'єктивні умови (джерела збирання, місцезнаходження своїх персональних даних; умови надання доступу до персональних даних; механізм автоматичної обробки персональних даних; які дії з персональними даними передбачатиме їх обробка; скільки часу персональні дані будуть зберігатися у володільця). Доступність інформації вказує на два елементи: 1) зміст її повинен бути доступним для розуміння особою, яка не є спеціалістом у сфері законодавства про захист персональних даних [81, с. 60]; 2) інформація повинна подаватись в наочній формі, доступній для сприйняття суб'єктом персональних даних. Достовірність інформації вказує на те, що вона повинна відповідати дійсності та не вводити суб'єкта персональних даних в оману. Своєчасність такої інформації означає, що уся необхідна інформації повинна бути надана суб'єкту персональних даних у момент запитування згоди на обробку його персональних даних.

Очевидно, що зміст та форма такої інформації, а також її відповідність вказаним вимогам може бути визначена тільки з урахуванням конкретних обставин. Поінформованість згоди суб'єкта персональних даних, крім того, має ще два важливих значення. По-перше, поінформованість є передумовою відкритості та прозорості обробки персональних даних, забезпечує контроль суб'єкта персональних даних за їх обробкою [187]. По-друге, зміна обставин обробки персональних даних, відомості про які були надані суб'єкту при отриманні його згоди, ставлять під сумнів поінформованість згоди щодо

подальшої обробки персональних даних. Це призводить до необхідності повідомити суб'єкта персональних даних про вказані зміни, а в окремих випадках – отримати нову згоду суб'єкта персональних даних (наприклад, при зміні мети).

Тісно з поінформованістю пов'язана інша умова дійсності згоди, а саме її конкретність, тобто згода повинна визначати мету та конкретні цілі обробки персональних даних. Співвідношення мети та цілей обробки персональних даних визначено в законі та полягає в наступному. Так, мета обробки персональних даних визначається в законі, установчих документах володільців баз персональних даних, положеннях, котрими регламентується їхня діяльність, тобто, мета має заздалегідь встановлений характер і пов'язана з видами діяльності відповідної юридичної особи чи фізичної особи-підприємця. У той же час, цілі, на задоволення котрих збираються персональні дані, визначаються згодою їх власника, відповідно мають більш конкретний, персоніфікований характер. Отже, мета обробки персональних даних обумовлює цілі, для реалізації яких фізичною особою може надаватися згода на використання конкретної інформації [192, с. 59].

Зміна визначеної мети обробки персональних даних на нову мету, яка є несумісною з попередньою, тягне за собою необхідність отримати згоду суб'єкта персональних даних на обробку його даних відповідно до зміненої мети. З цього приводу в літературі зазначається, що критерій сумісності/несумісності є суто відносним, що створює передумови для його вільного тлумачення як володільцями персональних даних, так і суб'єктами юрисдикційних повноважень. Дана обставина зумовлює ризик маніпуляцій, у ході яких первинна (узгоджена із суб'єктом персональних даних) мета обробки інформації без його згоди може бути змінена на іншу, зовні подібну, але відмінну по суті. Натомість пропонується, щоб будь-які зміни в цільовому призначенні обробки персональних даних узгоджувалися з їх суб'єктом [193, с. 115]. Дозволимо собі не погодитись із цією пропозицією, оскільки вона не

узгоджується зі стандартами захисту персональних даних в ЄС. Власне критерій «несумісність встановленим цілям» є імплементованим положенням п. b ч. 1 ст. 5 Загального регламенту про захист даних [49]. Підтвердженням цього також служить практика Суду ЄС. Прикладом є справа Deutsche Telekom AG v. Germany [**Error! Reference source not found.**], яка стосувалася питання необхідності отримувати нову згоду суб'єктів персональних даних при зміні назви третьої особи, якій такі дані передавались. Суд ЄС постановив, що не було необхідності в отриманні нової згоди, тому що суб'єкти персональних даних мали можливість надати згоду тільки для цілей здійснення обробки, які полягали в оприлюдненні їхніх даних, і не могли вибирати між різними адресними книгами, в яких могли бути надруковані ці дані. Тобто, «сумісність»у даному контексті є оціночним поняттям та може бути встановлена щодо кожного випадку окремо.

Наступною умовою дійсності згоди суб'єкта персональних даних є її однозначність. Так, згода повинна бути явно вираженою, зрозумілою та безсумнівною. З цієї ж причини згода повинна очевидно походити від конкретного суб'єкта персональних даних, при цьому не залишаючи сумнівів щодо його дозволу на обробку персональних даних [190, с. 120–121]. Така вимога змушує володільця персональних даних створювати механізм надання фізичними особами згоди, який би забезпечував, щоб така згода була або безпосередньо виражена, або випливала з поведінки суб'єкта персональних даних. Тобто, дії суб'єкта повинні приводити до безпомилкового висновку про надання ним згоди. Однак, це залежить від того, наскільки повну, достовірну та своєчасну інформацію, що дала можливість прийняти відповідне рішення, отримав суб'єкт персональних даних. При цьому, згода суб'єкта персональних даних не може випливати із його бездіяльності чи мовчання, оскільки мовчанню та бездіяльності притаманна неоднозначність [187]. Тому із двох застосовуваних моделей отримання згоди суб'єкта персональних даних – «opt out» (полягає у тому, що володілець персональних даних не повинен вводити в

оману суб'єктів стосовно обробки їх даних, а останні, в свою чергу, повинні мати можливість відмовитися від подальшоїобробки) та «opt in» (правомірною є тільки та обробка персональних даних, що здійснюється після попередньо отриманої згоди суб'єктів персональних даних) – стандартам ЄС відповідає лише остання.

Потрібно також зауважити, що умова однозначності стосується згоди і як загальної підстави для обробки персональних даних (п. 1 ч. 1 ст. 11 Закону України «Про захист персональних даних»), і як підстави для обробки так званих чутливих категорій даних (п. 1 ч. 2 ст. 7 Закону України «Про захист персональних даних»). Проте, в останньому випадку вимоги до такої згоди є підвищеними. Це обумовлено Загальним регламентом про захист даних [49], який використовує два різних терміни для позначення однозначності згоди суб'єкта персональних даних: «*unambiguous*» – як загальна вимога; «*explicit*» – для обробки чутливих категорій даних. По суті, це означає, що згода на обробку чутливих категорій даних повинна бути явно вираженою, тоді як згода, що випливає із дій суб'єкта персональних даних, не може бути підставою для обробки чутливих категорій даних [188]. На жаль, переклад цих термінів, здійснений Центром перекладів актів Європейського права при Міністерстві юстиції України та розміщений на сайті Верховної Ради України, не в повній мірі відображає вказану відмінність («недвозначно дав свою згоду» та «дав свою недвозначну згоду» відповідно). Тому використання вітчизняним законодавцем терміну «однозначна згода» лише щодо особливих вимог обробки персональних даних слід тлумачити як намагання підкреслити, що в цьому випадку суб'єкт персональних даних має безпосередньо та недвозначно надати дозвіл на обробку саме чутливих категорій даних [188].

Умови дійсності згоди суб'єкта персональних даних обумовлюють вимоги до її об'єктивованої форми. У першій редакції відповідного положення Закону України «Про захист персональних даних» вимагалось, щоб волевиявлення фізичної особи щодо надання дозволу на обробку її

персональних даних було документоване, зокрема, письмове, що, як нами було встановлено, не відповідало вище вказаним європейським стандартам. У подальшому, внаслідок неодноразових змін, ця вимога була значно спрощена [195; **Error! Reference source not found.**]. Сьогодні закон встановлює фактично єдину вимогу щодо форми згоди суб'єкта персональних даних, а саме: така форма повинна давати змогу зробити висновок про надання згоди (абзац четвертий ч. 1 ст. 2). Так, згода суб'єкта персональних даних може бути вчинена в письмовій формі, як правило, у вигляді окремого документу (згода на обробку персональних даних), або як одна з умов договору. Також згода суб'єкта персональних даних може бути надана шляхом конклюдентних дій, тобто, якщо його поведінка засвідчує волю на обробку персональних даних, зокрема, шляхом проставлення відмітки про надання дозволу на обробку своїх персональних даних під час реєстрації в інформаційно-телекомунікаційній системі суб'єкта електронної комерції. Щодо усної форми згоди, то фактично вона не заборонена, однак навряд чи усна форма зможе надати володільцю змогу підтвердити наявність згоди впродовж всього часу здійснення обробки персональних даних. Вказане тлумачення підтверджується комплексним аналізом положень ст.ст. 2, 6 та 11 Закону. Інше розуміння є недопустимим, оскільки передбачатиме існування ситуацій, коли персональні дані оброблятимуться начебто на підставі згоди, яка нічим не підтверджується. Така обробка не має законних підстав, а відтак є незаконною [81, с. 61]. Як вже було встановлено, згода суб'єкта персональних даних не може виражатися її мовчанням. Згода, вчинена у формі, що не відповідає зазначеним вимогам, не може бути підставою правомірної обробки персональних даних.

Національне законодавство, так само як і стандарти ЄС, не визначають безпосередньо момент, коли згода повинна бути надана. Однак, з аналізу та тлумачення окремих положень можна встановити, що згода повинна бути надана до того, як процес обробки персональних даних почнеться. Тобто отримання згоди на обробку персональних даних до початку самої обробки є

найголовнішою умовою правомірності такої обробки. При цьому, якщо обробка персональних даних була розпочата без згоди суб'єкта персональних даних, законодавство не надає йому можливість схвалити таку обробку згодом [188].

Окремо слід зазначити, що концепція «згоди» отримала новий розвиток відповідно до Загального регламенту про захист даних. Насамперед, було вдосконалено визначення поняття «згода суб'єкта персональних даних» шляхом нормативного закріплення такої умови дійсності як однозначність. Крім того, уточнено, що згода може бути надана у формі: письмової, в тому числі – з використанням електронних засобів, або усної заяви; безсумнівних підтверджувальних дій шляхом проставляння відмітки про надання згоди при відвідуванні сайту, вибору технічного налаштування при отриманні інформаційних послуг. Вказані важливі доповнення фактично випливають із застосованих ще відповідно до Директиви 95/46/ЄС вимог та демонструють спадковість правового регулювання [188].

Крім того, Загальний регламент про захист даних окремо встановлює умови дійсності згоди:

1) обов'язок доказування факту надання суб'єктом персональних даних згоди та її меж покладається на володільця персональних даних;

2) якщо згода надається як письмова заява, що містить також інші положення (які не стосуються обробки персональних даних), то така згода повинна бути представлена в манері, яка дозволяє чітко вирізнити її серед інших положень, в зрозумілій та легко доступній формі, із використанням зрозумілої та простої мови;

3) відкличність згоди визнається однією з умов її дійсності. Так, згода суб'єкта персональних даних може бути відкликана у будь-який момент. При цьому відкликання згоди не впливає на правомірність обробки персональних даних, яка йому передувала;

4) при оцінці добровільності згоди необхідно до брати уваги, серед іншого, й те, чи виконання договору було обумовлене наданням згоди на

обробку персональних даних, що не є обов'язковою для виконання такого договору [188].

Також Загальний регламент про захист даних регулює порядок надання згоди, якщо суб'єктом персональних даних є неповнолітня фізична особа: 1) неповнолітні, які досягли 16 років (законодавством країни цей вік може бути зменшений, але не молодше 13 років) самостійно надають згоду на обробку персональних даних; 2) згоду на обробку персональних даних фізичної особи, яка не досягла вказаного віку надають батьки (усиновлювачі), опікуни, піклувальники; 3) володілець персональних даних повинен вжити розумних заходів для того, щоб перевірити, що згода надається законними представниками малолітніх та неповнолітніх дітей.

Таким чином, під згодою суб'єкта на обробку персональних даних слід розуміти добровільне, поінформоване, конкретне, однозначне волевиявлення фізичної особи даних у письмовій формі або іншій формі, в тому числі – у формі конклюдентних дій, що, безсумнівно, підтверджує її дозвіл на обробку персональних даних відповідно до сформульованої мети їх обробки.

3.2 Підстави захисту прав суб'єкта персональних даних

Частина перша ст. 8 Закону України «Про захист персональних даних» проголошує особисті немайнові права на персональні дані непорушними. По суті, йдеться про закріплення принципу непорушності права на персональні дані. Цей принцип є галузевим втіленням принципу непорушності прав і свобод людини (ст. 21 Конституції України). У найбільш загальному розумінні цей принцип означає захист персональних даних від необґрунтованого втручання як держави, так й інших осіб, та охоплює щонайменше два положення. Наприклад, за підсумками першого року функціонування GDPR, наглядові органи країн європейської економічної зони зафіксували понад 144 тис запитів та скарг і понад 89 тис порушень даних. 63% із них були закриті, а 37%, станом

на травень 2019 р., – тривали [196]. Як наслідок запровадження GDPR, у січні цього року на італійського постачальника електроенергії та газу Eni Gas e Luce (EGL) були накладені штрафи в розмірі 8,5 млн та 3 млн євро. Перший за те, що компанія незаконно обробляла особисті дані, здійснюючи маркетингові дзвінки особам, які відмовилися від отримання таких дзвінків, а другий – за укладення контрактів із понад 7 тис клієнтів без їх повідомлення. Вони дізнавалися про це здебільшого після отримання першого рахунку від компанії. А на початку травня 2019 р. шведський орган управління захисту даних (DPA) наклав штраф у розмірі 75 мільйонів шведських крон (приблизно 7 мільйонів євро) на Google як оператора пошукової системи за невиконання вимог GDPR щодо вилучення персональних даних через неточність або оскільки така інформація була зайвою [196].

Також варто пам’ятати, що, з одного боку, ніхто не може зазнавати протиправного втручання в його право на персональні дані чи обмежень у його здійсненні. З іншого боку, суб’єкт права на персональні дані може бути обмежений у його здійсненні лише у випадках і в порядку, встановлених законом.

ЦК України в ч. 1 ст. 15 обумовлює право на захист суб’єктивного цивільного права, в тому числі й права на персональні дані, його порушенням, невизнанням або оспоренням. Розуміння вказаних понять, тобто порушення, невизнання та оспорювання суб’єктивного цивільного права, базується на тому, що усі вони є складовими більш широкого поняття – «підстави захисту суб’єктивного цивільного права» [197, с. 168], або, як їх ще називають, тріади підстав захисту суб’єктивних цивільних прав [198, с. 182]. Спільним для них є те, що вони полягають у посяганні на суб’єктивне цивільне право. Під посяганням прийнято розуміти непередбачений законом вплив на суб’єктивне право учасника цивільного обороту, що полягає у запереченні суб’єктивного права уповноваженої особи та виявляється у формах невизнання права, оспорювання права, порушення права [198, с. 189]. Відтак, підстави захисту

суб'єктивних цивільних прав визначають момент, з якого особа – носій відповідного суб'єктивного права має можливість реалізувати своє повноваження щодо захисту вказаного права [6, с. 181].

У найбільш загальному вигляді дані поняття розкриті, на наш погляд, Ю. В. Білоусовим, який вважає, що під поняттям «порушення» слід розуміти такий стан суб'єктивного права, при якому воно зазнало протиправного впливу з боку правопорушника, внаслідок якого суб'єктивне право зазнало зменшення або знищення; під поняттям «невизнання» – дії учасників цивільного правовідношення, що несе юридичний обов'язок перед уповноваженою особою, що спрямовані на заперечення в цілому або в певній частині суб'єктивного права іншого учасника цивільних правовідносин, внаслідок якого уповноважена особа позбавлена можливості реалізувати своє право; а під поняттям «оспорення» – такий стан цивільного правовідношення, при якому між учасниками існує спір з приводу наявності чи відсутності суб'єктивного права у сторін, а також приналежності такого права певній особі [199, с. 29]. Вказані визначення можуть бути застосовані й щодо підстав захисту персональних даних.

Очевидним є те, що особливості правової природи персональних даних як об'єкта цивільних правовідносин, з одного боку, та правової природи права на персональні дані як суб'єктивного цивільного права, з іншого боку, обумовлюють специфіку підстав їх захисту. Наприклад, О. П. Радкевич класифікує цивільні правопорушення у сфері обігу персональної інформації в мережі Інтернет на такі види: незаконне, свавільне втручання у сферу особистого й приватного життя та його таємницю (збирання, зберігання й розповсюдження інформації конфіденційного характеру); порушення права на таємницю кореспонденції в мережі Інтернет (отримання незаконного доступу до електронної документації); порушення права особи, яку зображено на фотографіях та в інших художніх творах у мережі Інтернет (використання фото-, відео-матеріалів із протиправною метою) [200, с. 16]. Попри те, що така

класифікація виконує важливе наукове завдання, вона не володіє ознакою універсальності, а тому не може бути використана для розкриття усієї різноманітності порушень права на персональні дані.

Варто зазначити, що чинне законодавство поряд із поняттям «порушення прав суб'єкта персональних даних» містить також пов'язане із ним поняття «порушення законодавства про захист персональних даних» (або подібне, але нетотожне – «порушенням вимог Закону України «Про захист персональних даних»). Так, «порушення законодавства про захист персональних даних» визнаються підставою для застосування суб'єктом персональних даних засобів правового захисту (п. 9 ч. 2 ст. 8 Закону України «Про захист персональних даних»), а також підставою для встановленої законом відповідальності (ст. 28 Закону України «Про захист персональних даних») [201]. Системний аналіз свідчить, що вказані поняття мають відмінний зміст та обсяг, а тому не є тотожними. Зокрема, «порушенням законодавства про захист персональних даних» може бути: неповідомлення або несвоєчасне повідомлення Уповноваженого Верховної Ради України з прав людини про обробку персональних даних або про зміну відомостей, що підлягають повідомленню згідно із законом, повідомлення неповних чи недостовірних відомостей; 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. Вказані «порушення законодавства про захист персональних даних» не завжди будуть призводити до «порушення прав суб'єкта персональних даних». Тобто, ці поняття співвідносяться як родове та видове, при цьому «порушення прав суб'єкта персональних даних» є видом «порушенням законодавства про захист персональних даних», однак не вичерпує зміст останнього [201].

Закон України «Про захист персональних даних» називає такі види порушень права на персональні дані: незаконна обробка; втрата; знищення;

пошкодження; приховування; ненадання чи несвоєчасне їх надання; надання відомостей, що є недостовірними чи ганьблять честь, гідність та ділову репутацію фізичної особи (п. 7 ч. 2 ст. 8); незаконне відстрочення або відмова у доступі до персональних даних (ст. 18); незаконний доступ до персональних даних (ч. 1 ст. 24). Системний аналіз вказаного закону дозволяє зробити висновок, що цей перелік не може вважатися повним, оскільки порушення прав суб'єкта персональних даних може також полягати у: незаконному ненаданні відомостей про джерела збирання, місцезнаходження своїх персональних даних, мету їх обробки, місцезнаходження або місце проживання (перебування) володільця чи розпорядника персональних даних; незаконному ненаданні інформації про умови надання доступу до персональних даних, зокрема, інформації про третіх осіб, яким передаються його персональні дані; ненаданні інформації про механізм автоматичної обробки персональних даних; незаконному автоматизованому рішенні, що має для суб'єкта персональних даних правові наслідки; незаконному неповідомленні суб'єкта персональних даних про дії з персональними даними (зокрема, про передачу персональних даних третій особі, а також про зміну, видалення чи знищення персональних даних або обмеження доступу до них). Однак, і після цього перелік порушень прав суб'єкта персональних даних не може претендувати на вичерпність [201].

Певно, що найбільш поширеним порушенням права на персональні дані є їх незаконна обробка. Порушення права на персональні дані можливе, наприклад, коли журналісти, не запитавши дозволу відомої особи, знімають подробиці її особистого (інтимного) життя прихованою камерою [202, с. 209]. Обробка персональних даних є незаконною, коли вона відбувається за відсутності, принаймі, однієї з установлених Законом підстав для її проведення. Способи такої обробки відрізняються багатоманітністю. Ними є, перш за все, незаконне збирання, зберігання, накопичення, адаптування, зміна, розповсюдження, передача персональних даних [203, с. 37]. Відповідно до легального визначення, поняття «обробка персональних даних» розуміється як

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 (ст. 2 Закону України «Про захист персональних даних»). Крім того, закон також містить розкриття окремих дій з обробки персональних даних:

– збирання персональних даних є складовою процесу їх обробки, що передбачає дії з підбору чи впорядкування відомостей про фізичну особу (ч. 1 ст. 12);

– накопичення персональних даних передбачає дії щодо поєднання та систематизації відомостей про фізичну особу чи групу фізичних осіб або внесення цих даних до бази персональних даних (ч. 1 ст. 13);

– зберігання персональних даних передбачає дії щодо забезпечення їх цілісності та відповідного режиму доступу до них (ч. 2 ст. 13);

– використання персональних даних передбачає будь-які дії володільця щодо обробки цих даних, дії щодо їх захисту, а також дії щодо надання часткового або повного права обробки персональних даних іншим суб'єктам відносин, пов'язаних із персональними даними (ч. 1 ст. 10);

– поширення персональних даних передбачає дії щодо передачі відомостей про фізичну особу за згодою суб'єкта персональних даних, чи без згоди суб'єкта персональних даних або уповноваженої ним особи лише у випадках, визначених законом, і лише (якщо це необхідно) в інтересах національної безпеки, економічного добробуту та прав людини (ч. 1, 2 ст. 14) [201].

Таким чином, чинне законодавство не містить визначення поняття «порушення права на персональні дані». Натомість нормативно встановлюються окремі склади порушень прав на персональні дані, які за своєю природою можуть бути як цивільно-правовими, в тому числі деліктами, так і публічно-правовими. До останніх можна віднести: адміністративне

правопорушення – ст. 188-39 Кодексу України про адміністративні правопорушення [204] – порушення законодавства у сфері захисту персональних даних; злочин – ст. 182 Кримінального кодексу України [205] – порушення недоторканності приватного життя, а саме – незаконне збирання, зберігання, використання, знищення, поширення конфіденційної інформації про особу або незаконна зміна такої інформації.

Крім того, право на персональні дані може бути порушено в межах трудових правовідносин. Наприклад, якщо працівники суб'єктів відносин, пов'язаних із персональними даними, які здійснюють використання персональних даних відповідно до своїх професійних, службових або трудових обов'язків, допустять розголошення у будь-який спосіб персональних даних, які їм було довірено або які стали відомі у зв'язку з виконанням професійних, службових або трудових обов'язків [201].

До винного працівника в цьому разі можливе застосування лише одного з передбачених частиною першою ст. 147 КЗпП дисциплінарного стягнення – догани. Водночас, працівники підприємства (установи, організації), які не забезпечили зберігання персональних даних працівника, можуть бути притягнути роботодавцем до обмеженої матеріальної відповідальності на підставі ст. 132 КЗпП. Притягнення винного працівника до повної матеріальної відповідальності у цьому випадку не можливе, оскільки ст. 134 КЗпП встановлений вичерпний перелік випадків повної матеріальної відповідальності працівників [104, с. 252].

Новий підхід з цього приводу закріплено в Загальному регламенті про захист даних, який містить легальне визначення поняття «порушення захисту персональних даних» («personal data breach», що також може бути перекладено як «витік персональних даних»). Так, відповідно до п. 12 ч. 1 ст. 4 вказаного Регламенту під порушенням захисту персональних даних розуміють порушення безпеки, що призводить до випадкового чи незаконного знищення, втрати, пошкодження, несанкціонованого розкриття або доступу до персональних

даних, які передано, збережено або оброблено іншим чином. Необхідність запобігання витоку персональних даних пояснюється тим, що, якщо витік належним чином і своєчасно не буде усунуто, це може призвести до заподіяння фізичним особам майнової та моральної шкоди, такої як втрата контролю над персональними даними або обмеження їх прав, дискримінація, крадіжка ідентифікаційних даних або шахрайство з персональними даними, фінансові втрати, несанкціоноване скасування використання псевдонімів, приниження репутації, порушення конфіденційності персональних даних, захищених професійною таємницею, або будь-які інші істотні економічні або соціальні втрати для відповідних фізичних осіб.

При цьому види порушень захисту персональних даних можна пояснити таким чином:

– знищення – персональні дані більше не існують або не існують у формі, придатній для використання;

– пошкодження – персональні дані були змінені, перекручені чи частково втрачені;

– втрата – персональні дані все ще існують, але володілець втратив контроль або доступ до них, або персональні дані більше не знаходяться в його володінні;

– несанкціоноване розкриття або доступ – розкриття або доступ до персональних даних здійснюється особою, яка не уповноважена на це [206].

При нагоді зауважимо, що і цей перелік видів порушень захисту персональних даних не може вважатися вичерпним. Усі порушення захисту персональних даних можуть бути поділені на три типи:

– порушення конфіденційності – несанкціоноване або випадкове розкриття чи доступ до персональних даних;

– порушення цілісності – несанкціонована або випадкова зміна, перекручення персональних даних;

– порушення доступності – несанкціоноване або випадкове знищення чи втрата персональних даних.

При цьому необхідно зазначити, що, відповідно до конкретних обставин, порушення захисту персональних даних може одночасно об'єднувати порушення конфіденційності, цілісності та доступності, або будь-яку їх комбінацію [206]. Як приклад такого поєднання різних порушень можна навести реєстрацію фейкових сторінок у соціальних мережах із використанням персональних даних фізичної особи.

У літературі вказується, що вперше поняття «фейк» стало використовуватися стосовно соціальних мереж, і в цьому випадку воно має два значення. Фейк – це фальшива сторінка сайта або, точніше, фальшивий сайт, створений для крадіжки персональних даних, зокрема – паролів, котрі в подальшому будуть використовуватися для розсилки спаму. Друге значення слова пов'язане з підробленим акаунтом, що створюється на будь-якому сайті, де є реєстрація. Фейковий акаунт – це анкета неіснуючої людини або реальної людини, але без її відома й із використанням її персональних даних. У соціальних мережах досить розповсюджені випадки неправомірної реєстрації акаунту, тобто, під іменем особи, але без її відома та, відповідно, без отримання її згоди на це як відносно пересічних фізичних осіб, так і щодо фізичних осіб публічного права [207, с. 288–289]. Прикладом такого порушення є справа бразильського півзахисника донецького футбольного клубу «Шахтар» Жадсона, який подав до суду на соціальну мережу orkut, створену компанією Google, за підроблений профіль в orkut, що нібито належить футболістові. Так, у соціальній мережі orkut є профіль користувача на ім'я Жадсон Родригес. У розділі «про себе» вказано, що профіль належить футболістові «Шахтаря». Сфера інтересів користувача обмежується футболом. Користувач досить активний в соціальній мережі, у нього 135 друзів. Крім того, він регулярно оновлює розділ «фотографії». Також в соціальній мережі orkut є співтовариство, присвячене Жадсону [208].

Щодо інших підстав захисту права на персональні дані, а саме невизнання та оспорення, то в літературі наводять такі їх приклади. Прикладом невизнання права на персональні дані може слугувати ситуація, коли заклад охорони здоров'я може відмовити громадянину у наданні доступу до його медичної картки, таким чином не визнаючи його права на доступ до власних персональних даних [202, с. 209]. Право на персональні дані може бути оспорене, наприклад, володільцем персональних даних, який не надає особі копії певних документів стосовно її родичів із мотивів того, що такі документи не стосуються самої особи або містять конфіденційну інформацію про сторонніх осіб [202, с. 209]. Враховуючи, що право на персональні дані є особистим немайновим, яке належить кожній фізичній особі, та є невід'ємним, зазначимо, що невизнання чи оспорення не може стосуватися права на персональні дані як такого або в цілому. Натомість, беручи до уваги охарактеризований вище взаємозв'язок права на персональні дані з іншими особистими немайновими правами, слід допустити можливість невизнання та (або) оспорення інших особистих немайнових прав, інформація про які відображається в персональних даних фізичної особи (таких як право на ім'я, індивідуальність, особисті папери, зображення тощо). Крім того, оспорення може стосуватися самого факту належності персональних даних тій чи іншій фізичній особі, тобто наявності відомостей, які допускають пряму чи опосередковану ідентифікацію фізичної особи [201].

На сьогодні в науковій літературі достатньо активно обговорюється питання про розширення переліку підстав захисту суб'єктивних цивільних прав. Зокрема, ґрунтуючись на аналізі чинного законодавства Р. О. Стефанчук приходить до висновку, що підставами цивільно-правового захисту можуть стати ще, принаймні, дві обставини: зловживання правом (ст. 12, 13 ЦК України), про що ми вже говорили вище, а також наявність небезпеки (ст. 282 ЦК України) та створення загрози життю, здоров'ю, майну фізичної особи або майну юридичної особи (ст. 1163-1165 ЦК України) [6, с. 181]. Твердження про

розширення переліку підстав захисту отримує своє підтвердження і на рівні законодавства про захист персональних даних. Так, п. 7 ч. 2 ст. 8 Закону України «Про захист персональних даних» встановлює право суб'єкта персональних даних на захист від випадкової втрати, знищення, пошкодження. А ч. 1 ст. 24 Закону України «Про захист персональних даних» закріплює кореспондуючий обов'язок володільців, розпорядників персональних даних та третіх осіб забезпечити захист цих даних від випадкових втрати або знищення. По суті, йдеться про покладання на володільців, розпорядників персональних даних та третіх осіб ризику їх випадкової втрати, знищення, пошкодження, та одночасно визнання такого ризику підставою захисту прав суб'єкта персональних даних.

Із цього приводу варто зауважити, що категорія «ризик» не має однозначного розуміння в теорії цивільного права. Одні автори, прихильники теорії «суб'єктивного ризику» вважають, що ризик – це психічне ставлення суб'єктів до результатів власних дій або до поведінки інших осіб, а також до можливого результату об'єктивного випадку і випадкових неможливих дій, які виражають в усвідомленому припущенні негативних, у тому числі не відшкодованих, майнових наслідків [209, с. 77]. Крім того, у наукових джерелах ризик розглядається як об'єктивна категорія, тобто, як можливість втрати майнових або особистих немайнових благ [210, с. 145], як можлива небезпека [211, с. 33], не стільки можлива, скільки ймовірна шкода [212, с. 47]. Також можна виділити концепцію двоаспектного ризику, що ґрунтується на тезі про взаємодію двох концепцій і визначення суб'єктивного ризику поряд із об'єктивним як збірної категорії, що одночасно поєднує в собі суб'єктивні і об'єктивні елементи [213, с. 81]. Екстраполюючи останню концепцію на предмет нашого дослідження, зазначимо, що ризик випадкової втрати, знищення, пошкодження персональних даних, слід розглядати: як об'єктивну категорію в розумінні змісту обов'язку забезпечення захисту персональних

даних; як суб'єктивну категорію в значенні підстави для захисту прав суб'єкта персональних даних.

Необхідність захисту персональних даних від будь-якого несанкціонованого, в тому числі випадкового, доступу підтверджується також практикою ЄСПЛ. Для прикладу можна привести справу I v. Finland [100]. До Європейського суду звернулася особа, що була хворою на СНІД. Вона проходила лікування у лікарні, де вона і працювала. В певний момент інформація про діагноз заявниці стала відомою широкому колу працівників лікарні. Вона, звернулася за захистом своїх прав до суду. Їй було відмовлено в задоволенні скарг. Суди визнали, що інформацію було незаконно поширено кимось із працівників лікарні. Однак, інформація щодо того, хто міг це зробити, зокрема, хто переглядав дані заявниці, не зберігалася лікарнею.

У цій справі ЄСПЛ встановив, що відсутні твердження стосовно будь-якого навмисного розголошення медичних даних заявниці, що могло б представляти собою втручання в її право на повагу до її приватного життя. Крім того, заявниця не заперечує факт збору та збереження її медичної інформації. Її скарга скоріше стосується неспроможності лікарні гарантувати захист даних заявниці від несанкціонованого доступу, або, в термінах Конвенції, порушення позитивного зобов'язання держави щодо забезпечення поваги до її приватного життя за допомогою впровадження системи правил і гарантій щодо захисту даних. У цьому контексті ЄСПЛ прийшов до правового висновку, що для гарантування захисту персональних даних потрібен практичний і ефективний механізм, який би, щонайперше, нівелював саму можливість будь-якого несанкціонованого доступу.

Покладання на володільців, розпорядників персональних даних та третіх осіб ризику випадкових втрати або знищення персональних даних має ще одне значення, а саме розподіл обов'язку доказування. У цій же справі I v. Finland [100] ЄСПЛ встановив, що заявниця програла цивільну справу через те, що не змогла довести по фактах справи причинно-наслідкового зв'язку між

недоліками в правилах безпеки доступу та поширенням інформації про стан її здоров'я. Проте, перенесення такого тягаря доказування на заявницю свідчить про ігнорування відомих на той момент недоліків в системі ведення документації в лікарні.

3.3 Форми та способи захисту прав суб'єкта персональних даних

Захист прав суб'єкта персональних даних, як і будь-яких суб'єктивних цивільних прав, здійснюється у відповідних формах захисту із застосуванням певних способів захисту. Методологічно будемо виходити із того, що під формою захисту розуміється комплекс внутрішньо погоджених організаційних заходів по захисту суб'єктивних прав і охоронюваних законом інтересів [214, с. 350]. При цьому прийнято розрізняти юрисдикційну та неюрисдикційну форми захисту. Відмінність між цими формами захисту полягає, як мінімум, у двох ознаках.

Першою ознакою виступає суб'єкт, який здійснює захист. В неюрисдикційній формі захисту сам суб'єкт персональних даних здійснює діяльність щодо їх захисту, самостійно, без звернення за допомогою до державних чи інших компетентних органів. Юрисдикційна форма захисту передбачає діяльність уповноважених державою органів щодо захисту порушених прав суб'єктивних персональних даних. Таким чином, суть її полягає в тому, що суб'єкт персональних даних звертається за захистом до державних чи інших компетентних органів, котрі уповноважені прийняти необхідні заходи для відновлення порушеного права і припинення правопорушення [202, с. 210].

Друга ознака вказує на порядок здійснення захисту. Так, при юрисдикційній формі процедура здійснення способів захисту чітко визначена законом, наприклад, в рамках процесуального законодавства. Тут обмежуються і можливості дій суб'єкта персональних даних, який звернувся за захистом

порушеного права, оскільки застосування заходів захисту здійснюється державним органом. У разі неюрисдикційної форми, свобода дії суб'єкта персональних даних є значно ширшою [214, с. 350].

Неюрисдикційна форма захисту прав суб'єкта персональних даних має низку особливостей. По-перше, інформаційна природа персональних даних зумовлює пріоритетне значення використання саме неюрисдикційної форми захисту порушених прав у порядку самозахисту [215, с. 350]. Право на самозахист суб'єкта персональних даних від порушень і протиправних посягань випливає зі ст. 19 ЦК України, та охоплює застосування ним засобів протидії, які не заборонені законом та не суперечать моральним засадам суспільства. Так, суб'єкт персональних даних може вжити заходів як для усунення вже наявного порушення, так і для попередження можливих посягань на його персональні дані. Наприклад, він може встановити спеціальне програмне забезпечення на своєму комп'ютері, що блокуватиме доступ до веб-сайтів, котрі запускають спеціальні програми для збирання персональних даних, або вдатися до криптографічних засобів захисту даних – спеціальних математичних та алгоритмічних засобів захисту персональних даних, що передаються за допомогою систем і мереж зв'язку, зберігаються і обробляються в комп'ютерах із використанням різних методів шифрування [202, с. 210].

З огляду на питання захисту персональних даних у мережі Інтернет, важливо враховувати керівні принципи, викладені в Рекомендації № (99) Комітету Міністрів Ради Європи щодо захисту недоторканості приватного життя в Інтернеті [216], які містять рекомендації користувачам щодо правил поведінки умережі Інтернет та постачальникам послуг Інтернету. Так, серед рекомендацій користувачам потрібно виокремити такі:

– необхідно використовувати всі доступні засоби для захисту даних та ліній зв'язку, як, наприклад, легально доступні засоби шифрування для конфіденційності електронної пошти, коди доступу до власного персонального комп'ютера;

– будь-яка трансакція, будь-яке відвідуваннясайту залишає в інтернеті так звані «сліди». Подібні «електронні сліди» можуть бути використані без відома суб'єкта персональнихданих для створення профілю пронього і його інтересів. Варто використовувати новітні технічні досягнення, що дозволяють проінформувати суб'єкта персональних даних про будь-який випадок можливості залишення відповідних «слідів», і дають йому змогу відмовитися від подальших дій;

– найкращий спосіб забезпечення недоторканності приватного життя – це анонімний доступ і анонімне використання послуг, анонімні засоби здійснення платежів. Якщо це можливо, слід з'ясовувати наявність технічнихзасобів для забезпечення анонімності. Повна анонімність не завжди можлива через певні законодавчі обмеження. У такому випадку, якщо це дозволено законодавством, варто використовувати псевдонім, що дозволить знати персональні дані суб'єкта тільки постачальникові послуг Інтернету;

– необхідно повідомляти постачальникові послуг Інтернету чи будь-кому іншому тільки ті дані, які необхідні для виконання певних дій, про які суб'єкт заздалегідь поінформований.Особлива обережність необхідна при використанні кредитних карток і номерів рахунків, які в Інтернеті можуть легко стати об'єктом зловживань;

– необхідно з обережністю ставитись до сайтів, де просять інформацію особистого характеру більшу, ніж це потрібно для доступу чи здійснення трансакції, чи не вказують для чого така інформація необхідна взагалі.

По-друге, законодавство України не тільки передбачає права суб'єкта персональних даних на самозахист, але й встановлює обов'язок володільців, розпорядників персональних даних та третіх осіб забезпечити захист цих даних (ч. 1 ст. 24 Закону України «Про захист персональних даних»). Зміст такого обов'язку охоплює собою навіть захист від випадкових втрати або знищення, від незаконної обробки, у тому числі незаконного знищення чи доступу до персональних даних. Це положення повністю відповідає

європейським стандартам, розглянутими нами вище (ст. 7 Конвенції про захист осіб у зв'язку з автоматизованою обробкою персональних даних; ст. 17 Директиви 95/46/ЄС; ст. 25 Загального регламенту про захист даних). По суті, ця норма покладає на володільця, розпорядника персональних даних та третіх осіб ризик випадкового порушення права на персональні дані. Пояснюється це тим, що персональні дані охороняються в режимі конфіденційної інформації, що виключає їх випадкове або несанкціоноване псування або випадкову їх втрату, а також несанкціонований доступ до них, їх зміну, блокування, передачу [217, с. 42]. Крім того, при деяких процесах обробки існує імовірність певних ризиків для прав і свобод суб'єктів даних в силу їхньої природи, їхнього обсягу чи їхніх цілей, як, наприклад, позбавлення фізичних осіб права, допомоги чи контракту, або через особливе використання нових технологій. Це в сукупності обумовило покладання обов'язку забезпечення встановленого режиму захисту персональних даних на сторону, що поширює ці дані, а також обов'язку сторони, якій передаються персональні дані, попередньо вжити заходів щодо забезпечення їх захисту (ч. 3, 4 Закону України «Про захист персональних даних»).

Захист від таких ризиків має здійснюватися на всіх етапах їх обробки, у тому числі за допомогою організаційних та технічних заходів. Так, організаційні заходи охоплюють: визначення порядку доступу до персональних даних працівників володільця/розпорядника; визначення порядку ведення обліку операцій, пов'язаних із 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 (п. 3.4 Типового порядку обробки персональних даних). Спеціальні технічні заходи забезпечення безпеки обробки персональних даних застосовуються, у тому числі, й щодо виключення несанкціонованого доступу до персональних даних, що обробляються, та у роботі технічного і програмного

комплексу, за допомогою якого здійснюється обробка персональних даних (п. 3.14 Типового порядку обробки персональних даних [175]).

По-третє, законодавство України передбачає такі спеціальні способи самозахисту права на персональні дані, як: 1) пред'являти вмотивовану вимогу володільцю персональних даних із запереченням проти обробки своїх персональних даних (п. 5 ч. 2 ст. 8 Закону України «Про захист персональних даних»); 2) 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 (п. 6 ч. 2 ст. 8 Закону України «Про захист персональних даних»). Про поширеність таких способів самозахисту інформаційних прав як звернення потерпілого до правопорушника з вимогою припинити незаконне втручання вказує у своїх працях А. О. Кодинець. Ефективність таких способів вчений обґрунтовує тривалістю судового розгляду спорів та адміністративної процедури захисту, а також труднощами у процесуальному доведенні факту правопорушення чи пошуку винного суб'єкта [215, с. 331].

Порядок пред'явлення вказаних вимог та їх розгляду, а також наслідки такого розгляду в Законі України «Про захист персональних даних» не регламентуються, а натомість визначаються п. 2.12 – 2.14 Типового порядку обробки персональних даних [175]. Форма таких вимог повинна бути письмовою, принаймні в силу прямої вказівки ч. 1 ст. 20 Закону України «Про захист персональних даних» для вимоги про внесення змін до персональних даних, та в силу застосування цієї норми та аналогії до інших вимог. На жаль, ні Закон, ні Типовий порядок не встановлюють правила, яким би мав відповідати зміст таких вимог. Вважаємо за можливе застосувати з цього приводу ч. 4 ст. 16 Закону України «Про захист персональних даних» як аналогію закону. Таким чином, у вимозі суб'єкта персональних даних повинно бути зазначено: 1) прізвище, ім'я та по батькові, місце проживання (місце перебування) і реквізити документа, що посвідчує суб'єкта персональних даних

як фізичну особу; 2) відомості про базу персональних даних, стосовно якої подається вимога, чи відомості про володільця чи розпорядника персональних даних; 3) перелік персональних даних, щодо яких пред'явлено вимогу; 4) мета та/або правові підстави для вимоги.

Ключовою ознакою вимог суб'єкта персональних даних є їх вмотивованість. В літературі поняття вмотивованості в цьому контексті пояснюється на прикладі, якщо мова йде про отримання суб'єктом рекламних повідомлень від володільця, для того, щоб виправити неточності в імені чи інших даних, суб'єкту достатньо просто вказати на неточність. Якщо ж зміна інформації про суб'єкта матиме вагомі юридичні наслідки, володілець має право вимагати від суб'єкта підтвердження того, що персональні дані дійсно потрібно змінити. При цьому на заявника не повинен покладатися надмірний тягар доведення того, що персональні дані підлягають зміні [81, с. 89]. Отже, поняття «вмотивована вимога» є оціночним терміном, зміст якого підлягає встановленню з урахуванням обставин кожної окремої справи. Оскільки законодавчо не визначені критерії вмотивованості вимоги, доцільно вважати вимогу вмотивованою, якщо вона містить достатні правові підстави для, відповідно, зміни, видалення чи знищення, або припинення обробки персональних даних. Такими підставами є:

– для зміни персональних даних – доведення того, що персональні дані суб'єкта (їх частина) є недостовірними;

– для знищення персональних даних – встановлення одного з таких фактів: 1) закінчення строку зберігання даних, визначеного згодою суб'єкта персональних даних на обробку цих даних або законом; 2) припинення правовідносин між суб'єктом персональних даних та володільцем чи розпорядником, якщо інше не передбачено законом; 3) видання відповідного припису Уповноваженого або визначених ним посадових осіб секретаріату Уповноваженого; 4) набрання законної сили рішенням суду щодо видалення

або знищення персональних даних; 5) зібрання персональних даних з порушенням вимог законодавства про захист персональних даних;

– для заперечення проти обробки персональних даних – доведення незаконності обробки персональних даних суб'єкта (їх частини).

При цьому ми критично ставимось до твердження: «Перш ніж передавати справи до судів, слід звертатися до володільця… Права … (маються на увазі права суб'єкта персональних даних – уточнено мною – Ю. Б.) повинні дотримуватись, передовсім, володільцем. Звернення до національного наглядового органу або безпосередньо до суду не допоможе, оскільки такий орган може лише порадити спершу звернутися до володільця, а суд визнає заяву неприйнятною» [87, с. 129]. Оскільки це суперечить рішенню Конституційного Суду України від 9 липня 2002 року у Справі про досудове врегулювання спорів, відповідно до якого право особи (громадянина України, іноземця, особи без громадянства, юридичної особи) на звернення до суду за вирішенням спору не може бути обмежене законом, іншими нормативно-правовими актами. Встановлення законом або договором досудового врегулювання спору за волевиявленням суб'єктів правовідносин не є обмеженням юрисдикції судів і права на судовий захист [218]. А обов'язковість досудового порядку урегулювання спору може бути визначена тільки законом України (ч. 4 ст. 124 Конституції України [219]). У той же час, суб'єкт персональних даних повинен мати право на ефективний спосіб судового захисту від порушень з боку володільця та/або розпорядника персональних даних, якщо він вважає, що його права на такі дані були порушені в результаті обробки його персональних даних із порушенням вимог законодавства (як це передбачено в ст. 79 Загального регламенту про захист даних).

Юрисдикційна форма захисту полягає в зверненні із заявою, скаргою чи в іншій формі суб'єкта персональних даних до компетентного державного органу, в тому числі суду, який уповноважений застосувати заходи, спрямовані на припинення та попередження правопорушення, відновлення порушеного

права чи компенсацію заподіяної порушенням шкоди. Вказана форма включає в себе загальний (судовий) та спеціальний (адміністративний) порядок захисту [202, с. 210]. Адміністративний порядок захисту персональних даних на сьогодні забезпечується діяльністю Уповноваженого Верховної Ради України з прав людини. Так, відповідно до ч. 1 ст. 22 Закону України «Про захист персональних даних», Уповноважений Верховної Ради України з прав людини здійснює контроль за додержанням законодавства про захист персональних даних у межах повноважень, передбачених законом. Процедуру здійснення Уповноваженим Верховної Ради України з прав людини контролю за додержанням вимог законодавства про захист персональних даних встановлено Порядком здійснення Уповноваженим Верховної Ради України з прав людини контролю за додержанням законодавства про захист персональних даних, затвердженим Наказом Уповноваженого Верховної Ради України з прав людини від 08 січня 2014 р. № 1/02-14 [220].

Незважаючи на те, що наявність незалежного контрольного (наглядового) органу у сфері захисту персональних даних відповідає європейським стандартам (ст. 28 Директиви 95/46/ЄС; ст. 51 – 59 Загального регламенту про захист даних), в науковій літературі зустрічається обґрунтована критика підходу до такого органу у вітчизняному законодавстві. Наприклад, К. С. Мельник стверджує, що покладена в основу Закону України «Про захист персональних даних» ідея включення інституту Омбудсмена в механізм здійснення завдань та функцій центральних органів виконавчої влади, що забезпечують формування та реалізацію державної політики у сфері персональних даних (контроль у приватному секторі/прийняття нормативно-правових актів) та наділення його не властивими повноваженнями у цій сфері є такою, що не повною мірою узгоджується з відповідними положеннями Конституції України [221, с. 119]. У будь-якому разі, функціонування такого наглядового органу повинно забезпечувати дві можливості: кожен суб’єкт даних повинен мати право подачі скарги в наглядовий орган, якщо вважає, що

обробка його персональних даних порушує законодавство; кожна фізична або юридична особа повинна мати право на ефективний засіб судового захисту відносно юридично обов'язкового для неї рішення наглядового органу.

Отже, саме судова форма захисту персональних даних вважається загальною, оскільки юрисдикція судів поширюється на будь-який спір, що виникає з приводу персональних даних (ч. 3 ст. 124 Конституції України), а право суб'єкта персональних даних на судовий захист гарантовано Конституцією України (ч. 1 ст. 55). Важливим у цьому контексті є висновок, до якого прийшла О. В. Кохановська, про те, що термінологічна база Закону України «Про персональні дані» відповідає приватно-правовому розумінню основного суб'єкта відносин захисту персональних даних, і це заслуговує на схвалення, оскільки дає змогу захистити права цієї особи приватно-правовими способами захисту в суді, а також є найбільш ефективними, виконують компенсаційну і відновлювану функцію, дозволяють відшкодувати шкоду, в тому числі й моральну [33**Error! Reference source not found.**, с. 31]. Подальше обґрунтування така позиція знаходить у працях А. О. Кодинця, який стверджує, що використання адміністративних механізмів не означає неможливість застосування для регулювання інформаційних відносин у сфері персональних даних приватноправових засад. У разі неправомірного поширення персональних даних правопорушник може бути притягнутий до цивільно-правової відповідальності у вигляді відшкодування збитків, компенсації моральної шкоди чи в іншій формі. Інструментарій цивільного права застосовується незалежно від адміністративно-правових механізмів регламентації інформаційної сфери, в тому числі незалежно від того, чи були включені персональні дані особи до відповідної бази, чи була вона належним чином зареєстрована тощо [215, с. 31].

Ці наукові погляди знаходять своє підтвердження в судовій практиці, де зустрічаються позови про захист права на персональні дані: 1) від протиправного збирання, накопичення, зберігання, використання персональних

даних, наприклад, щодо правомірності направлення адвокатських запитів і дотримання у зв'язку з цим адвокатським об'єднанням положень Закону України «Про захист персональних даних» [222]; 2) шляхом забезпечення дотримання встановленого законом порядку доступу до персональних даних, зокрема, на отримання довідки про забезпеченість житловою площею та комунальними послугами [223]; 3) від пролонгованого порушення у формі протиправного поширення персональних даних (наприклад, вимога припинити порушення особистих немайнових прав – зняти з дошки оголошень гуртожитку Державного закладу післядипломної освіти «Центр підвищення кваліфікації керівних працівників та спеціалістів промисловості» повідомлення із персональними даними (ПІП, адреси з номером кімнати, суми заборгованості) і припинити розповсюдження цих же персональних даних перед третіми особами без згоди суб'єкта персональних даних) [224]; 4) шляхом притягнення до цивільної відповідальності у формі відшкодування моральної шкоди, спричиненої поширенням конфіденційної інформації [225] тощо.

У вітчизняній цивілістиці зазначається, що універсальність судової форми захисту полягає в тому, що вона може надати суб'єкту даних широкий спектр способів захисту свого права [202, с. 210]. В основу нашого подальшого дослідження буде покладена така позиція, відповідно до якої під способом захисту суб'єктивних цивільних прав розуміються закріплені в законі матеріально-правові заходи примусового характеру, за допомогою котрих відбувається поновлення (визнання) порушених (оспорюваних) прав і вплив на правопорушника [214, с. 367]. Багатогранність правової природи права на персональні дані як суб'єктивного права, а також широке тлумачення змісту та обсягу поняття «персональні дані» як об'єкта права, обумовлюють складну систему способів їх захисту. Будучи суб'єктивним цивільним правом, право на персональні дані може захищатися будь-яким із загальних цивільно-правових способів. Відповідно до ч. 2 ст. 16 ЦК України, способами захисту, які можуть бути застосовані до будь-яких цивільних прав, в тому числі і права на

персональні дані, належать: визнання права; визнання правочину недійсним; припинення дії, яка порушує право; відновлення становища, яке існувало до порушення; примусове виконання обов'язку в натурі; зміна правовідношення; припинення правовідношення; відшкодування збитків та інші способи відшкодування майнової шкоди; відшкодування моральної (немайнової) шкоди; визнання незаконними рішення, дій чи бездіяльності органу державної влади, органу влади Автономної Республіки Крим або органу місцевого самоврядування, їхніх посадових і службових осіб; інший спосіб, що встановлений договором або законом чи судом у визначених законом випадках.

Поряд із загальними, в літературі прийнято виділяти спеціальні способи захисту, тобто такі, які застосовують для захисту окремих видів суб'єктивних цивільних прав. Оскільки право на персональні дані розглядається як самостійне особисте немайнове право, то йому притаманні усі способи захисту останніх. Так, Р. О. Стефанчук пропонує таку класифікацію способів захисту особистих немайнових прав: превентивно-пресікальні способи захисту, тобто ті з них, які спрямовані на попередження та припинення порушення, оспорення, невизнання особистого немайнового права чи реальної загрози вказаних дій (визнання права; припинення дії, яка порушує право; зміна правовідношення; припинення правовідношення; визнання незаконними рішення, дій чи бездіяльності органу державної влади, органу влади Автономної Республіки Крим або органу місцевого самоврядування, їхніх посадових і службових осіб тощо); відновлювальні способи захисту, тобто ті з них, які спрямовані на відновлення порушеного права (відновлення становища, яке існувало до порушення, та пов'язані із ним способи; спростування; відповідь; визнання правочину недійсним тощо); компенсаційні способи захисту, тобто ті з них, які спрямовані на додаткове компенсування збитків, що пов'язані із порушенням особистого немайнового права (відшкодування збитків та інші способи відшкодування майнової шкоди, відшкодування моральної (немайнової) шкоди тощо) [6, с. 194]. Значення цієї класифікації полягає в тому, що вона сприяє

вибору належного способу захисту права на персональні дані з урахуванням характеру порушення та його наслідків.

У той же час, право на персональні дані може захищатися в порядку, передбаченому для захисту інформаційних прав. Кодинець А. О. з цього приводу пропонує виокремити ті способи, що можуть застосовуватися, насамперед, для захисту прав: учасників відносних інформаційних відносин (зміна правовідношення; припинення правовідношення, визнання правочину недійсним; примусове виконання обов'язку в натурі); учасників абсолютних інформаційних прав (визнання незаконними рішення, дії чи бездіяльності органу державної влади, органу влади Автономної Республіки Крим або органу місцевого самоврядування, їхніх посадових і службових осіб; припинення дії, котра порушує право; визнання права); способи, придатні для захисту прав учасників як у відносних (зобов'язальних), так і в абсолютних відносинах (відновлення становища, яке існувало до порушення; відшкодування збитків та інші способи відшкодування майнової шкоди; відшкодування моральної (немайнової) шкоди) [215, с. 374–375]. Попри дещо умовний характер цієї класифікації, вона дозволяє розмежувати два випадки: захист права на персональні дані від порушень, які допускають володільці та/або розпорядники персональних даних (відносні відносини); захист права на персональні дані від порушень з боку інших осіб (абсолютні відносини).

Аналіз вказаних норм свідчить, що вони потребують певної систематизації, оскільки наділені вадами неповноти (зрозуміло, що право на оскарження охоплює й інші протиправні дії чи бездіяльність володільця або розпорядника персональних даних, а не тільки рішення про відстрочення або відмову в доступі) та відсутність чіткого розмежування між ними (наприклад, «право суб'єкта персональних даних на захист своїх персональних даних» та «право суб'єкта персональних даних застосовувати засоби правового захисту») [226]. На основі проведеного дослідження пропонуємо таку систему спеціальних способів захисту права на персональні дані.

По-перше, шляхом звернення до володільця та/або розпорядника персональних даних (неюрисдикційна форма) із вмотивованою вимогою:

– із запереченням проти обробки персональних даних;

– про зміну персональних даних;

– про знищення персональних даних;

– про припинення будь-яких інших порушень законодавства про захист персональних даних.

По-друге, шляхом оскарження до Уповноваженого Верховної Ради України з прав людини діяльності володільця, розпорядника, третіх осіб щодо обробки персональних даних, а саме:

– 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.

По-третє, шляхом звернення до суду з позовом:

– зобов'язати володільця та/або розпорядника персональних даних надати доступ до персональних даних;

– зобов'язати володільця та/або розпорядника персональних даних припинити обробку персональних даних, змінити персональні дані, знищити персональні дані;

– щодо застосування інших цивільно-правових способів для 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 [226].

Отже, основними спеціальними способами захисту права на персональні дані можна назвати вимоги: про припинення обробки персональних даних; про зміну персональних даних; про знищення персональних даних. При цьому, вони можуть бути реалізовані як в юрисдикційній, так і неюрисдикційній формі [226].

Так, суб'єкт персональних даних має право заперечувати проти їх обробки. Якщо такі заперечення обґрунтовані, володілець повинен припинити обробку її персональних даних. Інколи зустрічається твердження, що така вмотивована вимога суб'єкта персональних даних виключає можливість їх подальшої обробки, а отже – й зберігання володільцем і розпорядником. З огляду на це, єдино можливим правовим наслідком такої вимоги є знищення інформації [193, с. 118]. Однак, припинення використання персональних даних може відбуватися в різних формах, зокрема, шляхом їх знищення, блокування або без них. У літературі знищення даних визначається як їх цілковите та безповоротне видалення (наприклад, спалення документа). Поняття «блокування» пов'язується з відокремленням тим чи іншим чином певних даних від інформації, що підлягає обробці. Припинення використання шляхом блокування може мати місце, коли знищення даних неможливе з фізичних або нормативних причин (наприклад, фінансова звітність про анульовані банківські перекази), а також, коли в контексті певних правовідносин блокування є більш доцільним. Наприклад, британські асоціації прямого маркетингу не видаляють, а блокують дані громадян, які заявили про своє бажання не отримувати адресних рекламних пропозицій. Це пояснюється, зокрема, тим, що в разі видалення таких даних вони можуть знову бути помилково внесені до системи, змушуючи як громадянина, так і асоціацію вживати додаткових зусиль для їх повторного виключення [28**Error! Reference source not found.**, с. 147–148]. Прецедентним у контексті видалення та заперечення проти обробки персональних даних стало вже проаналізоване нами вище рішення Суду Європейського Союзу від 13 травня 2014 року у справі Google Spain SL, Google

Inc. v. Agencia Española de Protección de Datos (AEPD), Mario Costeja González [156].

Право особи пред'являти вимогу про зміну або знищення її персональних даних деталізується у ст. 15 Закону України «Про захист персональних даних», відповідно до якої «персональні дані видаляються або знищуються в порядку, встановленому відповідно до вимог закону. Персональні дані підлягають видаленню або знищенню у разі 1) закінчення строку зберігання даних, визначеного згодою суб'єкта персональних даних на обробку цих даних або законом або 2) припинення правовідносин між суб'єктом персональних даних та володільцем чи розпорядником, якщо інше не передбачено законом. Персональні дані, зібрані з порушенням вимог цього Закону, підлягають видаленню або знищенню у встановленому законодавством порядку». Крім цього, відповідно до ч. 1 та ч. 3 ст. 20 Закону України «Про захист персональних даних», володільці чи розпорядники персональних даних зобов'язані вносити зміни до персональних даних на підставі вмотивованої письмової вимоги суб'єкта персональних даних. Зміна персональних даних, які не відповідають дійсності, проводиться невідкладно з моменту встановлення невідповідності.

Реалізація цих норм може бути продемонстрована на прикладі рішення Вищого господарського суду України від 15 березня 2017 року у справі № 910/12950/16 [227]. Відповідно до обставин справи, 06.04.2010 ПАТ КБ «ПриватБанк» (банк) та ФОП ОСОБА_2 (клієнт) уклали договір банківського рахунку на комплексне обслуговування (далі – договір), згідно з яким клієнту у Печерській філії ПАТ КБ «ПриватБанк» відкрито поточний банківський рахунок у національній валюті. Клієнтом при відкритті рахунків була надана згода на збирання та обробку персональних даних. 06.04.2016 клієнт цінним листом з описом вкладення надіслав до ПАТ КБ «Приватбанк» вимогу (претензію) про розірвання договору банківського рахунка, видалення та знищення персональних даних, а також заяву про закриття поточного рахунку,

яка залишилась без відповіді банку. Залишаючи касаційну скаргу без задоволення, Суд враховував, що нормами чинного законодавства передбачено право клієнта в будь-який час подати заяву про закриття рахунку, що, в свою чергу, є підставою для розірвання договору банківського рахунку. Отже, господарські суди попередніх інстанцій дійшли правильного висновку щодо наявності підстав для задоволення вимог позивача про розірвання договору банківського рахунку на комплексне обслуговування від 06.04.2010; зобов'язання закрити поточний рахунок, відкритий у Печерській філії ПАТ КБ «ПриватБанк»; та, як наслідок зобов'язання, знищити всі персональні дані, отримані на підставі згоди клієнта під час дії договору банківського рахунку на комплексне обслуговування від 06.04.2010 [226].

Окремо слід розглянути питання відшкодування (компенсації) шкоди (як майнової, так і моральної), завданої порушенням права на персональні дані. Насамперед, звертає на себе увагу той факт, що Закон України «Про захист персональних даних» не містить норм, які би безпосередньо закріплювали право суб'єкта персональних даних на відшкодування такої шкоди. З одного боку, це не відповідає європейським стандартам, а саме ст. 82 Загального регламенту про захист даних (ст. 23 Директиви 95/46/ЄС), в яких закріплено, що будь-яка особа, якій завдано шкоди в результаті незаконної обробки чи будь-якої дії, несумісної із законодавством про захист персональних даних, має право на одержання компенсації від володільця та/або особи, яка обробляє персональні дані, за завдану шкоду. З іншого боку, це не позбавляє суб'єкта персональних даних можливості звернутися до суду з позовом про відшкодування майнової та/або моральної шкоди із застосуванням загальних підстав, а саме ст. 1166 та 1167 ЦК України.

Відшкодування шкоди традиційно відносять до тих способів захисту, які одночасно виступають засобами цивільно-правової відповідальності за порушення законодавства про захист персональних даних, під котрою розуміють вид юридичної відповідальності, що полягає у покладанні на

правопорушника негативних наслідків у вигляді обов'язку відшкодування чи компенсації шкоди (матеріальних збитків та / або моральної шкоди) чи інших обов'язків, спрямованих на поновлення порушеного права персональних даних [215, с. 379]. Згідно з доктриною цивільного права, умовами цивільно-правової відповідальності є: 1) протиправність поведінки (дії чи бездіяльності); 2) наявність майнової та (або) моральної шкоди; 3) причинно-наслідковий зв'язок між протиправною поведінкою і заподіяною шкодою; 4) вина особи, яка заподіяла шкоду. Проаналізуємо особливості цих умов в контексті відшкодування шкоди, заподіяної порушенням права на персональні дані.

Протиправність поведінки як умова деліктної відповідальності полягає в порушенні права на персональні дані, що може проявитися: у незаконній обробці та випадковій втраті, знищенні, пошкодженні, умисному приховуванні, ненаданні чи несвоєчасному їх наданні, а також наданні відомостей, що є недостовірними чи принижують честь, гідність та ділову репутацію фізичної особи; недодержанні встановленого законодавством про захист персональних даних порядку захисту персональних даних, що призвело до незаконного доступу до них або іншого порушення прав суб'єкта персональних даних; незаконному збиранні, зберіганні, використанні, знищенні, поширенні персональних даних або незаконній зміні персональних даних тощо [226].

Порушенням права на персональні дані суб'єкту може бути заподіяна як моральна (може полягати у душевних стражданнях, яких фізична особа зазнала у зв'язку з протиправною поведінкою щодо неї самої, членів її сім'ї чи близьких родичів; у приниженні честі та гідності, а також ділової репутації фізичної особи), так і майнова шкода (реальні збитки та упущена вигода). У будь-якому разі сам факт заподіяння шкоди повинен бути встановлений. Прикладом може слугувати рішення колегії суддів судової палати у цивільних справах Апеляційного суду Автономної Республіки Крим від 21.01.2014 у справі № 106/5771/13-ц [225], яким скасовано рішення суду першої інстанції в частині стягнення на користь позивача відшкодування моральної шкоди з

ухваленням нового рішення про відмову у задоволені позову в цій частині. Рішення було обґрунтовано тим, що позивачем – із порушенням вимог процесуального законодавства – не надано належних та допустимих доказів заподіяння йому моральної шкоди поширенням інформації про його персональні дані, жодними доказами не доведено, що він зазнав у зв'язку з цим будь-яких немайнових втрат, душевних страждань, погіршення здоров'я, змін у життєвих стосунках тощо.

Важливою умовою відшкодування шкоди є наявність причинно-наслідкового зв'язку між протиправним діянням та заподіяною шкодою. Пояснимо це на прикладі рішення Голосіївського районного суду м. Києва від 08.06.2017 року у справі № 752/12262/15-ц [224]. Так, у процесі судового засідання встановлено, що позивач у справі страждає на ряд захворювань, серед яких гіпертонічна хвороба, а 26 червня 2015 року з ним стався гіпертонічний криз, який він переніс на ногах. У той же час, протиправні дії відповідача (оприлюднення персональних даних) щодо нього мали місце 10.06.2015 року. Беручи до уваги, що позивач страждає на ряд захворювань, а також розрив у часі між тим, коли мало місце відносно нього правопорушення, вчинене відповідачем та гіпертонічним кризом, що стався з ним, суд не може встановити, що причиною і гіпертонічного кризу були дії відповідача.

У той же час, розуміння права на персональні дані як одного з прав людини, гарантованого на рівні конституційних актів та міжнародних договорів вносить свої корективи щодо встановлення факту заподіяння шкоди та її спричинення протиправною поведінкою. На це звертає увагу Верховний Суд України в постанові від 27 вересня 2017 року у справі № 369/5585/15-ц [228]. Так, Верховний Суд України вказує, що відмовляючи у задоволенні заявлених вимог з підстав недоведеності спричинення шкоди, суди фактично поклали на позивача обов'язок довести наявність у нього душевних страждань із приводу порушення його права на таємницю телефонного спілкування, що є неприпустимим з огляду на правову природу такого права, гарантії від

порушень якого закріплені Конституцією України. У даному випадку суди мали б виходити із презумпції спричинення позивачу моральної шкоди відповідачем та обов'язку саме відповідача спростувати таку презумпцію [226].

Частина друга статті 1166 ЦК України встановлює презумпцію вини заподіювача шкоди, тобто особа, яка завдала шкоду, буде вважатися винною, якщо вона сама не доведе відсутність своєї вини. Тобто, у деліктних зобов'язаннях, в тому числі щодо відшкодування шкоди, завданої порушенням персональних даних, саме на відповідача покладено обов'язок спростування презумпції вини шляхом доведення відсутності його вини у завданні шкоди позивачу (якщо зазначена презумпція в суді не спростована, це є підставою для висновку про наявність вини відповідача – заподіювача шкоди).

У той же час, спеціальне законодавство може встановлювати додаткові гарантії захисту персональних даних окремих категорій осіб. Перш за все, до таких випадків слід віднести персональні дані працівників. Попри те, що Кодекс законів про працю України [61] навіть не використовує термін «персональні дані», він все ж містить норми, спрямовані на їх захист, а саме: заборону вимагати при укладенні трудового договору деякі відомості та документи (ст. 25); зміну формулювання причин звільнення, у разі визнання такого формулювання неправильним або таким, що не відповідає чинному законодавству, у випадках, коли це не тягне за собою поновлення працівника на роботі (ч. 3 ст. 235). Натомість проект Трудового кодексу України [229] виносить захист персональних даних працівника на рівень основних обов'язків роботодавця: надання на вимогу працівників повної та достовірної інформації щодо їхньої трудової діяльності, а також безоплатне надання працівникам копій документів, пов'язаних із виконанням трудових обов'язків, що містять їхні персональні дані (ч. 1 ст. 24); забезпечення захисту та конфіденційності персональних даних працівника в порядку, встановленому законодавством, а також у будь-який час на вимогу працівника ознайомлення його з

персональними даними, внесення змін до них у разі їх невідповідності фактичним даним (ч. 1 ст. 24).

Приклади спеціального захисту персональних даних можна знайти і в інших законодавчих актах: гарантії захисту та безпеки персональних даних виборців (ст. 11 Закону України «Про Державний реєстр виборців» [230]); права осіб, персональні дані (інформація про особу) яких внесені до Єдиного державного демографічного реєстру (ст. 9 Закону України «Про Єдиний державний демографічний реєстр та документи, що підтверджують громадянство України, посвідчують особу чи її спеціальний статус» [231]); Гарантії захисту та безпеки персональних та службових даних військовозобов'язаних (призовників) (ст. 10 Закону України «Про Єдиний державний реєстр військовозобов'язаних» [232]) тощо.

Крім того, суб'єкт персональних даних має право звертатися за захистом своїх прав і свобод до відповідних міжнародних судових установ, за умови використання всіх національних засобів юридичного захисту (Конституція України ч. 5 ст. 55). Особливу увагу в цьому контексті слід звернути на захист права на персональні дані в ЄСПЛ. Вище нами вже було встановлено, що практика ЄСПЛ визнає право на персональні дані таким, що охоплюється змістом ст. 8 ЄКПЛ, а саме правом на повагу до приватного і сімейного життя. При цьому, враховуючи концепцією горизонтального застосування прав людини, та відповідно до доктрини позитивних обов'язків держави забезпечити повагу до приватного життя, практика ЄСПЛ охоплює і випадки, коли право на персональні дані зазнає втручання не з боку держави, а збоку приватних осіб.

Наприклад, порушенням визнано відсутність заходів примусу постачальника послуг до розкриття особи, яка розшукується за розміщення непристойного оголошення про неповнолітню особу з використанням персональних даних останньої на сайті знайомств в Інтернеті (Case of K.U. v. Finland [233]). Так, У 1999 р. невідома особа розмістила оголошення сексуального характеру на сайті знайомств в Інтернеті від імені заявника, якому

було дванадцять років, і без його відома. Оголошення містило інформацію про вік, рік народження і фізичні характеристики заявника і вказувало, що він шукав інтимних стосунків з чоловіком. Воно також включало посилання на сторінку в Інтернеті, де можна було знайти його фотографію і номер телефону. Була подана скарга в поліцію, але постачальник послуг відмовився розкрити особу людини, що помістила оголошення, оскільки вважав себе зобов'язаним дотримувати правила про конфіденційність. Районний суд згодом відхилив зроблений на підставі Закону про карне розслідування запит поліції про видачу наказу, що зобов'язує постачальника послуг розкрити особу, що подала оголошення, ухваливши, що відсутнє положення закону, яке могло би бути використане для примусу постачальника послуг до недотримання професійної таємниці і до розкриття такої інформації в справах, менш тяжких злочинів, як, наприклад, наклеп.

ЄСПЛ, встановивши факт порушення ЄКПЛ, 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 ЄКПЛ (restitutio in integrum);

– інші заходи, передбачені у рішенні ЄСПЛ.

Висновки до Розділу 3

1. Згода суб'єкта персональних даних є проявом його можливості вільно визначати свою поведінку в сфері особистого життя, спрямованим на уповноваження володільця персональних даних на їх подальшу обробку, та на забезпечення контролю суб'єкта персональних даних за їх обробкою.

Згода суб'єкта персональних даних має, принаймні, три значення: 1) можливість фізичної особи діяти певним чином; 2) юридичний факт; 3) об'єктивована форма.

2. Згода суб'єкта персональних даних має усі ознаки одностороннього правочину: є дією особи (добровільним волевиявленням фізичної особи), спрямованою на набуття, зміну або припинення цивільних прав та обов'язків (щодо надання дозволу на обробку її персональних даних).

Об'єктивована форма згоди суб'єкта персональних даних повинна давати змогу зробити висновок про надання згоди та може бути вчинена: в письмовій формі, як правило, у вигляді окремого документу (згода на обробку персональних даних), або як одна з умов договору; шляхом конклюдентних дій, тобто, якщо його поведінка засвідчує волю на обробку персональних даних, зокрема, шляхом проставлення відмітки про надання дозволу на обробку своїх персональних даних під час реєстрації в інформаційно-телекомунікаційній системі суб'єкта електронної комерції.

3. Згода суб'єкта персональних даних відрізняється від інших підстав обробки персональних даних тим, що інші підстави обробки обтяжені додатковою умовою – «тестом на необхідність». Тобто, обробка персональних даних буде вважатися правомірною, якщо вона є необхідною для досягнення цілей, обумовлених у відповідній підставі. Якщо ж обробка персональних даних виходить за межі такої необхідності, то для її здійснення вже потрібна згода суб'єкта персональних даних. Водночас, отримання згоди суб'єкта персональних даних не звільняє їх володільця від обов'язку дотримуватись

загальних та особливих вимог до обробки персональних даних. Більше того, згода фізичної особи на обробку персональних даних не тягне за собою її відмову від прав суб'єкта персональних даних чи звуження їх змісту. Так само згода на обробку персональних даних не позбавляє та не обмежує можливості захисту персональних даних.

4. Виділено та охарактеризовано умови дійсності згоди суб'єкта персональних даних: добровільність, поінформованість, конкретність, однозначність. Вказані умови застосовуються у сукупності. Здійснено доктринальний аналіз умов дійсності згоди та порядку його надання, наведених у Загальному регламенті про захист даних.

5. Запропоновано при поділі підстав на види використовувати як критерій наявність чи відсутність згоди, а також враховувати, в чиїх інтересах здійснюється обробка персональних даних. Це дало змогу виділити чотири види таких підстав:

1) обробка персональних даних здійснюється за згодою суб'єкта персональних даних;

2) обробка персональних даних здійснюється в інтересах суб'єкта персональних даних, але незалежно від згоди останнього (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; захист життєво важливих інтересів суб'єкта персональних даних);

3) обробка персональних даних здійснюється незалежно від згоди суб'єкта персональних даних для задоволення публічних інтересів (дозвіл на обробку персональних даних, наданий володільцю персональних даних відповідно до закону, виключно для здійснення його повноважень; необхідність виконання обов'язку володільця персональних даних, передбаченого законом);

4) обробка персональних даних здійснюється в інтересах третіх осіб незалежно від згоди суб'єкта персональних даних за умови пропорційності

такого втручання в його особисте життя (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).

6. До підстав захисту прав суб'єкта персональних даних віднесено посягання на права суб'єкта персональних даних, які охоплюють: 1) порушення, в тому числі порушення безпеки обробки персональних даних, що призвело до їх випадкового чи незаконного знищення, втрати, пошкодження, несанкціонованого розкриття або доступу до персональних даних та спричинило порушення конфіденційності, цілісності та доступності таких даних; 2) невизнання, заперечення в цілому або в певній частині прав суб'єкта персональних даних, внаслідок якого він позбавлений можливості реалізувати свої права; 3) оспорення наявності чи відсутності прав суб'єкта персональних даних, приналежності таких прав певній особі, а також самого факту належності персональних даних тій чи іншій фізичній особі; 4) невизнання та (або) оспорення інших особистих немайнових прав, інформація про які відображається в персональних даних фізичної особи (таких як право на ім'я, індивідуальність, особисті папери, зображення тощо); 5) ризик випадкової втрати, знищення, пошкодження персональних даних.

7. Виділено типи порушення захисту персональних даних: 1) порушення конфіденційності – несанкціоноване або випадкове розкриття чи доступ до персональних даних; 2) порушення цілісності – несанкціонована або випадкова зміна, перекручення персональних даних; 3) порушення доступності – несанкціоноване або випадкове знищення чи втрата персональних даних. При цьому, порушення захисту персональних даних може одночасно об'єднувати порушення конфіденційності, цілісності та доступності або будь-яку їх комбінацію. Наприклад, реєстрація фейкових сторінок у соціальних мережах із використанням персональних даних фізичної особи.

Необхідність захисту персональних даних від будь-якого несанкціонованого, в тому числі випадкового, доступу підтверджується у роботі практикою ЄСПЛ.

8. Право на персональні дані може бути захищено як в неюрисдикційній, так і юрисдикційній формах.

9. Система спеціальних способів захисту права на персональні дані включає в себе: 1) звернення до володільця та/або розпорядника персональних даних (неюрисдикційна форма) з вмотивованою вимогою (із 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) оскарження до Уповноваженого Верховної Ради України з прав людини діяльності володільця, розпорядника, третіх осіб щодо обробки персональних даних (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 порушуються законодавство про захист персональних даних; 3) звернення до суду з позовом (зобов'язати володільця та/або розпорядника персональних даних надати доступ до персональних даних; зобов'язати володільця та/або розпорядника персональних даних припинити обробку персональних даних, змінити персональні дані, знищити персональні дані; щодо застосування інших цивільно-правових способів для 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.

Ключовою ознакою вимог суб'єкта персональних даних про захист є їх вмотивованість. Поняття «вмотивована вимога» є оціночним, оскільки його

зміст підлягає встановленню з урахуванням обставин кожної окремої справи. Запропоновано вважати вимогу вмотивованою, якщо вона містить достатні правові підстави для зміни, видалення, знищення, припинення обробки персональних даних.

10. За порушення права на персональні дані можуть застосовуватися такі заходи цивільно-правової відповідальності, як відшкодування майнової та моральної шкоди. Право на відшкодування шкоди надається суб'єкту персональних даних ст. 82 Загального регламенту про захист даних (ст. 23 Директиви 95/46/ЄС). Порядок застосування такої цивільно-правової санкції закріплено у главі 82 ЦК України.

Обґрунтовано необхідність при вирішенні справ щодо захисту прав на персональні дані виходити з презумпції спричинення позивачу моральної шкоди відповідачем, а також права відповідача спростувати таку презумпцію.

ВИСНОВКИ

У дисертації запропоновано теоретичне обґрунтування вирішення наукової проблеми цивільних правовідносин щодо персональних даних. Визначено правову природу, поняття та види персональних даних. Розкрито європейські стандарти цивільно-правового регулювання відносин щодо персональних даних. Виявлено особливості участі у відносинах щодо персональних даних осіб, які їх обробляють, а також підстави виникнення цивільних правовідносин щодо персональних даних. Визначено підстави, форми та способи захисту прав суб'єкта персональних даних. Обґрунтовано теоретичні положення та сформульовано конкретні пропозиції з удосконалення законодавства та правозастосування у сфері цивільних правовідносин щодо персональних даних.

Отримані узагальнювальні положення дисертаційного дослідження дали можливість сформулювати висновки та рекомендації, спрямовані на досягнення поставлених завдань:

1. Із позицій цивільно-правової доктрини запропоновано розуміти персональні дані як особисте немайнове благо фізичної особи. Хоча це благо характеризується немайновою природою, в силу сучасного рівня соціально-економічних відносин та специфіки інформаційного простору (у тому числі Інтернет-середовища) персональні дані об'єктивно можуть набувати майнової цінності. При цьому, відомості про фізичну особу самі по собі залишаються немайновим благом, оскільки не створюються в процесі виробництва та не мають фінансової вартості. Майнова цінність персональних даних обумовлена особистістю самої особи (наприклад, загальновідомої) або створюється в процесі обробки персональних даних. Така цінність полягає у економічній оборотоздатності персональних даних, що перетворює їх на особливо вразливий об'єкт цивільних правовідносин.

2. Право на персональні дані є цивільно-правовим за своєю природою, оскільки відносини, що виникають з приводу персональних даних, сповна відповідають ознакам, закріпленим в ч. 1 ст. 1 ЦК України. Це право є самостійним особистим немайновим правом, що обумовлено специфікою персональних даних як об'єкта цивільних правовідносин. Так, персональні дані є за своєю сутністю інформацією про фізичну особу, в тому числі – про її особисті немайнові блага та ознаки, котрі її індивідуалізують. Зазначене дозволило сформулювати у дослідженні пропозицію про доповнення змісту ЦК України новою статтею 302^1 Цивільного кодексу України.

Водночас підкреслено необхідність відмежовувати поняття «персональних даних» від суміжних йому понять: «інформація про особу», «відомості про особисте життя фізичної особи», «ознаки, що індивідуалізують фізичну особу». Головним для відмежування таких суміжних правових категорій є факт обробки відповідних відомостей. Тобто, відомості набувають правового режиму персональних даних внаслідок того, що стають предметом обробки.

3. Запропоновано визначення права на персональні дані як особистого немайнового права, що забезпечує соціальне буття фізичної особи, і специфіка котрого полягає в його об'єкті (персональні дані); меті (захист права на приватність та інших особистих немайнових прав у зв'язку з обробкою персональних даних); змісті (сукупності активних та пасивних правомочностей, а також правомочність захисту, які можуть бути реалізовані як в абсолютних, так і відносних правовідносинах).

4. Особиста немайнова природа персональних даних та їх взаємозв'язок з носієм, дозволив визначити суб'єктом персональних даних винятково фізичну особу, тобто, людину як учасника цивільних відносин, персональні дані якої обробляються, та яка наділена особистими немайновими правами на персональні дані, а тому виступає у правовідносинах щодо персональних даних управомоченою особою, правам якої кореспондують обов'язки інших

учасників. Здатність фізичної особи бути суб'єктом персональних даних виникає з моменту народження при здійсненні процедури її ідентифікації.

Важливим елементом цивільно-правового регулювання права на персональні дані є необхідність захисту персональних даних після смерті їх суб'єкта («посттанативні права»), що дозволило запропонувати поширення законодавства про захист персональних даних на відносини щодо обробки відомостей про померлу особу («посттанативні права»). У роботі сформульовано пропозицію доповнити статтею 4^{1}Закон України «Про захист персональних даних».

5. Аналіз європейських стандартів охорони персональних даних дозволив ствекрджувати, що найбільш повно вони відображені в Загальному регламенті про захист даних, норми якого слід розглядати у їх взаємозв'язку із положеннями Конвенції про захист прав людини і основоположних свобод і Конвенції Ради Європи про захист фізичних осіб при автоматизованій обробці персональних даних, які доповнюють і конкретизують їх зміст щодо здійснення та захисту права на персональні дані. В основу європейських стандартів захисту права на персональні дані покладено принципи, закріплені в Загальному регламенті про захист даних, а саме: законності, легітимної мети, пропорційності обробки персональних даних, актуальності персональних даних, обмеженого у часі зберігання персональних даних. Норма Загального регламенту про захист даних (як і аналогічна норма Директиви 95/46/ЄС) щодо заборони передавати персональні дані до країни, в якій не забезпечується належний рівень захисту персональних даних, зумовила транскордонний, навіть трансатлантичний вплив на зближення законодавства про захист персональних даних. Закон України «Про захист персональних даних» є фактично імплементацією стандартів Директиви 95/46/ЄС, а тому при тлумаченні його норм варто використовувати також і зміст відповідних норм Директиви. Станом на сьогодні назріла необхідність приведення положень

названого Закону у відповідність до нововведень Загального регламенту про захист даних.

Практика ЄСПЛ виробила критерії правомірного обмеження прав на персональні дані, що відповідають загальним принципам правомірного втручання в приватне життя: втручання відповідає закону; втручання здійснюється із легітимною метою; втручання є необхідним у демократичному суспільстві.

6. Поняття «суб'єкт персональних даних» є загальним, тобто своїм обсягом охоплює будь-яку фізичну особу, відомості про яку підлягають обробці, незалежно від типу правовідносин, в яких така обробка відбувається. Запропоновано поділ суб'єктів персональних даних на види. За класифікаційний критерій взято спеціальний правовий модус, який суб'єкт персональних даних набув у силу законодавства. Значення такого поділу полягає в тому, що той чи інший правовий модус може спричиняти зміну правового режиму персональних даних та (або) особливості здійснення та захисту особистих немайнових прав їх суб'єкта. Зрозуміло, що перелік таких правових модусів не може бути ані повним, ані вичерпним. Тому акцентуємо свою увагу лише на трьох із них, котрі фактично можуть стосуватися будь-якої фізичної особи: здобувач освіти, працівник, пацієнт.

Наголошено, що зміст права на персональні дані нині потребує доповнення новими правомочностями. До таких правомочностей віднесено право на мобільність та право на забуття. Право на мобільність персональних даних закріплено в ст. 20 Загального регламенту про захист даних. Причиною його запровадження є поширення обробки персональних даних в мережі Інтернет та необхідність забезпечити можливість вільного переміщення персональних даних від одного володільця (провайдера, соціальної мережі) до іншого. Зміст права на мобільність персональних даних включає в себе можливість суб'єкта персональних даних: отримати від володільця персональні дані у форматі, придатному для подальшого використання; передати такі

персональні дані іншому володільцю; вимагати від володільця безпосередньої передачі таких персональних даних іншому володільцю при технічній можливості. Право на забуття, зміст якого полягає у можливості суб'єкта персональних даних вимагати від володільця видалення даних, які його стосуються, частково визнає Закон України «Про захист персональних даних». Так, у Законі закріплюється: право суб'єкта персональних даних пред'являти вмотивовану вимогу щодо знищення своїх персональних даних будь-яким володільцем та розпорядником персональних даних, якщо ці дані обробляються незаконно чи є недостовірними (п. 6 ч. 2 ст. 8); підстави та умови видалення або знищення персональних даних (ч. 2, 3 ст. 15).

7. До осіб, які беруть участь у правовідносинах щодо персональних даних віднесено володільця персональних даних і розпорядника персональних даних.

Наголошено, що володілець характеризується такими ознаками як власна правосуб'єктність, має можливість діяти самостійно чи разом з іншими суб'єктами у випадках, коли два і більше суб'єкти визначають мету та засоби обробки персональних даних (співволодільці), спроможний визначати мету та інші умови обробки персональних даних.

Розпорядник персональних даних є факультативним (додатковим) суб'єктом правовідносин із приводу персональних даних, який є володільцем персональних даних або за законом йому надано право обробляти такі дані від імені володільця.

У відносинах обробки персональних даних беруть участь також треті особи, які: 1) не є стороною відносних правовідносин між суб'єктом даних та їх володільцем (розпорядником); 2) мають охоронюваний законом інтерес щодо персональних даних; 3) перебувають у правовідносинах із володільцем (розпорядником) щодо передачі даних; 4) об'єктом таких відносин виступають персональні дані одного і того ж суб'єкта персональних даних; 5) з моменту отримання персональних даних набувають статусу їх володільця чи розпорядника.

Поряд із третіми особами виділяють ще одного учасника відносин із приводу персональних даних – одержувача, яким визнається лише особа, якій передаються персональні дані, тоді як для третьої особи така ознака не обов'язкова.

8. До підстав виникнення цивільних правовідносин щодо персональних даних віднесено згоду суб'єкта персональних даних. Згода суб'єкта персональних даних є проявом можливості вільно визначати свою поведінку в сфері особистого життя, спрямованим на уповноваження володільця персональних даних на їх подальшу обробку та забезпечення контролю суб'єкта персональних даних за їх обробкою. Необхідність обробки персональних даних в інтересах третіх осіб, незалежно від згоди суб'єкта персональних даних, за умови пропорційності такого втручання в його особисте життя є єдиною підставою, яка відповідно до законодавства вимагає дотримання балансу між колідуючими інтересами. Тобто, вимагається одночасна наявність двох умов: необхідність захисту законних інтересів володільця персональних даних або третьої особи, якій передаються персональні дані; такі інтереси переважають потреби захисту основоположних прав і свобод суб'єкта персональних даних у зв'язку з обробкою його даних.

9. До підстав захисту прав суб'єкта персональних даних віднесено посягання на права суб'єкта персональних даних, що охоплюють різного роду порушення. Право на персональні дані може бути захищено як в неюрисдикційній, так і юрисдикційній формах.

Неюрисдикційна форма захисту прав суб'єкта персональних даних має низку особливостей: 1) пріоритетне значення використання самозахисту обумовлено інформаційною природою персональних даних; 2) на володільців, розпорядників і третіх осіб покладено обов'язок забезпечити захист персональних даних, навіть захист від випадкових втрати або знищення, від незаконної обробки, у тому числі незаконного знищення чи доступу до персональних даних; 3) суб'єкт персональних даних має право пред'явити

вмотивовану вимогу до володільця, розпорядника щодо припинення порушення своїх прав.

Юрисдикційна форма захисту персональних включає в себе загальний (судовий) порядок захисту, оскільки юрисдикція судів поширюється на будь-який спір, що виникає з приводу персональних даних, та спеціальний (адміністративний) порядок захисту, який сьогодні забезпечується діяльністю Уповноваженого Верховної Ради України з прав людини.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Цивільний кодекс України : Закон України від 16 січня 2003 року № 435-IV. База даних «Законодавство України» / ВР України. URL: http://zakon5.rada.gov.ua/laws/show/435-15.

2. Про інформацію : Закон України в редакції Закону № 2938-VI від 13.01.2011. *Відомості Верховної Ради України*. 2011. № 32. Ст. 313.

3. Про захист персональних даних : Закон України від 01.06.2010 р. № 2297–VI. *Офіційний вісник України*. 2010. № 49. Ст. 1604.

4. Сліпченко С. О. Місце об'єктів особистих немайнових правовідносин у системі об'єктів цивільного права. *Право і суспільство*. 2013. № 6.2. С. 92-97.

5. Кохановська О. В. Цивільно-правові проблеми інформаційних відносин в України : автореферат дис. ... д-ра юрид. наук : 12.00.03 Цивільне право, сімейне право, цивільний процес, міжнародне приватне право. Київ : Б. в., 2006. - 34 с.

6. Стефанчук Р. О. Особисті немайнові права фізичних осіб (поняття, зміст, система, особливості здійснення та захисту): Монографія / Відп. ред. Я. М. Шевченко. Київ : КНТ, 2007. 626 с.

7. Посикалюк О. О. До питання про об'єкт особистих немайнових прав фізичних осіб. *Юридична Україна*. 2009. № 5. С. 65-71.

8. Стефанчук Р. О. Захист честі, гідності та репутації в цивільному праві: Монографія. Київ : Науковий світ, 2001. 303 с.

9. Каретник О. С. До питання про правову природу персональних даних фізичної особи : цивілістичні аспекти. *Право України: Юридичний журнал*. 2014. № 9. С. 192-200.

10. Richard A. Posner. The Right of Privac. *Georgia Law Review*. 1978. Vol. 12. № 3. P. 393-422.

11. Information privacy law: Textbook / D. J. Solove, M. Rotenberg. N. Y., 2003. 795 p.

12. Романюк І. І. До поняття суб'єктивного права на власні персональні дані, його ознак і місця в системі особистих немайнових прав в Україні. *Науковий вісник Ужгородського національного університету : Серія: Право*. 2012. Вип. 20. Ч. 2. Т. 1. С. 233–237.

13. Посикалюк О. О. Особисті немайнові права фізичних осіб в романській, германській, англо-американській системах приватного права. Київ: Науково-дослідний інститут приватного права і підприємництва НАПрН України. 2011. 205 с.

14. Агарков М. М. Предмет и система советского гражданского права. *Избранные труды. Т. П. М*, 2002. С. 269-317.

15. Гражданское право: актуальные проблемы теории и практики /Под общ. ред. В.А. Белова. М.: Юрайт-Издат, 2007. 993 с.

16. Сліпченко С. О. Місце об'єктів особистих немайнових правовідносин у системі об'єктів цивільного права. *Право і суспільство*. 2013. № 6.2. С. 92-97.

17. Про доступ до судових рішень: Закон України від 22 грудня 2005 року № 3262-IV. *Відомості Верховної Ради України*. 2006. № 15. Ст. 128.

18. Про організацію формування та обігу кредитних історій: Закон України від 23 червня 2005 року № 2704-IV. *Відомості Верховної Ради України*. 2005. № 32. Ст. 421.

19. Про звернення громадян: Закон України від 2 жовтня 1996 року № 393/96-ВР. *Відомості Верховної Ради України*. 1996. № 47. Ст. 256.

20. Про телебачення і радіомовлення: Закон України в редакції Закону № 3317-IV від 12.01.2006. *Відомості Верховної Ради України*. 2006. № 18. Ст. 155.

21. Камінська Н. В. Захист персональних даних: проблеми внутрішньодержавного, наднаціонального і міжнародно-правового

регулювання. *Науковий вісник Національної академії внутрішніх справ*. 2015. № 3. С. 106-114.

22. Романюк І. І. Законодавчі та теоретичні підходи до визначення поняття персональних даних та відмежування його від суміжних понять. *Актуальні питання публічного та приватного права*. 2014. № 1. С. 82-90.

23. Аномалії в цивільному праві України : навч.-практ. посіб. / відп. ред. Р. А. Майданик. Київ : Юстініан, 2007. 912 с.

24. Серебряник, О. О. Інформація про особу як об'єкт цивільних прав : дис. ... канд. юрид. наук : 12.00.03. Івано-Франківськ, 2016. 209 с.

25. Рішення Конституційного Суду України у справі за конституційним поданням Жашківської районної ради Черкаської області щодо офіційного тлумачення положень частин першої, другої статті 32, частин другої, третьої статті 34 Конституції України від 20 січня 2012 року № 2-рп/2012 . *Офіційний вісник України*. 2012. № 9. Ст. 332.

26. Кардаш А. В. Інформація про особу та персональні дані: окремі аспекти співвідношення. *Форум права*. 2017. № 4. С. 87-92.

27. Красавчикова Л. О. Личная жизнь граждан под охраной закона. Москва : Юрид. лит., 1983. 160 с.

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

29. Стефанчук М. О. Цивільно-правові наслідки зміни соціально-індивідуалізуючих ознак фізичної особи. *Jurnalul juridicnaţional: teorie şipractică.* 2015. № 6. С. 153-156.

30. Волкова Н. В. Засоби індивідуалізації фізичних осіб (окремі аспекти). *Актуальні питання держави і права*. 2008. № 39.С. 238-243.

31. Конвенція про захист прав людини і основоположних свобод від 04.11.1950 р. База даних «Законодавство України» / ВР України. URL: http://zakon3.rada.gov.ua/ laws/show/995_004.

32. Про захист фізичних осіб при обробці персональних даних і про вільне переміщення таких даних: Директива 95/46/ЄС Європейського Парламенту і Ради від 24 жовтня 1995 року. База даних «Законодавство України» / ВР України. URL: http://zakon5.rada.gov.ua/laws/show/994_242.

33. Кохановська О. В. До питання про захист персональних даних в Україні. *Вісник Верховного Суду України*. 2011. № 6. С. 28-33.

34. Opinion 4/2007 on the concept of personal data, 01248/07/EN WP 136, Adopted on 20th June, Article 29 Data Protection Working Party URL : http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2007/wp136_en.pdf.

35. Великий тлумачний словник сучасної української мови (з дод. і допов.) / Уклад, і голов, ред. В. Т. Бусел. Київ; Ірпінь: ВТФ «Перун», 2005. 1728 с.

36. Мельник К. С. Теоретико-правовий зміст терміна «персональні дані». *Інформація і право*. 2013. № 3. С. 49-57.

37. Шишка Р. Б. До проблеми індивідуалізації фізичної особи. *Еволюція цивільного законодавства: проблеми теорії і практики. Матеріали міжнародної науково-практичної конференції*. 29-30квітня 2004 р., м. Харків. Київ : Академія правових наук України, НДІ приватного права і підприємництва, НДІ інтелектуальної власності, Національна юридична академія ім. Я. Мудрого, 2004. С.153-162.

38. Різак М. В. Класифікація персональних даних як необхідний елемент введення ефективної комунікації в суспільстві. *Науковий вісник Міжнародного гуманітарного університету*. 2013. Вип. 6-3 (1). С. 90-94.

39. Про доступ до публічної інформації: Закон України від 13 січня 2011 року № 2939-VI. *Офіційний вісник України*. 2011. № 10. Ст. 446.

40. Про авторське право і суміжні права: Закон України В редакції Закону № 2627-III від 11.07.2001. *Відомості Верховної Ради України*. 2001. № 43. Ст. 214.

41. Про правовий захист баз даних: Директива 96/9/ЄС Європейського Парламенту та Ради від 11 березня 1996 року. База даних «Законодавство України» / ВР України. URL: http://zakon3.rada.gov.ua/laws/show/994_241.

42. Серебряник О. О. Інформація про особу як об'єкт цивільних прав : автореф. дис. ... канд. юрид. наук : 12.00.03; Івано-Франків. ун-т права ім. короля Данила Галицького. Івано-Франківськ, 2016. 20 с.

43. Теремецький В. І. Суб'єкти відносин, пов'язаних з персональними даними. *Право і Безпека*. 2015. № 2. С. 171-176.

44. Про державну реєстрацію актів цивільного стану: Закон України від 1 липня 2010 року № 2398-VI. *Відомості Верховної Ради України*. 2010. № 38. Ст. 509.

45. Сопілко І. М. Механізм захисту персональних даних: проблеми та перспективи. *Юридичний вісник. Повітряне і космічне право*. 2013. № 2. С. 66-70.

46. Case of Odievre v. France, App. No.42326/98 URL: http://hudoc.echr.coe.int/eng?i=001-60935.

47. Про захист персональних даних : проект Закону України від 25.03.2008, № 2273. База даних «Законодавство України» / ВР України. URL: http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=32124

48. Про поховання та похоронну справу: Закон України від 10 липня 2003 року № 1102-IV. *Відомості Верховної Ради України*. 2004. № 7. Ст. 47.

49. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). URL: http://eur-lex.europa.eu/legalcontent/EN/TXT/PDF/?uri=CELEX:32016R0679&from=ENм

50. Data Protection Act, 16th July 1998. URL : https://www.legislation.gov.uk/ukpga/1998/29/pdfs/ukpga_19980029_en.pdf

51. Personal Data Act (1998: 204), Sweden, 29th April 1998. URL : http://arno.uvt.nl/show.cgi?fid=134865.

52. Personal Data Protection Act Promulgated State Gazette No. 1/4.01.2002, effective 1.01.2002, supplemented, SG No. 70/10.08.2004, effective 1.01.2005, SG No. 93/19.10.2004, No. 43/20.05.2005, effective 1.09.2005, amended and supplemented, SG No. 103/23.12.2005, amended, SG No. 30/11.04.2006, effective 12.07.2006, Bulgaria.URL : www.legislationline.org/documents/id/8515.

53. Act Of 6 August 2004 Relative To The Protection Of Individuals With Regard To The Processing Of Personal Data. URL : https://www.cnil.fr/sites/default/files/typo/document/Act78-17VA.pdf.

54. Personal Data Protection Act of the Republic Of Slovenia (No. 001-22-148/04), 15th July 2004. URL : http://ec.europa.eu/justice/data-protection/law/files/implementation/personal_data_protection_act_rs_2004.pdf.

55. Положення про Єдину державну електронну базу з питань освіти, в редакції постанови Кабінету Міністрів України від 12 липня 2017 р. № 550. База даних «Законодавство України» / ВР України. URL: http://zakon2.rada.gov.ua/laws/show/752-2011-%D0%BF

56. Булеца С. Б. Персональні дані пацієнта. *Науковий вісник Ужгородського національного університету*: Серія ПРАВО. Випуск 22. Частина 2. Том 1, 2014. С. 186-191.

57. Основи законодавства України про охорону здоров'я від 19 листопада 1992 року № 2801-XII. *Відомості Верховної Ради України*. 1993. № 4. Ст. 19.

58. Case of M.S. v. SWEDEN, Court (Chamber). Judgment (Merits and Just Satisfaction). 27.08.1997. App. No. 20837/92. URL: http://hudoc.echr.coe.int/eng?i=001-58177

59. Про державні фінансові гарантії медичного обслуговування населення: Закон України від 19 жовтня 2017 року № 2168-VIII. *Офіційний вісник України.* 2018. № 4.

60. Сенюта І. Я. Захист персональних даних у сфері охорони здоров'я: алгоритм змін. *Науковий вісник Херсонського державного університету. Серія «Юридичні науки»*. Випуск 6-1/2014. 2014. С. 216–221.

61. Кодекс законів про працю України, затверджений Законом № 322-VIII від 10.12.71. База даних «Законодавство України» / ВР України. URL: http://zakon2.rada.gov.ua/laws/show/322-08.

62. Чанишев Р. І. Міжнародні стандарти захисту персональних даних працівника і законодавство України. *Актуальні проблеми держави і права*. 2011. Вип. 57. С. 275-281.

63. Working document on a common interpretation of Article 26(1) of Directive 95/46/EC of 24 October 1995, 2093/05/EN WP 114, Adopted on 25 November 2005. URL: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2005/wp114_en.pdf

64. Щорічна доповідь Уповноваженого Верховної Ради України з прав людини про стан дотримання прав і свобод людини і громадянина в Україні, 2016. URL : http://www.ombudsman.gov.ua.

65. Лагутіна І. В. Юридичний механізм забезпечення особистих немайнових трудових прав працівників. Дисертація д-ра юрид. наук: 12.00.05, Нац. ун-т «Одес. юрид. акад.». Одеса, 2015. 390 с.

66. Порядок надання відомостей з Єдиного державного реєстру юридичних осіб, фізичних осіб – підприємців та громадських формувань, затверджений Наказом Міністерства юстиції України від 10.06.2016 № 1657/5. База даних «Законодавство України» / ВР України. URL: http://zakon0.rada.gov.ua/laws/show/z0839-16.

67. Порядок обробки персональних даних у базі персональних даних – Державному реєстрі фізичних осіб – платників податків, затверджений Наказом

Міністерства фінансів України від 24.02.2015 № 210. База даних «Законодавство України» / ВР України. URL: http://zakon2.rada.gov.ua/laws/show/z0278-15.

68. Про електронну комерцію: Закон України від 3 вересня 2015 року № 675-VIII . *Відомості Верховної Ради України*. 2015. № 45. Ст. 410

69. Про організацію формування та обігу кредитних історій: Закон України від 23 червня 2005 року № 2704-IV. *Відомості Верховної Ради України*. 2005. № 32. Ст. 421.

70. Конвенція про захист прав людини і основоположних свобод від 04.11.1950. База даних «Законодавство України» / ВР України. URL: http://zakon3.rada.gov.ua/ laws/show/995_004

71. Конвенція про захист осіб у зв'язку з автоматизованою обробкою персональних даних від 28 січня 1981 року. *Офіційний вісник України*. 2011. № 1. Ст. 85.

72. Брижко В. М. Захист персональних даних: реалії та практика сучасності. *Інформація і право*. 2013. № 3. С. 31-48.

73. 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 06.07.2010 р. № 2438–VI. *Офіційний вісник України*. 2010. № 58. Ст. 1994.

74. Пазюк А. В. Міжнародно-правове регулювання інформаційної сфери (теоретичні і практичні аспекти) : дис. ... д-ра юрид. наук : 12.00.11.; Київ. нац. ун-т ім. Т. Шевченка. Київ, 2016. 567 с.

75. Кравчук М. М. Конституційно-правові аспекти захисту персональних даних у мережі Інтернет. *Наукові записки Інституту законодавства Верховної Ради України.* 2013. №2. С. 40-45.

76. Брижко В. М. Сучасні основи захисту персональних даних в європейських правових актах. *Інформація і право*. 2016. № 3. С. 45-57.

77. Бєлова Ю.Д. Стандарти захисту права на персональні дані відповідно до Директиви 95/46/ЕС. *Часопис «Університетські наукові записки» Хмельницького університету управління та права*. 2017. № 3 (63). С. 130-139.

78. Safe Harbor Privacy Principles, issued by the U.S. Department of commerce on July 21, 2000. URL: https://rm.coe.int/16806af271.

79. 2000/520/EC: Commission Decision of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the safe harbour privacy principles and related frequently asked questions issued by the US Department of Commerce (notified under document number C(2000) 2441) (Text with EEA relevance.): URL: http://eur-lex.europa.eu/eli/dec/2000/520/oj.

80. Кирилюк О. Становление универсального международно-правового регулирования в сфере защиты персональных данных. *Legea si Viata*. 2015. № 11. С. 75-86

81. Захист персональних даних: правове регулювання та практичні аспекти : наук.-практ. посіб. / [Бем М. В. та ін.] ; Спіл. програма Європ. Союзу та Ради Європи «Зміцнення інформ. сусп-ва в Україні». Київ : К.І.С, 2015. 219 с.

82. Мельник К. С. Правові механізми захисту персональних даних в Європейському Союзі. *Правова інформатика*. 2013. № 4. С. 55-61.

83. Бєлова Ю.Д. Стандарти захисту права на персональні дані відповідно до практики ЄСПЛ. *Україна на шляху до Європи: реформа цивільного процесуального законодавства*. Зб. наук. праць Матеріали Міжнар. наук.-практ. конф. Київ: ВД Дакор, 2017. С. 86-89.

84. Case of Amann v. Switzerland, App. No.27798/95 URL: http://hudoc.echr.coe.int/eng?i=001-58497.

85. Case of Rotaru v. Romania, App. No.28341/95 URL: http://hudoc.echr.coe.int/eng?i=001-58586.

86. Case of Leander v. Sweden, App. No.9248/81 URL: http://hudoc.echr.coe.int/eng?i=001-57519.

87. Посібник з європейського права у сфері захисту персональних даних / [Агенція Європ. Союзу з питань основополож. прав (FRA), Рада Європи, Європ. суд з прав людини]. Київ : К.І.С, 2015. 215 с.

88. Case of Segerstedt-Wiberg and others v. Sweden, Application No. 62332/00. URL: http://hudoc.echr.coe.int/eng?i=001-75591.

89. Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the regions «A comprehensive approach on personal data protection in the European Union». URL : http://ec.europa.eu/justice/news/ consulting_public/0006/com_2010_609_en.pdf.

90. Баранов О. А., Брижко В. М. Захист персональних даних в сфері інтернет речей. *Інформація і право*. 2016. № 2. С. 85–91.

91. План заходів 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, затверджений постановою Кабінету Міністрів України від 25 жовтня 2017 р. № 1106. База даних «Законодавство України» / ВР України. URL: https://www.kmu.gov.ua/storage/app/uploads/public/5a9/ff6/48a/5a9ff648a9ed3343915004.doc.

92. Пилипчук В. Г., Брижко В. М. Трансформація системи захисту персональних даних та приватності в контексті євроінтеграції. *Вісник Національної Академії правових наук України*. 2017/2. № 3. С. 36-50.

93. Справа «Х та інші проти Росії», App. №. 78042/16 та 66158/14Документ у перекладі президента Спілки адвокатів України Олександра Дроздова та директора АБ «Дроздова та партнери» Олени

Дроздової. URL: https://www.echr.com.ua/translation/sprava-x-ta-inshi-proti-rosi%D1%97/

94. Case of Rotaru v. Romania, App. No.28341/95. URL: http://hudoc.echr.coe.int/eng?i=001-58586.

95. Роанья И. Защита права на уважение частной и семейной жизни в рамках Европейской конвенции о защите прав человека / Ивана Роанья. Воронеж: ООО Фирма «Элист», 2014 196 с.

96. Case of Gaskin v. The United Kingdom, App. № 10454/83. URL: http://hudoc.echr.coe.int/eng?i=001-57491

97. Case of K.H. and others v. Slovakia, App. №.32881. URL: http://hudoc.echr.coe.int/eng?i=001-145421.

98. Case of Haralambie v. Romania, App. №.21737/03. URL: http://hudoc.echr.coe.int/eng?i=002-1286.

99. Case of Odievre v. France, App. №.42326/98. URL: http://hudoc.echr.coe.int/eng?i=001-60935.

100. Case of I v. Finland, App. №.20511/03. URL: http://hudoc.echr.coe.int/eng?i=001-87510.

101. Case of Ciubotaru v. Moldova, App. №.27138/04. URL: http://hudoc.echr.coe.int/eng?i=001-98445.

102. Case of Segerstedt-Wiberg and others v. Sweden, Application. № 62332/00. URL: http://hudoc.echr.coe.int/eng?i=001-75591

103. Хартія основних прав Європейського Союзу від 07.12.2000 р. База даних «Законодавство України» / ВР України. URL: http://zakon3.rada.gov.ua/laws/show/994_524.

104. Шевчук С. Судовий захист прав людини: Практика Європейського суду з прав людини у контексті західної правової традиції. Вид. 2-е, випр., доп. Київ : Реферат, 2007. 848 с.

105. Посикалюк О. О. Захист права працівника на приватність в практиці Європейського Суду з прав людини. *Університетські наукові записки*. 2016. № 3. С. 112-124.

106. Ус М. В. Колізії суб'єктивних цивільних прав : автореферат дис. ... канд. юрид. наук : 12.00.03 Цивільне право і цивільний процес; сімейне право; міжнародне приватне право; Нац. ун-т «юрид. акад. України ім. Я. Мудрого». Х. : б. в., 2011. 20 с.

107. Посикалюк О. О. Захист особистих немайнових прав фізичної особи Європейським Судом з прав людини. *Університетські наукові записки*. 2008. № 3 (27). С. 124-128.

108. Консолідовані версії Договору про Європейський Союз та Договору про функціонування Європейського Союзу з протоколами та деклараціями від 07.02.1992, 25.03.1957. URL: http://zakon5.rada.gov.ua/laws/show/994_b06.

109. Бєлова Ю.Д. Поняття та зміст прав суб'єкта персональних даних. *Науково-практичний журнал Соціологія права*. 2017. № 3-4. С. 13-21.

110. КСУ визнав неконституційним надання Міністерству фінансів України права отримувати інформацію, що містить персональні дані. Інформація відділу комунікацій Конституційного Суду України та правового моніторингу. URL: http://www.ccu.gov.ua/novyna/ksu-vyznav-nekonstytuciynym-nadannya-ministerstvu-finansiv-ukrayiny-prava-otrymuvaty

111. Case of Satakunnan Markkinapörssi Oy and Satamedia Oy v. Finland. URL: http://hudoc.echr.coe.int/eng?i=001-175121.

112. Társaság a Szabadságjogokért v. Hungary. URL: http://hudoc.echr.coe.int/eng?i=001-92171.

113. Case of BREYER v. GERMANY, Application no. 50001/12. URL: https://www.statewatch.org/media/documents/news/2020/feb/echr-breyer-v-germany-sim-card-privacy-judgment-30-1-20.pdf

114. Мікуліна М. Щодо передачі персональних даних за запитами правоохоронних органів. *Підприємництво, господарство і право*. 2016. № 3. С. 37-42.

115. Борисова Л. В. Захист прав суб'єктів персональних даних. *Форум права*. 2013. № 1. С. 96-100.

116. Бобрик В. І. Право власності на персональні дані. *Вісник Хмельницького інституту регіонального управління та права*. 2002. № 2. С. 114-117.

117. Victor J. The EU General Data Protection Regulation: Toward a Property Regime for Protecting Data Privacy . *The Yale Law Journal.* 2013. № 123. P. 513-528.

118. Карпенко Д. В. Правовий режим охорони бази персональних даних на підприємствах України. *Форум права*. 2012. № 1. С. 432-437.

119. Директива 96/9/ЄС Європейського Парламенту та Ради від 11 березня 1996 року про правову охорону баз даних. База даних «Законодавство України» / ВР України. URL: http://old.minjust.gov.ua/file/31335.

120. Різак М. Правовий статус автора (творця, розробника) бази персональних даних. *Віче*. 2014. № 18. С. 16-19.

121. Case of S. and Marper v. The United Kingdom, App. No(s).30562/04, 30566/04. URL: http://hudoc.echr.coe.int/eng?i=001-117631.

122. Порівняльно-правове дослідження відповідності законодавства України законодавству ЄС у сфері персональних даних / В. М. Брижко, А. І. Радянська, М. Я. Швець. Київ : Тріумф, 2006. 256 с.

123. Lynskey O. Deconstructing data protection: the «added-value» of a right to data protection in the EU legal order. *International and Comparative Law Quarterly.* Vol. 63 (3). P. 569–597.

124. Andrade N. Oblivion: The Right to be Different ... from Oneself: Re–proposing the Right to be Forgotten. The Ethics of Memory in a Digital Age:

Interrogating the Right to be Forgotten. New York: Palgrave Macmillan, 2014. P. 65–81.

125. Новітнє вчення про тлумачення правових актів : навч. посіб. з курсу тлумачення прав. актів для суддів, що проходять підвищ. кваліфікації, і канд. на посади суддів, що проходять спец. підготов. / [В. Г. Ротань та ін. ; відп. ред. В.Г. Ротань]. Х. : Право, 2013. - 751 с.

126. Ткачук О. Витоки сучасного розуміння права на справедливий суд . *Visegrad Journal on Human Rights*. 2016. № 1/2. С. 188-193.

127. Case of Regner v. The Czech Republic, App. № 35289/11. URL: http://hudoc.echr.coe.int/eng?i=001-177299.

128. Case of Poleshchuk v. Russia, App. № 60776/00. URL: http://hudoc.echr.coe.int/eng?i=001-94340.

129. Case of Markovic and others v. Italy, App. № 1398/03. URL: http://hudoc.echr.coe.int/eng?i=001-78623

130. Case of Koch v. Germany, App. № 497/09. URL: http://hudoc.echr.coe.int/eng?i=001-112282.

131. Case of Hatton and others v. The United Kingdom, App. № 36022/97. URL: http://hudoc.echr.coe.int/eng?i=001-61188.

132. Health Care and EU Law: Legal Issues of Services of General Interest / Editors: J. W. van de Gronden, E. Szyszczak, U. Neergaard, M. Krajewski. The Hague, The Netherlands, T.M.C. Asser press, 2011. P. 211-239.

133. Bishop C. Internationalizing the Right to Know: Conceptualizations of Access to Information in Human Rights Law: A dissertation submitted in partial fulfillment of the requirements for the degree of Doctor of Philosophy; University of North Carolina at Chapel Hill. 2009. 268 p.

134. Постанова Вищого господарського суду України від 15 березня 2017 року у справі № 910/12950/16. URL: http://reyestr.court.gov.ua/Review/65345347.

135. Рішення Апеляційного суду Львівської області від 20 травня 2014 року у справі № 442/117/14. URL: http://reyestr.court.gov.ua/Review/38910939.

136. Бєлова Ю.Д. Право на мобільність як новий стандарт захисту персональних даних в ЕС. *Наукові записки Інституту законодавства Верховної Ради України*. 2017. №2. С. 56-61.

137. Privacy and competitiveness in the age of big data: The interplay between data protection, competition law and consumer protection in the Digital Economy: Preliminary Opinion of the European Data Protection Supervisor, March 2014. URL: https://secure.edps.europa.eu/EDPSWEB/edps/Consultation/big_data.

138. Вимоги до структури та змісту XML-схеми архівних електронних документів, затверджені Наказом Міністерства юстиції України від 11.11.2014 № 1886/5. URL: http://zakon2.rada.gov.ua/ laws/show/z1423-14/print1476733629827296.

139. Swire P. Why the Right to Data Portability Likely Reduces Consumer Welfare: Antitrust and Privacy Critique. *Maryland Law Review*. 2013. Volume 72, Issue 2. P. 335-380.

140. Graef I. Putting the right to data portability into a competition law perspective. *Law. The Journal of the Higher School of Economics, Annual Review*. 2013. P. 53-63

141. Lundqvist B. Big Data, Open Data, Privacy Regulations, Intellectual Property and Competition Law in an Internet of Things World (December 29, 2016). *Faculty of Law, University of Stockholm Research* Paper №. 1. SSRN URL: https://ssrn.com/abstract=2891484

142. Guidelines on the right to data portability, Adopted on 13 December 2016 by Article 29 Data Protection Working Party. URL: http://ec.europa.eu/justice/data-protection/index_en.htm.

143. Sloot B. Do data protection rules protect the individualand should they? An assessment of the proposedGeneral Data Protection Regulation. *International Data Privacy Law*. 2014. Vol. 4. No. 4. P. 307–325.

144. Concerns and Ideas about the Developing English Law of Privacy (and how knowledge of foreign law might be of help) / B. Markesinis, C. O'Cinneide, J. Fedtke, M. Hunter-Henin. URL: http://www. ucl.ac.uk/laws/global_law/publications/institute/docs/privacy_100804.pdf.

145. Serohin V.A. «The Right to Be Forgotten» as an Element of the Data Privacy. European Reforms Bulletin. 2015. № 4. P. 161-165.

146. Посикалюк О. О. Межі захисту особистих немайнових прав публічних осіб: порівняльно-правове дослідження. *Приватне право і підприємництво. Збірник наукових праць.* Вип. 13, 2014 р. Київ. : Науково-дослідний інститут приватного права і підприємництва Національної академії правових наук України. 2014. С. 197–200.

147. Посикалюк О. О. Загальне особисте немайнове право («allgemeine Persönlichkeitsrecht») за німецьким цивільним правом. *Право України* 2010. № 3. С. 253-259.

148. Stupariu I. Defining the Right to be Forgotten.A Comparative Analysis between the EU and the US. URL: http://dx.doi.org/10.2139/ssrn.2851362

149. Bundesverfassungs gericht (First Division) 5 June 1973, BVerfGE 35, 202. URL: http://germanlawarchive.iuscomp.org/?p=62

150. Spence v. Caputo, 2015 WL 630294. URL: https://www.gpo.gov/fdsys/pkg/USCOURTS-pawd-2_12-cv-01077/pdf/USCOURTS-pawd-2_12-cv-01077-1.pdf.

151. Rustad M., Kulevska S.Reconceptualizing the right to be forgotten toenable transatlantic data flow. *Harvard Journal of Law & Technology*. Volume 28, Number 2. P. 349-417.

152. An act to add Chapter 22.1 (commencing with Section 22580) to Division 8 of the Business and Professions Code, relating to the Internet, 23.09.13. URL: https://leginfo.legislature.ca.gov/faces/billNavClient.xhtml?bill_id=201320140SB568

153. Case of M.M. v. The United Kingdom, Application No. 24029/07. URL: http://hudoc.echr.coe.int/eng?i=001-114517.

154. Case of Österreichischer Rundfunk v. Austria Application № 35841/02. URL: http://hudoc.echr.coe.int/eng?i=001-78381.

155. Siry L. Forget Me, Forget Me Not: Reconciling Two Different Paradigms of the Right to Be Forgotten. *Kentucky Law Journal*. 2014-2015. Volume 103. № 3. P. 311–344.

156. Google Spain SL, Google Inc. v. Agencia Española de Protección de Datos (AEPD), Mario Costeja González, Case C-131/12. URL: http://curia.europa.eu/juris/document/document.jsf?docid=152065&doclang=en.

157. Пащенко И. Ю. Проблемы нормативного регулирования «права быть забытым» в сети интернет. *Евразийская адвокатура*. 2016. № 3. С. 106-113

158. Видалення результатів пошуку відповідно до закону про конфіденційність користувачів із ЄС: Звіт про роботу служб Google. URL: https://transparencyreport.google.com/eu-privacy/overview?hl=uk.

159. Балытников В. В., Кузнецов Д. А. Актуальные проблемы правового регулирования масс-медиа в решениях европейских судов наднационального уровня. *Международное правосудие*. 2015. № 1. С. 88-101.

160. O'Hara K. The digital citizen: the right to be forgotten: the good, the bad and the ugly. *IEEE Internet Computing*. № 19 (4). P. 73-79.

161. Pereiraa Â., Vesnić-Alujevića L., Ghezzia A. The Ethics of Forgetting and Remembering in the Digital World through the Eye of the Media. *The Ethics of Memory in a Digital Age: Interrogating the Right to be Forgotten*. New York: Palgrave Macmillan, 2014. P. 9-27

162. Markou C. The «Right to Be Forgotten»: Ten ReasonsWhy It Should Be Forgotten . *Law, Governance and Technology Series: Issues in Privacy and Data Protection*. Volume 20. P. 203-226

163. Korenhof P.Timing the Right to Be Forgotten: A Studyinto «Time» as a Factor in Deciding AboutRetention or Erasure of Data. *Law, Governance and Technology Series: Issues in Privacy and Data Protection*. Volume 20. P. 171–202.

164. Сухорольський П. Право бути забутим у правовій системі Європейського Союзу: реалії, проблеми та перспективи. *Наука міжнародного права на рубежі століть. Тенденції розвитку та трансформації : до 25 років каф. міжнар. права Львів. нац. ун-ту ім. Івана Франка*. Львів : ЛНУ імені Івана Франка, 2016. С. 90-101.

165. SzekelyI. The Right to be Forgotten and the New Archival Paradigm. *The Ethics of Memory in a Digital Age: Interrogating the Right to be Forgotten.* New York: Palgrave Macmillan, 2014. P. 28-49.

166. Guidelines on the implementation of the Court of Justice of the European Union judgment on «Google Spain and inc.v. Agencia Española De Protección De Datos (AEPD) and Mario Costeja González» C-131/12, Adopted on 26 November 2014 by the Article 29 Data Protection Working Party. URL: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp225_en.pdf

167. Про судову практику у справах про захист гідності та честі фізичної особи, а також ділової репутації фізичної та юридичної особи: Постанова Пленуму Верховного Суду України від 27.02.2009 № 1 База даних «Законодавство України» / ВР України. URL: http://zakon3.rada.gov.ua/laws/show/v_001700-09.

168. Дело о защите персональных данных в соцсетях: Facebook выплатит $550 млн. URL: https://sud.ua/ru/news/abroad/160124-delo-o-zaschite-personalnykh-dannykh-v-sotssetyakh-facebook-vyplatit-550-mln

169. Різак М. В. Володілець (розпорядник) бази персональних даних: окремі питання. *Порівняльно-аналітичне право*. 2013. № 1. С. 192–198.

170. Opinion 1/2010 on the concepts of «controller» and «processor», Adopted by the Article 29 Data Protection Working Party on 16 February 2010. URL: http://ec.europa.eu/justice_home/fsj/privacy/index_en.htm.

171. Козак В. Захист персональних даних та правила приватності при дослідженнях в Інтернет. *Маркетинг в Україні*. 2013/1. № 3. С. 49-70.

172. Цвірюк Д. В. Роль адміністративного законодавства у правовому регулюванні відносин, пов'язаних з персональними даними. *Форум права*. 2014. № 1. С. 516-521.

173. Цвірюк Д. В. Проблеми визначення прав і обов'язків володільця та розпорядника персональних даних. *Науковий вісник Херсонського державного університету. Серія «Юридичні науки»*. Випуск 2. Том 3. С. 199–204.

174. Бровченко І .О. Участь третіх осіб у цивільно-правових зобов`язаннях: автореф. дис... канд. юрид. наук: 12.00.03; Нац. юрид. акад. України ім. Я.Мудрого. Х., 2009. 20 с.

175. Типовий порядок обробки персональних даних, затверджений Наказом Уповноваженого Верховної Ради України з прав людини від 08.01.2014 № 1/02-14 URL: http://zakon3.rada.gov.ua/laws/show/v1_02715-14#n11.

176. Різак М. Права та обов'язки третіх осіб у правовідносинах обігу та обробки персональних даних в Україні. *Віче*. 2014. № 14. С. 21-24

177. Cheung A. Moving beyond Consent for Citizen Science in Big Data Health Research. *University of Hong Kong Faculty of Law Research Paper*. 2017. № 006 URL: http://dx.doi.org/10.2139/ssrn.2943185.

178. Hurd H. The Moral Magic of Consent. *Legal Theory*. 1996. Volume 2, Issue 2. P. 121-146.

179. Schermer B., Custers B., van der Hof S. The Crisis of Consent: How Stronger Legal Protection May Lead to Weaker Consent in Data Protection. *Ethics and Information Technology*. 2014. Volume 16, Issue 2. P. 171-182.

180. Романюк І. Особливості змісту та реалізації права на персональні дані в Україні та зарубіжних країнах. *Вісник Київського національного*

університету імені Тараса Шевченка. Юридичні науки. 2013. Вип. 2. С. 102-106.

181. Faden R. R., Beauchamp T. L. A History and Theory of Informed Consent. New York: Oxford University Press, 1986. 392 p.

182. Mantelero A. The Future of Consumer Data Protection in the E.U. Rethinking the «Notice and Consent» Paradigm in the New Era of Predictive Analytics. *Computer Law and Security Review*. 2014. Issue 30. P. 643-660.

183. Горпинюк О. П.Правова регламентація накопичення та використання приватної інформації в Україні. *Вісник Кримінологічної асоціації України*. 2013. № 4. С. 214-226.

184. Цвірюк Д. В. Підстави обробки персональних даних за законодавством України. *Вісник Харківського Національного університету внутрішніх справ.* 2014. № 2013. Вип. 4 (63). С. 138-146.

185. ZanfirG. Forgetting About Consent. Why The Focus Should Be On «Suitable Safeguards» in Data Protection Law. *Reloading Data Protection: Multidisciplinary Insights and Contemporary Challenges*. Springer Science & Business Media, 2014. P. 237-257.

186. Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF), Federación de Comercio Electrónico y Marketing Directo (FECEMD) v. Administración del Estado: Judgment of the Court of Justice of the European Union, 24 November 2011. URL: http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:62010CJ0468&from=EN.

187. Opinion 15/2011 on the definition of consent. Adopted on 13 July 2011. URL: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2011/wp187en.pdf.

188. Бєлова Ю.Д. Умови дійсності згоди на обробку персональних даних. *Підприємництво, господарство і право*. 2017. № 11. С.14-18.

189. Bygrave L. A., Schartum D. W. Consent, Proportionality and Collective Power. Reinventing Data Protection? / ed. Serge Gutwirth et al. Heidelberg: Springer, 2009. P. 157-173.

190. Borghi M., Ferretti F., Karapapa S. Online data processing consent under EU law: a theoretical framework and empirical evidence from the UK. *International Journal of Law and Information Technology*. Vol. 21. № 2 (2013). P. 109-153.

191. Крисань Т. Є. Види цивільно-правових гарантій суб'єктивних прав та критерії їх класифікації. *Бюлетень Міністерства юстиції України*. 2012. № 1. С. 57-66.

192. Заярний О. Адміністративна деліктність у сфері використання персональних даних та засоби її запобігання. *Вісник Київського національного університету імені Тараса Шевченка. Юридичні науки*. 2013. Вип. 95. С. 57-63.

193. Петрицький А. Л. Актуальні проблеми правового забезпечення захисту персональних даних в Україні. *Вісник Маріупольського державного університету. Серія Право*. 2013. Вип. 6. С. 111-119.

194. Deutsche Telekom AG v. Bundesrepublik Deutschland: Judgment of the Court (Third Chamber) of 5 May 2011. URL: http://curia.europa.eu/juris/celex.jsf?celex=62009CJ0543&lang1=en&type=TXT&ancre=.

195. Про внесення змін до деяких законів України щодо діяльності Уповноваженого Верховної Ради України з прав людини у сфері захисту персональних даних : Закон України від 13 травня 2014 року № 1262-VII. *Відомості Верховної Ради України*. 2014. № 27. Ст. 914.

196. Матола В. «Баги» державних реєстрів, або як захистити персональні дані. URL: https://lb.ua/pravo/2020/05/19/457892_bagi_derzhavnih_reiestriv_abo_yak.html

197. Цивільний кодекс України: Науково-практичний коментар (пояснення, тлумачення, рекомендації з використанням позицій вищих судових інстанцій, Міністерства юстиції, науковців, фахівців). Т. 1: Загальні положення / за ред. проф. І. В. Спасибо-Фатєєвої. Х.: ФО-П Колісник А.А., 2010. 320 с.

198. Богданов Е. В., Богданов Д. Е. , Богданова Е. Е. Развитие гражданского права России. Тенденции, перспективы, проблемы: монография. М.: ЮНИТИ-ДАНА: Закон и право, 2014. 335 с.

199. Цивільний кодекс України: Науково-практичний коментар: У 2 ч.: Ч. 1 / А. Ю. Бабаскін, І. А. Безклубий, Н. В. Безсмертна та ін. / За заг. ред. Я. М. Шевченко. Київ : Концерн «Видавничий Дім «Ін Юре»«, 2004. 692 с.

200. Радкевич О. П. Цивільно-правова охорона і захист персональної інформації в мережі Інтернет : автореф. дис. ... канд. юрид. наук : 12.00.03; Нац. акад. внутр. справ України. Київ : [б. в.], 2014. 20 с.

201. Бєлова Ю.Д. Підстави захисту прав суб'єкта персональних даних. *Jurnalul Juridic National: teorie si practica*. 2018. № 8. С.74-78.

202. Романюк І. І. Цивільно-правові способи захисту права особи на власні персональні дані. Науковий вісник Херсонського державного університету. Серія «Юридичні науки». 2014. Вип. 2. Т. 1. С. 208-214.

203. Бєлоусов О. Ілюзія дотримання законодавства про захист персональних даних у цифровому середовищі. *Юридична Газета*. 2013 р. № 14. С. 37.

204. Кодекс України про адміністративні правопорушення від 07.12.1984 № 8073-XURL База даних «Законодавство України» / ВР України. URL: http://zakon3.rada.gov.ua/laws/show/80731-10.

205. Кримінальний кодекс України від 5 квітня 2001 року № 2341-III. База даних «Законодавство України» / ВР України. URL: http://zakon3.rada.gov.ua/laws/show/2341-14.

206. Guidelines on Personal data breach notification under Regulation 2016/679, Adopted on 3 October 2017by Article 29 Data Protection Working Party URL: http://ec.europa.eu/newsroom/document.cfm?doc_id=47741

207. Кулініч О. О. Теоретичні проблеми реалізації та захисту права фізичної особи на власне зображення: дис. ... д-ра юрид. наук : 12.00.03; Нац. ун-т «Одес. юрид. акад.». Одеса : 2017. 488 с.

208. Футболист «Шахтера» подал в суд на социальную сеть. *Юридическая практика*. URL: http://www.yurpractika.com/news.php?id=0018287.

209. Ойгензихт В. А. Проблеми риска в гражданском праве. Душанбе, 1972. 158 с.

210. Красавчиков О. А. Возмещение вреда причинённого источником повышенной опасности. М., 1966. 200 с.

211. Малеин Н. С. Вина необходимое условие имущественной ответственности. *Соетское. государство и право*. 1971. № 2. С. 33–36.

212. Мезрин Б.Н. О юридической природе риска в советском гражданском праве. *Гражданское право и способы его защиты*. Свердловск, 1974. С. 47.

213. Майданик Р. А. Аномаліїв цивільному праві України: Навч.-практ. посібник. Київ : Юстініан, 2007. 912 с.

214. Кохановська О. В. Теоретичні проблеми інформаційних відносин у цивільному праві. Київ; Видавничо-поліграфічний центр «Київський університет», 2006. 463 с.

215. Кодинець А. О. Цивільно-правове регулювання зобов'язальних інформаційних відносин: методологія, теорія, практика: дис. ... д-ра юрид. наук : 12.00.03; Київ. нац. ун-т ім. Т. Шевченка. - Київ : 2017. 470 с.

216. Рекомендація N R (99) 5 Комітету Міністрів державам-членам Ради Європи «Про захист недоторканності приватного життя в Інтернеті» від 23.02.1999. URL: http://zakon2.rada.gov.ua/laws/show/994_357

217. Кулініч О. О. Цивільно-правовий захист персональних даних фізичних осіб. Актуальні проблеми держави і права. 2007. Вип. 33. С. 41–45.

218. Рішення Конституційного Суду України у справі за конституційним зверненням Товариства з обмеженою відповідальністю «Торговий Дім «Кампус Коттон клаб» щодо офіційного тлумачення положення частини другої статті 124 Конституції України (справа про досудове врегулювання спорів) від 9

липня 2002 року № 15-рп/2002. Офіційний вісник України. 2002. № 28. Ст. 1333.

219. Конституція України, прийнята на п’ятій сесії Верховної Ради України 28 червня 1996 року. База даних «Законодавство України» / ВР України. URL: http://zakon2.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80.

220. Порядок здійснення Уповноваженим Верховної Ради України з прав людини контролю за додержанням законодавства про захист персональних даних, затверджений Наказом Уповноваженого Верховної Ради України з прав людини від 08.01.2014 № 1/02-14. База даних «Законодавство України» / ВР України. URL: http://zakon2.rada.gov.ua/laws/show/v1_02715-14.

221. Мельник К. С. Правові та організаційні засади захисту персональних даних в умовах євроінтеграції України: дис. ... канд. юрид. наук : 12.00.07; НДІ інформатики і права НАПрН України. Київ : [б. в.], 2016. 228 с

222. Рішення Апеляційного суду міста Києва у справа № 575/43109/16-ц від 23 березня 2017 року. URL: http://www.reyestr.court.gov.ua/Review/65739004.

223. Ухвала Вищого спеціалізованого суду України з розгляду цивільних і кримінальних справ у справі № 6-40349св13 від 02 квітня 2014 року.URL: http://www.reyestr.court.gov.ua/Review/38119227.

224. Рішення Голосіївського районного суду м. Києва у справі № 752/12262/15-ц від 08.06.2017 року. URL: http://www.reyestr.court.gov.ua/Review/67045882.

225. Рішення Апеляційного суду Автономної Республіки Крим у справі № 106/5771/13-ц від 21 січня 2014 р. URL: http://www.reyestr.court.gov.ua/ Review/37443227.

226. Бєлова Ю.Д. Система спеціальних цивільно-правових способів захисту права на персональні дані. *Юридичний журнал «Право України».* Випуск 1/2019. С. 314-327.

227. Рішення Вищого господарського суду України від 15 березня 2017 року у справі № 910/12950/16. URL: http://www.reyestr.court.gov.ua/Review/65345347#.

228. Постанова Верховного Суду України від 27 вересня 2017 року у справі № 369/5585/15-ц. URL: http://www.reyestr.court.gov.ua/Review/70427210#.

229. Трудовий кодекс України: проект від 27.12.2014 № 1658. URL: http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=53221

230. Про Державний реєстр виборців: Закон України від 22 лютого 2007 року № 698-V. *Відомості Верховної Ради України*. 2007. № 20. Ст. 282.

231. Про Єдиний державний демографічний реєстр та документи, що підтверджують громадянство України, посвідчують особу чи її спеціальний статус : Закон України від 20 листопада 2012 року № 5492-VI. *Відомості Верховної Ради України*. 2013. № 51. Ст. 716.

232. Про Єдиний державний реєстр військовозобов'язаних: Закон України від 16 березня 2017 року № 1951-VIII. *Відомості Верховної Ради*. 2017. № 18.Ст.217.

233. Case of K.U. v. Finland. App. No.2872/02. URL: http://hudoc.echr.coe.int/eng?i=001-117361.

ДОДАТКИ

Додаток А

СПИСОК ОПУБЛІКОВАНИХ ПРАЦЬ ЗА ТЕМОЮ ДИСЕРТАЦІЇ

в яких опубліковані основні наукові результати дисертації:

1. Бєлова Ю.Д. Право на мобільність як новий стандарт захисту персональних даних в ЕС. *Наукові записки Інституту законодавства Верховної Ради України*. 2017. № 2. С. 56-61.

2. Бєлова Ю.Д. Стандарти захисту права на персональні дані відповідно до Директиви 95/46/ЕС. *Часопис «Університетські наукові записки» Хмельницького університету управління та права*. 2017. № 3 (63). С. 130-139.

3. Бєлова Ю.Д. Умови дійсності згоди на обробку персональних даних. *Підприємництво, господарство і право*. 2017. № 11. С.14-18.

4. Бєлова Ю.Д. Поняття та зміст прав суб'єкта персональних даних. *Науково-практичний журнал «Соціологія права»*. 2017. № 3-4. С. 13-21.

5. Бєлова Ю.Д. Підстави захисту прав суб'єкта персональних даних. *Jurnalul Juridic National: teorie si practica*. 2018. № 8. С.74-78.

6. Бєлова Ю.Д. Система спеціальних цивільно-правових способів захисту права на персональні дані. *Юридичний журнал «Право України»*. 2019. Вип. 1. С. 314-327.

7. Белова Ю.Д. Защита прав субъекта персональных данных. *Visegrad Journal on Human Rights*. 2020. № 4. С.24-39.

8. Бєлова Ю.Д. Згода та інші підстави виникнення цивільних правовідносин щодо персональних даних. *Юридичний вісник*. 2020. № 3. С.348-355.

які засвідчують апробацію матеріалів дисертації:

9. Бєлова Ю.Д. *Цивільні правовідносини щодо персональних даних* : Монографія. Хмельницький : ФОП Мельник А.А., 2019. 192 с.

10. Бєлова Ю.Д. Право на мобільність персональних даних. *Інформаційні технології у судочинстві* : зб. матер. всеукр. наук.-практ. конф., яка проводиться в рамках тижня цивільного процесу. Одесса : Фенікс, 2017. С. 89-92.

11. Бєлова Ю.Д. Стандарти захисту права на персональні дані відповідно до Директиви 95/46/ЄС: теоретико-адаптаційні аспекти. *Теорія та практика адаптації законодавства України до законодавства ЄС* : матеріали міжнар. наук.-практ. столу. Єреван : Видавництво Eurasian Social Science Assjciation, 2017. С. 16-18.

12. Бєлова Ю.Д. Стандарти захисту права на персональні дані відповідно до практики ЄСПЛ. *Україна на шляху до Європи: реформа цивільного процесуального законодавства* : зб. наук. праць Матеріали Міжнар. наук.-практ. конф. К. : ВД Дакор, 2017. С. 86-89.

13. Бєлова Ю.Д. Участь розпорядника у відносинах щодо персональних даних. *Актуальні проблеми юридичної науки:* зб. тез Міжнародної наукової конференції «Шістнадцяті осінні юридичні читання» : (у 2-х част). Частина перша. Хмельницький : Хмельницький університет управління та права, 2017. С. 101-102.

14. Бєлова Ю.Д. Право суб'єкта персональних даних на забуття. *Актуальні проблеми інтелектуального, інформаційного та IT права :* зб. матеріалів Другої Всеукраїнської науково-практичної конференції. Львів : Юрид. ф –т Львів. нац. ун –ту ім. І. Франка, 2017. С. 76- 79.

15. Бєлова Ю.Д. Сучасні підходи до розуміння категорії персональних даних. *Актуальні питання розвитку юридичної науки та практики:* матеріали Міжнародної науково-практичної конференції : в 2-х томах. Том 2. К., 2018. С. 15-16.

16. Бєлова Ю.Д. Сучасні підходи до класифікації персональних даних. *Проблеми цивільного права та процесу, присвячена світлій пам'яті Пушкіна О.А. :* матеріали науково-практичної конференції. Харків. 2018. С. 311-314.

17. Бєлова Ю.Д. Персональні дані як об'єкт спадкових правовідноси. *Правове регулювання суспільних відносин: актуальні проблеми та вимоги сьогодення:* матеріали Міжнародної науково-практичної конференції. Запоріжжя : Запорізька міська громадська організація «Істина». 2018. С. 25-28.

18. Бєлова Ю.Д. Порушення прав суб'єкта персональних даних як підстава їх захисту. *Актуальні проблеми юридичної науки:* зб. тез Міжнародної наукової конференції «Сімнадцяті осінні юридичні читання» : (у 2-х част). Частина друга. Хмельницький : Хмельницький університет управління та права, 2018. С. 8-11.

19. Бєлова Ю. Д. Правова природа персональних даних. *Конституційні цінності: правова природа та практика реалізації : збірник тез Міжнародної науково-практичної конференції «Конституційні цінності: правова природа та практика реалізації»* (м. Хмельницький, 17 травня 2019 року). [у 2-х част.]. Частина 1. Хмельницький : Хмельницький університет управління та права імені Леоніда Юзькова, 2019. С. 51-54.

Додаток Б

«ЗАТВЕРДЖУЮ»

Ректор Хмельницького університету управління та права
імені Леоніда Юзькова
_____ О.М. Омельчук
«___» _____ 2020 р.

АКТ
про реалізацію наукових досліджень
БЄЛОВОЇ Юлії Дмитрівни на тему:
«Цивільні правовідносини щодо персональних даних»

Комісія у складі:
голови комісії: декан юридичного факультету, к.ю.н.
Крушинский Сергій Антонович
членів комісії: завідувач кафедри цивільного права та процесу, д.ю.н., професор
Гринько Світлана Дмитрівна,
професор кафедри цивільного права та процесу, к.ю.н., професор
Білоусов Юрій Валерійович,

стверджує цим актом, що розроблені в ході дисертаційного дослідження Бєлової Юлії Дмитрівни наукові положення і висновки з теми «Цивільні правовідносини щодо персональних даних» були детально вивчені колективом кафедри цивільного права та процесу Хмельницького університету управління та права імені Леоніда Юзькова та реалізовані у навчальному процесі.

Зокрема дисертанткою були надані для ознайомлення наукові публікації:

Список опублікованих праць за темою дисертації:

в яких опубліковані основні наукові результати дисертації:

1. Бєлова Ю.Д. Право на мобільність як новий стандарт захисту персональних даних в ЕС. *Наукові записки Інституту законодавства Верховної Ради України*. 2017. №2. С. 56-61.
2. Бєлова Ю.Д. Стандарти захисту права на персональні дані відповідно до Директиви 95/46/ЕС. *Часопис «Університетські наукові записки» Хмельницького університету управління та права*. 2017. № 3 (63). С. 130-139.
3. Бєлова Ю.Д. Умови дійсності згоди на обробку персональних даних. *Підприємництво, господарство і право*. 2017. № 11. С.14-18.
4. Бєлова Ю.Д. Поняття та зміст прав суб'єкта персональних даних. *Науково-практичний журнал «Соціологія права»*. 2017. № 3-4. С. 13-21.
5. Бєлова Ю.Д. Підстави захисту прав суб'єкта персональних даних. *Jurnalul Juridic National: teorie si practica*. 2018. №8. С.74-78.
6. Бєлова Ю.Д. Система спеціальних цивільно-правових способів захисту права на персональні дані. *Юридичний журнал «Право України»*. 2019. Вип. 1. С. 314-327.

7. Белова Ю.Д. Защита прав субъекта персональных данных. *Visegrad Journal on Human Rights*. 2020. №4. С.24-39.

8. Бєлова Ю.Д. Згода та інші підстави виникнення цивільних правовідносин щодо персональних даних. *Юридичний вісник*. 2020. №3. С.348-355.

які засвідчують апробацію матеріалів дисертації:

9. Бєлова Ю.Д. *Цивільні правовідносини щодо персональних даних*: Монографія. Хмельницький: ФОП Мельник А.А., 2019. 192 с.

10. Бєлова Ю.Д. Право на мобільність персональних даних. *Інформаційні технології у судочинстві*: зб. матер. всеукр. наук.-практ. конф., яка проводиться в рамках тижня цивільного процесу . Одесса: Фенікс, 2017. С. 89-92.

11. Бєлова Ю.Д. Стандарти захисту права на персональні дані відповідно до Директиви 95/46/ЄС: теоретико-адаптаційні аспекти. *Теорія та практика адаптації законодавства України до законодавства ЄС*: матеріали міжнар. наук.-практ. столу. Єреван: Видавництво Eurasian Social Science Assjciation, 2017. С.16-18.

12. Бєлова Ю.Д. Стандарти захисту права на персональні дані відповідно до практики ЄСПЛ. *Україна на шляху до Європи: реформа цивільного процесуального законодавства*: зб. наук. праць Матеріали Міжнар. наук.-практ. конф. Київ: ВД Дакор, 2017. С. 86-89.

13. Бєлова Ю.Д. Участь розпорядника у відносинах щодо персональних даних. *Актуальні проблеми юридичної науки:* зб. тез Міжнародної наукової конференції «Шістнадцяті осінні юридичні читання»: (у 2-х част). Частина перша. Хмельницький: Хмельницький університет управління та права, 2017. С. 101-102.

14. Бєлова Ю.Д. Право суб'єкта персональних даних на забуття. *Актуальні проблеми інтелектуального, інформаційного та ІТ права:* зб. матеріалів Другої Всеукраїнської науково-практичної конференції. Львів: Юрид. ф –т Львів. нац. ун –ту ім. І. Франка, 2017. С. 76- 79.

15. Бєлова Ю.Д. Сучасні підходи до розуміння категорії персональних даних. *Актуальні питання розвитку юридичної науки та практики:* матеріали Міжнародної науково-практичної конференції: в 2-х томах. Том 2. К.:, 2018. С. 15-16.

16. Бєлова Ю.Д. Сучасні підходи до класифікації персональних даних. *Проблеми цивільного права та процесу, присвячена світлій пам'яті Пушкіна О.А.:* матеріали науково-практичної конференції. Харків. 2018. С. 311-314.

17. Бєлова Ю.Д. Персональні дані як об'єкт спадкових правовідноси. *Правове регулювання суспільних відносин: актуальні проблеми та вимоги сьогодення:* матеріали Міжнародної науково-практичної конференції. Запоріжжя: Запорізька міська громадська організація «Істина». 2018. С. 25-28.

18. Бєлова Ю.Д. Порушення прав суб'єкта персональних даних як підстава їх захисту. *Актуальні проблеми юридичної науки:* зб. тез Міжнародної наукової конференції «Сімнадцяті осінні юридичні читання»: (у 2-х част). Частина друга. Хмельницький: Хмельницький університет управління та права, 2018. С. 8-11.

19. Бєлова Ю. Д. Правова природа персональних даних. *Конституційні цінності: правова природа та практика реалізації : збірник тез Міжнародної науково-практичної конференції «Конституційні цінності: правова природа та практика реалізації»* (м. Хмельницький, 17 травня 2019 року). [у 2-х част.]. Частина 1. Хмельницький : Хмельницький університет управління та права імені Леоніда Юзькова, 2019. С. 51-54.

Наведені наукові публікації були розглянуті науково-педагогічними працівниками кафедри цивільного права та процесу Хмельницького університету управління та права імені Леоніда Юзькова та були включені до матеріалів лекційних занять з дисципліни «Цивільне право» (Тема 6 «Фізичні особи як суб`єкти цивільних правовідносин»; Тема 9 «Об'єкти цивільних правовідносин»; Тема 15 «Поняття, види та захист особистих немайнових прав фізичних осіб»; Тема 21 «Загальні положення про право інтелектуальної власності»).

Голова комісії: **Сергій КРУШИНСКИЙ**

Члени комісії: **Світлана ГРИНЬКО**

Юрій БІЛОУСОВ

Підпис
ЗАСВІДЧУЮ:
Нач. ВК ХУУП
імені Леоніда Юзькова

Підпис
ЗАСВІДЧУЮ:
Нач. ВК ХУУП
імені Леоніда Юзькова

Підпис
ЗАСВІДЧУЮ:
Нач. ВК ХУУП
імені Леоніда Юзькова