ІНСТИТУТ ДЕРЖАВИ І ПРАВА імені В. М. КОРЕЦЬКОГО
НАЦІОНАЛЬНА АКАДЕМІЯ НАУК УКРАЇНИ

Кваліфікаційна наукова
праця на правах рукопису

КОВАЛЕНКО ЮЛІЯ ОЛЕКСАНДРІВНА

УДК 341.1/8:341.231.14

ДИСЕРТАЦІЯ

ЗАХИСТ ПЕРСОНАЛЬНИХ ДАНИХ У ПРАКТИЦІ ЄВРОПЕЙСЬКОГО СУДУ З ПРАВ ЛЮДИНИ ТА СУДУ ЄВРОПЕЙСЬКОГО СОЮЗУ: ПОРІВНЯЛЬНИЙ АНАЛІЗ

Спеціальність 293 «Міжнародне право»
Галузь знань 29 «Міжнародні відносини»

Подається на здобуття ступеня доктора філософії (PhD)

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

Науковий керівник: ФАЛАЛЄЄВА Людмила Григорівна, доктор юридичних наук, доцент

Київ – 2023

АНОТАЦІЯ

Коваленко Ю. О. Захист персональних даних у практиці Європейського суду з прав людини та Суду Європейського Союзу: порівняльний аналіз. – *Кваліфікаційна наукова праця на правах рукопису.*

Дисертація на здобуття ступеня доктора філософії за спеціальністю 293 «Міжнародне право» (29 – Міжнародні відносини). – Інститут держави і права імені В. М. Корецького Національна академія наук України, Київ, 2023.

Дисертація є комплексним науковим дослідженням міжнародно-правових засад регулювання захисту персональних даних. Актуальність дисертаційної роботи зумовлена необхідністю системного дослідження теоретичних та практичних проблем, пов'язаних із захистом персональних даних у Раді Європи та Європейському Союзі, систематизації застосовуваних у цій сфері підходів і принципів, а також оцінки їх впливу на формування стандартів захисту персональних даних.

У роботі розкрито юридичний зміст понять – «персональні дані», «чутливі дані», «обробка даних», «європейські стандарти захисту персональних даних». Досліджено ґенезу права на захист персональних даних у міжнародному праві та його становлення як самостійного основоположного права людини крізь призму рішень міжнародних судових органів – Європейського суду з прав людини та Суду Європейського Союзу. Констатовано, що право на захист персональних даних є предметом тривалої дискусії.

Доведено, що тривалий час право на захист персональних даних розглядалося як один із аспектів права на захист приватного життя і не було чітко визначено. Поступовому виокремленню та закріпленню як основоположного права людини на захист персональних даних сприяла широкомасштабна комп'ютеризація і цифровізація багатьох сфер суспільного життя, впровадження новітніх технологічних розробок і необхідність транскордонної передачі великих обсягів даних. Запропоновано відхід від сприйняття права на захист персональних даних як окремого аспекту права на повагу до приватного життя та його визнання як

самостійного основоположного права людини з огляду на його роль у сучасному інформаційному суспільстві.

У праці здійснено аналіз різних підходів до розуміння приватності та захисту даних, які переважно сформувалися в рамках американської та європейської моделей захисту даних. Наголошено на проблемних аспектах міжнародно-правового регулювання захисту персональних даних. Доведено, що становлення стандартів захисту персональних даних відбувалося переважно у рамках діяльності Ради Європи та Європейського Союзу, а тому поширеним є використання терміну «європейські стандарти захисту персональних даних». Зауважено, що в умовах глобалізаційного розвитку європейські стандарти захисту персональних даних поступово набули значного поширення і сприяли гармонізації норм щодо захисту персональних даних на міжнародному рівні. Обґрунтовано позицію щодо визнання європейських стандартів захисту персональних даних як найбільш прогресивних норм у досліджуваній сфері.

Доведено, що з огляду на еволюційний розвиток європейських стандартів захисту даних виправданою є їх класифікація на: перше покоління (Керівні принципи ОЕСР щодо захисту права на приватність і транскордонні потоки персональних даних, схвалені Рекомендацією Ради ОЕСР від 23 вересня 1980 р., та Конвенція № 108 про захист осіб у зв'язку з автоматизованою обробкою персональних даних 1981 р.), друге покоління (Конвенція № 108 про захист осіб у зв'язку з автоматизованою обробкою персональних даних 1981 р., оновлена Додатковим протоколом 2001 р., та Директива 95/46/ЄС про захист фізичних осіб при обробці персональних даних і про вільне переміщення таких даних 1995 р.) та третє покоління (оновлена Конвенція № 108+ зі змінами, внесеними Протоколом CETS № 223, та Регламент Європейського Парламенту і Ради (ЄС) 2016/679 про захист фізичних осіб під час обробки персональних даних та їх вільного обігу (Загальний регламент про захист даних) 2016 р.). Оновлена Конвенція № 108+ та Загальний регламент про захист даних спрямовані на забезпечення права на захист персональних даних кожної особи, як самостійного основоположного права, відокремленого від права на захист приватного

життя, незалежно від національності чи місця проживання особи, що свідчить про персоноцентризм та екстериторіальність застосування їх норм.

Зроблено висновок, що сучасною тенденцією європейської системи захисту персональних даних є формування взаємоузгоджених стандартів у цій сфері, що виникли з огляду на популяризацію транскордонного обміну персональними даними, з метою досягнення єдності в правовому регулюванні, що узгоджувало б фундаментальні цінності поваги до недоторканості приватного життя особи й безперешкодний обмін інформацією між державами. Відповідно, у досліджуваній сфері прослідковується уніфікація європейських стандартів захисту персональних даних і їх широке впровадження на глобальному рівні.

У дисертаційному дослідженні проаналізовано основні міжнародно-правові акти, які регулюють захист персональних даних, а також висвітлено практику міжнародних та національних судових органів щодо забезпечення права на повагу до приватного життя та права на захист персональних даних. Розкрито особливості правових засад регулювання захисту персональних даних у Раді Європи та Європейському Союзі, сутність і особливості захисту персональних даних у Європейському суді з прав людини та Суді Європейського Союзу, вивчено та систематизовано основні принципи, концепції та підходи, застосовні у справах, пов’язаних із захистом персональних даних.

Доведено, що принципи, доктрини, підходи та інтерпретаційні техніки, що застосовуються Європейським судом з прав людини та Судом Європейського Союзу у справах, пов’язаних з питаннями захисту персональних даних, є взаємопов’язаними та взаємодоповнюючими. Сформульовано висновок про те, що право на захист персональних даних тісно пов’язане з іншими основоположними правами людини, а тому при оцінці меж втручання у ці права, задля запобігання порушенню самої суті конкуруючих прав, має бути забезпечений справедливий баланс між правами інших осіб, приватними та публічними інтересами.

Окрему увагу приділено стану виконання Україною міжнародно-правових зобов’язань щодо захисту персональних даних та стан адаптації чинного

законодавства до *acquis* ЄС. Визначено перспективи розвитку національного законодавства у досліджуваній сфері.

Наголошено, що попри узгодженість на міжнародному рівні норм і принципів захисту персональних даних та термінології у цій сфері, у вітчизняній міжнародно-правовій доктрині і практиці виникають певні проблеми стосовно єдності використання понятійно-категоріального апарату в сфері захисту персональних даних. Запропоновано розмежування понять «персональні дані», «інформація про особу», «конфіденційна інформація» та «інформація про приватне життя особи», оскільки неточність формулювання згаданих понять у вітчизняному законодавстві в контексті захисту персональних даних призводить до існування конкуруючих норм та нерідко до звуження права на захист персональних даних. З метою забезпечення уніфікації термінологічного апарату в цій сфері визнано виправданим використання саме терміну «персональні дані» для позначення інформації, що підлягає обробці та містить відомості про ідентифіковану особу чи особу, яку можна ідентифікувати.

Проаналізовано чинне законодавство України щодо захисту персональних даних та практику його застосування, виявлено застарілість окремих правових норм і підходів у цій сфері.

Зауважено, що законодавству України у сфері захисту персональних даних притаманні наступні ознаки: складна структурованість та розгалуженість відповідних правових норм у різних актах; некоректність або відсутність чіткого визначення конкретного змісту термінів та категорій, які не є повною мірою взаємоузгодженими; неоднозначне інтерпретування законодавчих норм під час правозастосування; застарілість норм вітчизняного законодавства у сфері захисту персональних даних та їх невідповідність європейським стандартам у цій сфері.

Доведено, що виконання Україною своїх міжнародно-правових зобов’язань у сфері забезпечення і дотримання права на захист персональних даних є триваючим процесом, що постійно розвивається з огляду на впровадження новітніх технологій, глобалізаційні процеси, євроінтеграційний і євроатлантичний зовнішньополітичні пріоритети розвитку держави, виклики та загрози сучасності, серед іншого, пов’язані зі збройною агресією проти України. Вивчено процес еволюції національного

законодавства України у сфері захисту персональних даних в аспекті євроінтеграційної і євроантлантичної зовнішньої політики держави, адаптації до права Європейського Союзу у цій сфері, відповідних стандартів у цій сфері в контексті забезпечення інформаційної безпеки держави. Наголошено на важливості функціонування незалежного інституційного механізму контролю у сфері захисту персональних даних, який розглядається як важливий елемент європейських стандартів у цій сфері.

Зроблено висновок про необхідність увідповіднення українського законодавства у сфері захисту персональних даних до європейських стандартів захисту даних третього покоління, а саме оновленої Конвенції № 108+ зі змінами, внесеними Протоколом CETS № 223, та Загального регламенту про захист даних 2016 р., що забезпечило б ефективність гарантування права на захист персональних даних.

Ключові слова: захист персональних даних, Рада Європи, Європейський Союз, міжнародна організація, правове регулювання, право ЄС, міжнародне право прав людини, права людини, права та інтереси, Європейський суд з прав людини, ЄСПЛ, Суд Європейського Союзу, Суд ЄС, європейські стандарти захисту персональних даних, інформаційне суспільство.

SUMMARY

Kovalenko Y. O. Protection of personal data in the jurisprudence of the European Court of Human Rights and the Court of Justice of the European Union: a comparative analysis. – *Qualifying scientific work on the rights of manuscript*.

The dissertation for the degree of Doctor of Philosophy in specialty 293 «International Law» (29 – International Relations). – V. M. Koretsky Institute of State and Law of National Academy of Sciences of Ukraine, Kyiv, 2023.

The dissertation is a comprehensive scientific study of the international legal principles of regulation of personal data protection. The relevance of the dissertation is determined by the need for a systematic study of theoretical and practical problems related to the protection of personal data in the Council of Europe and the European Union,

systematization of the approaches and principles used in this field, as well as an assessment of their impact on the formation of personal data protection standards.

The work revealed the legal meaning of the concepts – «personal data», «sensitive data», «data processing», «European standards for personal data protection». The genesis of the right to the protection of personal data in international law and its formation as an independent fundamental human right through the prism of the decisions of international judicial bodies – the European Court of Human Rights and the Court of Juctice of the European Union – have been studied. It is noted that the issue of the nature of the right to the protection of personal data is the subject of a long debate.

For a long time, the right to the protection of personal data was considered as one of the aspects of the right to the protection of private life and was not clearly defined. Large-scale computerization and digitization of many spheres of social life, the introduction of the latest technological developments and the need for transborder flow of large volumes of data contributed to the gradual separation and consolidation of the fundamental human right to the protection of personal data. It is proposed to shift from the perception of the right to the protection of personal data as a separate aspect of the right to respect for private life to its recognition as an independent fundamental human right in view of its role in the modern information society.

The work analyzes different approaches to understanding of privacy and data protection, which were mainly formed within the framework of American and European data protection models. Emphasis is placed on problematic aspects of international legal regulation of personal data protection. It has been proven that the establishment of personal data protection standards took place mainly within the framework of the activities of the Council of Europe and the European Union, and therefore the use of the term European personal data protection standards is proposed to denote the guiding principles in this area. It has been noted that in the conditions of globalization development, European personal data protection standards gradually gained a significant spread and contributed to the harmonization of norms regarding the protection of personal data at the international level. It has been substantiated the need to recognize European standards of personal data protection as the most progressive norms in the researched field.

It has been proven that, in view of the evolutionary development of European personal data protection standards, their classification into: first generation (OECD Guidelines for the Protection of the Right to Privacy and Cross-Border Flows of Personal Data, approved by the Recommendation of the OECD Council of 23 September 1980, and Convention No. 108 on protection of individuals with regard to automated processing of personal data of 1981), second generation (Convention No. 108 on the protection of individuals with regard to automated processing of personal data of 1981, updated by the Additional Protocol of 2001, and Directive 95/46 /EU on the protection of natural persons in the processing of personal data and on the free movement of such data of 1995) and the third generation (Convention No. 108+, with amendments introduced by the Protocol CETS № 223, and the Regulation (EU) 2016/679 of the European Parliament and of the Council 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) of 2016). The modernized Convention No. 108+ and the General Data Protection Regulation are aimed at ensuring the right to the protection of personal data of each person, as an independent fundamental right, separated from the right to the protection of private life, regardless of the nationality or place of residence of the person, which indicates person-centrism and extraterritorial application their norms.

It has been concluded that the current trend of the European system of personal data protection is the formation of mutually agreed standards in this area, which arose in view of the popularization of tnasborder exchange of personal data, with the aim of achieving unity in legal regulation, which would harmonize the fundamental values of respect for the inviolability of a person's private life and unhindered exchange of information between states. Accordingly, unification of European personal data protection standards and their wide implementation at the global level are being followed in the researched field.

The dissertation study analyzed the main international legal acts that regulate the protection of personal data, as well as highlighted the practice of international and national judicial bodies on ensuring the right to respect for private life and the right to the protection of personal data. The peculiarities of the legal basis of the regulation of personal data protection in the Council of Europe and the European Union, the essence and features of the

protection of personal data in the European Court of Human Rights and the Court of the European Union has been acknowledged, the main principles, concepts and approaches applicable in cases related to the protection of personal data has been studied and systematized.

It has been proven that the principles, concepts, approaches and interpretation techniques used by the European Court of Human Rights and the Court of Justice of the European Union in cases related to personal data protection issues are interrelated and mutually complementary. The conclusion was formulated that the right to the protection of personal data is closely related to other fundamental human rights, and therefore, when assessing the limits of interference with these rights, in order to prevent violation of the very essence of rights at stake, a fair balance must be ensured between the rights of other persons, private and public interests.

Particular attention is paid to the state of fulfilment of international legal obligations by Ukraine regarding the protection of personal data and the state of adaptation of current legislation to the EU *acquis*. The prospects for the development of national legislation in the researched area have been determined. It is emphasized that despite the consensus on the international level regarding the norms and principles of personal data protection and terminology in this area, certain problems arise in domestic international legal doctrine and practice regarding the unity of the use of the conceptual and categorical apparatus in the field of personal data protection. It is proposed to distinguish the concepts of «personal data», «information about a person», «confidential information» and «information about a private life of a person», since the inaccuracy of the formulation of the mentioned concepts in domestic legislation in the context of personal data protection leads to the existence of competing norms and often to narrowing of the right to protection of personal data. In order to ensure the unification of the terminological apparatus in this area, it is justified to use the term «personal data» to designate information that is subject to processing and contains information about an identified person or a person who can be identified.

The current legislation of Ukraine on the protection of personal data and the practice of its application was analyzed, and the obsolescence of certain legal norms and approaches in this area was revealed.

It was noted that the legislation of Ukraine in the field of personal data protection has the following features: complex structure and branching of relevant legal norms in various acts; incorrectness or lack of a clear definition of the specific content of terms and categories that are not fully consistent with each other; ambiguous interpretation of legislative norms during law enforcement; the obsolescence of domestic legislation in the field of personal data protection and their non-compliance with European standards in this field.

It has been proven that fulfilment of international legal obligations by Ukraine in the field of ensuring and observing the right to the protection of personal data is an ongoing process that is constantly developing in view of the introduction of the latest technologies, globalization processes, European integration and Euro-Atlantic foreign policy priorities of the state's development, challenges and threats of modern times, among other things, those related to the armed aggression against Ukraine. The process of evolution of the national legislation of Ukraine in the field of personal data protection in the aspect of European integration and Euro-Atlantic foreign policy of the state, adaptation to the law of the European Union in this area, relevant standards in this area in the context of ensuring information security of the state has been studied. The importance of the functioning of an independent institutional control mechanism in the field of personal data protection, which is considered an important element of European standards in this field, has been emphasized.

It is concluded that there is a need to modernize Ukrainian legislation in the field of personal data protection in accordance with third-generation European personal data protection standards, namely Convention No. 108, with amendments introduced by Protocol CETS № 223, and the General Datap Protection Regulation of 2016, which would ensure the effectiveness of guaranteeing the right to personal data protection.

Keywords: personal data protection, Council of Europe, European Union, international organization, legal regulation, EU law, international human rights law, human rights, rights and interests, European Court of Human Rights, ECtHR, Court of Justice of the European Union, CJEU, European personal data protection standards, information society.

СПИСОК ПУБЛІКАЦІЙ ЗДОБУВАЧА ЗА ТЕМОЮ ДИСЕРТАЦІЇ, В ЯКИХ ОПУБЛІКОВАНІ ОСНОВНІ НАУКОВІ РЕЗУЛЬТАТИ

Список публікацій, в яких опубліковані основні наукові результати дисертації:

1. Коваленко Ю. О. Становлення та розвиток європейських стандартів захисту персональних даних. *Наукові записки Інституту законодавства Верховної Ради України*. 2020. № 5. С. 59-67.
2. Kovalenko Y. The Right to Privacy and Protection of Personal Data: Emerging Trends and the Implications for Development in the Jurisprudence of the European Court of Human Rights. *Masaryk University Journal of Law and Technology*. 2022. Vol. 16. No. 1. P. 37-57 (*Scopus*).
3. Kovalenko Y. Balancing right to personal data protection towards other fundamental rights through the prism of the case law of the ECtHR and the CJEU. *Visegrad Journal on Human Rights*. 2022. No. 2. P. 52-57.

Наукові публікації, які засвідчують апробацію матеріалів дисертації:

4. Коваленко Ю. О. До питання становлення права на захист персональних даних у міжнародному праві. *Актуальні дослідження правової та історичної науки (випуск 24)*: матеріали міжн. наук.-практ. конф. (м. Тернопіль, 21 лип. 2020 р.). Тернопіль, 2020. С. 30-33.
5. Коваленко Ю. О. Еволюція європейських стандартів захисту персональних даних. *Актуальні проблеми законодавства України: пріоритетні напрями його вдосконалення*: матеріали міжн. наук.-практ. конф. (м. Одеса, 9-10 жовт. 2020 р.). Одеса, 2020. С. 13-16.
6. Kovalenko Y. O. Right to data protection in the times of COVID-19: challenges and prospects in the ECtHR. *Сучасне правотворення: питання теорії та практики*: матеріали міжн. наук.-практ. конф. (м. Дніпро, 4-5 черв. 2021 р.). Дніпро: ГО «Правовий світ», 2021. С. 145-149.
7. Kovalenko Y. The place of the right to data protection in the existent human rights framework. *Права людини як індикатор розвитку сучасної держави*: матеріали міжн.

наук.-практ. конф. (м. Київ, 13 груд. 2021 р.). Київ: «Видавництво Людмила», 2021. С. 16-18.

8. Коваленко Ю. Геномна інформація людини (ДНК): облік в умовах воєнного стану та ризики під час обробки. *Закон і Бізнес*. 2022. URL: https://zib.com.ua/ua/153699.html (дата звернення: 03.10.2023).

9. Коваленко Ю. О. До питання застосування Судом Європейського Союзу доктрини свободи розсуду та доктрини верховенства права ЄС в контексті захисту персональних даних. *Topical issues of modern jurisprudence*: *international scientific conference* (Częstochowa, Republic of Poland, 5-6 April 2023). Riga, Latvia: «Baltija Publishing», 2023. P. 224-228.

10. Коваленко Ю. О. Виконання Україною міжнародно-правових зобов'язань у сфері захисту персональних даних в контексті євроатлантичної інтеграції. *Science and Technology: LVII International Scientific and Practical Conference* (Great Britain, Birmingham, 14-15 September 2023). Birmingham, Great Britain: «Nika Publishing», 2023. P. 19-24.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

ВРУ	Верховна Рада України
ГА ООН	Генеральна Асамблея ООН
ДЄС	Договір про Європейський Союз
Директива 95/46/ЄС	Директива 95/46/ЄС Європейського Парламенту і Ради про захист фізичних осіб при обробці персональних даних і про вільне переміщення таких даних
ДФЄС	Договір про функціонування Європейського Союзу
Конвенція 1950 р., ЄКПЛ	Конвенція про захист прав людини і основоположних свобод 1950 р.
ЄС	Європейський Союз
ЄСПЛ	Європейський суд з прав людини
ЗУ	Закон України
Загальний регламент про захист даних	Регламент Європейського Парламенту і Ради (ЄС) 2016/679 про захист фізичних осіб у зв'язку з обробкою персональних даних і про вільний рух таких даних, та про скасування Директиви 95/46/ЄС
КСУ	Конституційний Суд України
КМРЄ	Комітет міністрів Ради Європи
Конвенція № 108	Конвенція № 108 про захист фізичних осіб у зв'язку з автоматизованою обробкою персональних даних 1981 р.
Конвенція № 108+	Конвенція № 108 про захист фізичних осіб у зв'язку з автоматизованою обробкою персональних даних, зі змінами, внесеними Протоколом CETS № 223
МПГПП 1966 р.	Міжнародний пакт про громадянські та політичні права
ОЕСР	Організація економічного співробітництва та розвитку
ООН	Організація Об'єднаних Націй
ПАРЄ	Парламентська асамблея Ради Європи
РЄ	Рада Європи
Суд ЄС	Суд Європейського Союзу
УПС	Угода про партнерство і співробітництво між Україною і Європейськими Співтовариствами та їх державами-членами
УА	Угода про асоціацію між Україною, з однієї сторони, та Європейським Союзом, Європейським співтовариством з атомної енергії і їхніми державами-членами, з іншої сторони
Хартія ЄС	Хартія Європейського Союзу про основоположні права

ВСТУП

Актуальність теми. З нестримним розвитком інформаційних технологій актуалізуються питання захисту персональних даних особи, становлення та еволюції права на захист персональних даних, формування та розвитку сучасних європейських стандартів у цій сфері.

Першочергово захист персональних даних розглядався як складова приватності та був тісно пов'язаний із закріпленням права на повагу до приватного життя в основних міжнародно-правових документах з прав людини – статті 12 Загальної декларації прав людини 1948 р., статті 17 Міжнародного пакту про громадянські та політичні права 1966 р., а згодом й у статті 8 Конвенції про захист прав людини і основоположних свобод 1950 р. Втім, широкомасштабна цифровізація та використання інтернет-технологій, хмарних технологій, технологій штучного інтелекту, популяризація транскордонного обміну даними зумовила необхідність розробки, прийняття та посилення стандартів захисту персональних даних, а також визнання права на захист персональних даних як основоположного права людини.

Актуальність обраної теми дослідження підкреслює те, що захист персональних даних регламентований у численних міжнародно-правових актах як безпосередньо, так і опосередковано, тобто через закріплення права на повагу до приватного та сімейного життя. Примітно, що у міжнародному праві прослідковується фрагментація норм щодо захисту персональних даних, що обумовлено відсутністю універсального міжнародного договору в цій сфері, а також культурними, історичними відмінностями у сприйнятті приватності та підходів до захисту персональних даних і, відповідно, існуванням конкуруючих правових режимів захисту даних. За відсутності такого міжнародного договору становлення стандартів захисту персональних даних відбувалося переважно у рамках діяльності Ради Європи та Європейського Союзу, а тому доволі поширеним у доктрині і практиці є використання категорії «європейські стандарти захисту персональних даних», що охоплює найбільш узагальнені, керівні правові засади, підходи та принципи у цій сфері.

Зауважимо, що для вітчизняної науки міжнародного права важливим є з'ясування стану адаптації національного законодавства і практики до європейських стандартів у сфері захисту персональних даних. Особливої актуальності це питання набуло з огляду на євроінтеграційний вектор зовнішньої політики України та набуття статусу кандидата на вступ до Європейського Союзу, адже обов'язок забезпечення належного рівня захисту персональних даних відповідно до найвищих міжнародних, зокрема європейських стандартів, встановлено статтею 15 Угоди про асоціацію між Україною, з однієї сторони, та Європейським Союзом, Європейським співтовариством з атомної енергії і їхніми державами-членами, з іншої сторони 2014 р. Окремої уваги заслуговує дослідження керівного акту Європейського Союзу у цій сфері - Регламенту Європейського Парламенту і Ради 2016/679 про захист фізичних осіб під час обробки персональних даних та їх вільного обігу (Загального регламенту про захист даних), що набув чинності 25 травня 2018 р., а також імплементація його положень у національне законодавство України.

У науці міжнародного права правове регулювання захисту персональних даних досліджувалося у працях вчених, серед яких Л. Биграве, Г. Грінліф, Б. ван дер Слот, А. В. Пазюк, П. М. Сухорольський. Окремі аспекти захисту персональних даних у Раді Європи та у судовій практиці Європейського суду з прав людини (далі – ЄСПЛ) висвітлювали – М. В. Бем, Н. Бистром, С. Гатвьорс, І. М. Городиський, Дж. МакБрайд, П. де Херт. Захист персональних даних у Європейському Союзі та Суді Європейського Союзу (далі – Суд ЄС) вивчали – І. З. Брацук, М.-П. Грандер, Г. Гонсалес-Фустер, С. Стромхольм, М. Тцану, І. М. Яворська.

Теоретичне розроблення окремих аспектів даної проблематики можна простежити у працях вітчизняних науковців, серед яких К. А. Андрущенко, В. М. Брижко, С. Б. Карвацька, Т. В. Комарова, В. Ю. Кузьма, С. Т. Мішуровська, В. І. Муравйов, Н. Б. Мушак, Н. М. Оніщенко, Р. А. Петров, О. С. Переверзева, І. М. Проценко, Ю. С. Размєтаєва, В. О. Серьогін, Л. Г. Фалалєєва, І. В. Яковюк та інші. Роботи цих авторів, безумовно, мають наукове та практичне значення, проте дослідження механізмів захисту персональних даних у Раді Європи та Європейському Союзі, сучасний стан, еволюція та перспективи розвитку, а також підходи ЄСПЛ та

Суду ЄС щодо забезпечення права на захист персональних даних у вітчизняній науці міжнародного права дослідженні лише фрагментарно.

Таким чином, актуальність дисертаційної роботи зумовлена необхідністю системного та комплексного дослідження теоретичних та практичних проблем, пов'язаних із захистом персональних даних у Раді Європи та Європейському Союзі, систематизації застосовуваних у цій сфері підходів і принципів, а також оцінки їх впливу на формування європейських стандартів захисту персональних даних. Водночас існує потреба у подальшому вивченні процесу формування теоретико-методологічних засад захисту персональних даних в Україні з огляду на судову практику ЄСПЛ та Суду ЄС та її впровадження в Україні, а також євроінтеграційний вектор зовнішньої політики України.

Мета і завдання дослідження. *Метою* дисертації є комплексний аналіз правових засад захисту персональних даних, сформованих у Раді Європи та Європейському Союзі, а також теоретичне обґрунтування впливу практики ЄСПЛ та Суду ЄС на формування і розвиток концептуальних підходів до захисту персональних даних, визначення перспективних напрямів розвитку доктринальної бази та формулювання практичних рекомендацій щодо модернізації механізму захисту персональних даних в Україні крізь призму європейських стандартів у цій сфері.

Досягненню мети дисертаційної роботи кореспондують такі *завдання*:

- проаналізувати становлення та розвиток права на захист персональних даних у доктрині та практиці міжнародного права, а також концептуальні підходи до права на захист персональних даних у сучасному міжнародному праві;

- розглянути понятійно-категоріальний апарат, зокрема такі ключові поняття, як «персональні дані», «чутливі дані», «обробка даних», «псевдонімізація», «знеособлення», «контролер даних», «оператор даних», «треті особи» та основні принципи захисту персональних даних;

- розкрити правові засади регулювання захисту персональних даних у Раді Європи та підходи ЄСПЛ у цій сфері;

- з'ясувати механізми захисту персональних даних в Європейському Союзі у світлі практики Суду ЄС;

- визначити та охарактеризувати особливості захисту персональних даних та вплив практики ЄСПЛ та Суду ЄС на формування європейських стандартів захисту персональних даних;

- дослідити законодавчі гарантії захисту персональних даних та практику їх забезпечення з огляду на виконання Україною міжнародно-правових зобов'язань у цій сфері;

- визначити стан впровадження європейських стандартів захисту персональних даних у законодавство України та напрями його вдосконалення;

- дослідити процес еволюції законодавства України у процесі його адаптації до *acquis* Європейського Союзу;

Об'єкт дослідження – міжнародно-правові та інтеграційні відносини, пов'язані з правом на захист персональних даних у ЄСПЛ та Суді ЄС, відповідно.

Предмет дослідження – правові засади регулювання захисту персональних даних, сформульовані в актах Ради Європи і Європейського Союзу в світлі практики ЄСПЛ та Суду ЄС.

Методи дослідження. Методологічну основу дисертаційної роботи становлять загальнонаукові та спеціальні методи наукового пізнання, застосовані для об'єктивного аналізу предмета дослідження.

Історико-правовий метод застосовано для аналізу виникнення права на захист персональних даних як основоположного права людини, а також розвитку європейських стандартів захисту даних і еволюції законодавства України у процесі адаптації до *acquis* ЄС (підрозділи 1.1, 1.2, 2.2, 3.1, 4.3). Використання загальнонаукових методів аналізу та синтезу дало змогу виявити спільні та відмінні риси наявних режимів захисту персональних даних (підрозділ 1.2). За допомогою логіко-семантичного методу досліджено та уточнено понятійно-категоріальний апарат, основні дефініції у сфері захисту персональних даних (підрозділи 1.3, 4.1, 4.2, 4.4).

За допомогою формально-логічного методу визначено основні міжнародно-правові поняття, пов'язані із захистом персональних даних (підрозділи 1.3, 4.1). Метод аналізу даних та збору інформації дозволив вивчити питання, пов'язані з

регламентуванням права на захист персональних даних у міжнародно-правових актах та практиці міжнародних судових органів у цій сфері (підрозділи 2.1, 3.1, 3.2). Системний метод надав можливість узагальнити основні принципи і підходи ЄСПЛ та Суду ЄС у сфері захисту персональних даних (підрозділи 2.2, 2.3, 3.3, 3.4). У процесі дослідження, шляхом порівняльно-правового аналізу даних вивчено проблемні аспекти захисту персональних даних у практиці ЄСПЛ та Суду ЄС, а також особливості імплементації європейських стандартів захисту персональних даних в Україні (підрозділи 2.2, 2.3, 3.3, 3.4, 4.2).

Наукова новизна отриманих результатів полягає в тому, що дисертація є одним з перших комплексних порівняльно-правових досліджень, у якому на підставі вивчення судової практики ЄСПЛ та Суду ЄС, а також доктринальних поглядів вітчизняних і зарубіжних вчених, з'ясовано теоретичні та практичні проблеми захисту персональних даних. До найбільш важливих результатів, що становлять наукову новизну, можна віднести наступні:

вперше:

- науково обґрунтовано значення і роль європейських стандартів захисту персональних даних у вітчизняній науці міжнародного права та у процесі вдосконалення національного законодавства. В умовах глобалізаційного розвитку європейські стандарти захисту персональних даних, як найбільш узагальнені, керівні правові засади, підходи та принципи у цій сфері, поступово набули значного поширення і сприяли гармонізації норм щодо захисту персональних даних на міжнародному рівні;

- обґрунтовано поділ європейських стандартів захисту персональних даних на три покоління з огляду на їх еволюційний розвиток, а саме на: перше покоління (Керівні принципи ОЕСР щодо захисту права на приватність і транскордонні потоки персональних даних, схвалені Рекомендацією Ради ОЕСР від 23 вересня 1980 р., та Конвенція № 108 про захист осіб у зв'язку з автоматизованою обробкою персональних даних 1981 р.), друге покоління (Конвенція № 108 про захист осіб у зв'язку з автоматизованою обробкою персональних даних 1981 р., оновлена Додатковим протоколом 2001 р., та Директива 95/46/ЄС про захист фізичних осіб при

обробці персональних даних і про вільне переміщення таких даних 1995 р.) та третє покоління (оновлена Конвенція № 108+ зі змінами, внесеними Протоколом CETS № 223, та Загальний регламент про захист даних 2016 р.). Європейські стандарти захисту персональних даних третього покоління – оновлена Конвенція № 108+ та Загальний регламент про захист даних – гарантують право на захист персональних даних як основоположне право кожної людини, незалежно від національності чи місця проживання, що свідчить про персоноцентричність та екстериторіальність застосування їх норм;

- систематизовано основні підходи, концепції і принципи, які використовують ЄСПЛ та Суд ЄС в контексті захисту персональних даних, а також вплив практики Європейського суду з прав людини та Суду ЄС на забезпечення основоположного права людини на захист персональних даних та утвердження європейських стандартів захисту персональних даних;

- визначено перспективні напрями адаптації законодавства України відповідно до європейських стандартів захисту персональних даних, що закріплені у Конвенції № 108+ зі змінами, внесеними Протоколом CETS № 223, та Загальному регламенті про захист даних, зокрема щодо оновлення основних термінів, таких як «контролер даних» та «оператор даних», та закріплення нових термінів, таких як «профайлінг», «псевдонімізація», «обмежена обробка», «наглядовий орган», удосконалення визначення поняття «згода на обробку даних», деталізації прав суб'єкта даних;

- обґрунтовано доцільність удосконалення інституційного механізму контролю у сфері захисту персональних даних в Україні відповідно до вимог європейських стандартів захисту персональних даних, з урахуванням критеріїв незалежності, об'єктивності, неупередженості та безсторонності, що сприятиме ефективній реалізації права на захист персональних даних;

удосконалено:

- підходи до періодизації становлення та розвитку європейських стандартів захисту персональних даних з огляду на національні, історичні та ідеологічні сприйняття права на приватність та права на захист персональних даних та існування різних конкуруючих моделей захисту даних – європейської, для якої характерна

наявність загального акту у сфері регулювання захисту персональних даних і створення єдиного контролюючого органу із захисту даних, а також американської, яка вирізняється наявність низки актів для різних галузей і, відповідно, покладення функції з контролю на різні органи у відповідних галузях;

- концепцію розмежування права на приватне життя та права на захист персональних даних з огляду на їх роль в інформаційному суспільстві, а також визнання права на захист персональних даних як самостійного основоположного права людини;

- підходи до узагальнення практики ЄСПЛ та Суду ЄС з урахуванням європейських стандартів захисту персональних даних, що визначає межі втручання держави у право на захист персональних даних та сприяє ефективній реалізації цього права;

- теорію співвідношення і розмежування категорій «персональні дані», «конфіденційна інформація», «інформація про приватне та сімейне життя» у вітчизняній науці міжнародного права. З урахуванням європейських стандартів захисту персональних даних, з метою забезпечення уніфікації термінологічного апарату у цій сфері виправданим є використання саме терміну «персональні дані» для позначення інформації, що підлягає обробці та містить відомості про ідентифіковану особу чи особу, яку можна ідентифікувати;

набули подальшого розвитку:

- концепція еволюції європейських стандартів захисту персональних даних з огляду на комп'ютеризацію суспільного життя, використання передових цифрових технологій та розвитку інформаційного суспільства;

- рекомендації щодо удосконалення законодавчого регулювання права на захист персональних даних в Україні задля підвищення ефективності останнього і законодавчого закріплення гарантій його захисту з огляду на впровадження новітніх технологій, глобалізаційні процеси, євроінтеграційну і євроатлантичну зовнішню політику України, виклики та загрози сучасності;

- оцінка необхідності вироблення в Україні єдиної судової практики з питань захисту персональних даних відповідно до європейських стандартів у цій сфері, а також орієнтованість на підходи, висвітлені у практиці ЄСПЛ та Суду ЄС.

Практичне значення одержаних результатів для вітчизняної науки міжнародного права полягає в тому, що сформульовані положення, висновки та пропозиції мають важливе значення для гарантування права на захист персональних даних як основоположного права людини, розуміння сучасних тенденцій розвитку європейських стандартів захисту персональних даних та визначення основних етапів імплементації європейських стандартів у цій сфері у законодавство України.

Викладені у дисертаційному дослідженні наукові положення і висновки можуть бути враховані: *у законотворчій діяльності* під час удосконалення законодавства відповідно до основних європейських стандартів захисту персональних даних; *у вітчизняній судовій практиці* в процесі правозастосування європейських стандартів захисту персональних даних; *у навчальному процесі* під час викладання дисциплін «Міжнародне право», «Теорія та практика міжнародного права», «Правові аспекти діяльності Ради Європи», «Право Європейського Союзу», під час підготовки навчальних посібників і програм з теорії та практики міжнародного права у сфері захисту основоположних прав людини, а також інших навчально-методичних матеріалів з питань захисту персональних даних.

Особистий внесок здобувача полягає у самостійній постановці й розробці наукової теми, з'ясуванні міжнародно-правових засад захисту персональних даних, систематизації підходів і принципів, застосованих у практиці ЄСПЛ та Суду ЄС при розгляді справ щодо захисту персональних даних, окресленні шляхів імплементації європейських стандартів захисту персональних даних у законодавство України.

Наукові положення, результати, висновки та практичні рекомендації, викладені у дисертації, отримано автором особисто.

Апробація матеріалів дисертації. Результати дослідження, його основні висновки та рекомендації оприлюднені на шести міжнародних науково-практичних конференціях, зокрема: *Актуальні дослідження правової та історичної науки (випуск 24)* (м. Тернопіль, 21 липня 2020 р.), *Актуальні проблеми законодавства України:*

пріоритетні напрями його вдосконалення (м. Одеса, 9-10 жовтня 2020 р.), *Сучасне правотворення: питання теорії та практики* (м. Дніпро, 4-5 червня 2021 р.), *Права людини як індикатор розвитку сучасної держави* (м. Київ, 13 грудня 2021 р.), *Topical issues of modern jurisprudence*: *international scientific conference* (Częstochowa, Republic of Poland, 5-6 April 2023), *Science and Technology: LVII International Scientific and Practical Conference* (Great Britain, Birmingham, 14-15 September 2023), а також у науковій публікації в електронному виданні.

Публікації. Основні положення та результати проведеного дослідження опубліковано у трьох наукових статтях, зокрема одна з них – у вітчизняному фаховому виданні, одна – у періодичному науковому виданні, проіндексованому в наукометричній базі даних Scopus, одна – у науковому періодичному виданні з фахового напряму держави-члена Європейського Союзу. Крім того, отримані результати було оприлюднено у шести тезах доповідей на міжнародних науково-практичних конференціях, а також у науковій публікації в електронному виданні.

Структура та обсяг дисертації. Дисертаційна робота включає вступ, чотири розділи, що охоплюють тринадцять підрозділів, висновки, список використаних джерел та додаток. Повний обсяг дисертації становить 261 сторінку, з них основний текст становить 214 сторінок, список використаних джерел налічує 346 найменувань і розміщений на 41 сторінці, додаток на 2 сторінки.

РОЗДІЛ 1. СТАНОВЛЕННЯ ТА РОЗВИТОК ПРАВА НА ЗАХИСТ ПЕРСОНАЛЬНИХ ДАНИХ У МІЖНАРОДНОМУ ПРАВІ

1.1 Виникнення права на захист персональних даних у доктрині та практиці міжнародного права

Інформація про людину, насамперед її ім'я, а також інші відомості про її приватне життя завжди розглядалася як важливий елемент для індивідуалізації та інтеграції людини у суспільство. Відтак важливою цінністю серед різноманіття прав людини є захист приватного аспекту життя особи або захист приватності (від лат. privatus – приватний, особистий), що тісно пов'язаний з людською честю, гідністю та репутацією.

Приватність як філософська категорія пов'язана з самореалізацією, самоствердженням, а також розширенням індивідуальної свободи, розвитку особистісної ідентичності поза будь-яким тиском. Вважається, що приватність утвердилась ще за доби виникнення перших цивілізацій, відтак приватність не можна тлумачити як надбання винятково західної культури [1, с. 517]. Концепція приватності має історичні витоки у добре відомих філософських дискусіях щодо питання розмежування публічної сфери політичної діяльності та приватної сфери, пов'язаної з сімейним та побутовим життям, індивідуальними інтересами, серед іншого, у працях Платона («Закони», «Держава») та Арістотеля («Політика»). Отже, поняття приватності має глибоке історичне коріння, що впливає на те як широко його сприймають та захищають у різних культурах.

Наприклад, у римському приватному праві термін «privatus» позначав осіб, які вийшли з сімейства і були звільнені від особистої залежності та підпорядкування главі сім'ї, відповідно, стали автономними і отримали свій особистий правовий статус та соціальне визнання. Відповідно, термін «приватний» інтерпретується як незалежний, автономний, водночас автономність особи розглядається як сукупність тих прав, які має така особа [2, с. 17].

Власне, як правовий інститут, який регулює захист недоторканності приватного життя, приватність вперше була закріплена в англо-саксонській правовій системі, де вона окреслюється терміном «прайвесі» (англ. privacy – приватна справа, таємниця,

усамітненість). Прайвесі як правова категорія пов’язана із захистом інтимної сфери приватного життя людини. У США відповідно до спеціального закону (The Privacy Act, 1974) до прайвесі належить: незаконне втручання у просторово обмежене місце існування особи чи втручання в її особисті справи, несанкціоноване опублікування фактів приватного життя особи, використання її імені в рекламі без відповідної згоди тощо [3, с. 53].

Варто зазначити, що у вітчизняній юридичній науці зустрічається використання правового терміну «privacy» як за допомогою транслітерації – прайвесі і, відповідно, право на прайвесі (В. О. Серьогін), так і шляхом перекладу з англійської – приватність, право на приватність (А. В. Пазюк, В. М. Брижко, Ю. С. Размєтаєва). Вважаємо, що найбільш рівнозначним відповідником терміну «прайвесі» в українській мові є саме термін «приватність».

Вважається, що вперше юридичне визначення приватності та дослідження персональних даних як юридичної категорії було сформоване в США і пов’язане з іменами американських вчених Семюеля Уоррена і Луїса Брендайса. У науковій статті «Право на приватність» 1890 р., опублікованій у журналі «Гарвардський огляд права» юристи С. Уоррен і Л. Брендайс дослідили чи чинний на той час закон дозволяв належним чином забезпечити захист конфіденційності інформації про особу. Вчені відзначили, що інтенсивність і складність життя, сприяли просуванню цивілізації, і людина, під вишуканим впливом культури, стала більш чутливою до публічності, відтак самотність і приватність є важливішими для особистості. Автори справедливо зазначили: «Звичаєве право закріплює за кожною людиною право визначити, зазвичай, в якій мірі її думки, почуття і емоції повинні бути передані іншим» [4]. Саме ці два науковці вперше спробували сформувати концепцію права на приватність як можливість особи контролювати інформацію про себе, а також проаналізували обмеження права на приватне життя та засоби його правового захисту, провівши аналогію із законами, що регулювали питання захисту від наклепу і дифамації, а також положень, що стосувалися захисту інтелектуальної власності.

Вагому роль у формуванні концепції захисту приватності у США мала прецедентна практика американських судів, зокрема, однією з найбільш знакових справ

є *Olmstead v. U.S.* (1928 р.). Ця справа є відомою, оскільки стосується вирішення питання про перехоплення розмов, однак більшу зацікавленість викликає не саме рішення у справі, а окрема думка судді Верховного Суду Л. Брендайса. Розглядаючи питання втручання у приватне життя державними установами суддя Л. Брендайс, не погоджуючись з рішенням суду, зазначив: *«… право особи бути залишеним у спокої є найбільш всеохопним з прав людини і є правом, яке найбільше цінується цивілізованими людьми. Щоб захистити це право, кожне невиправдане втручання уряду в приватне життя людини, не залежно від використаних засобів, слід вважати порушенням ...»* [5]. Згодом думка судді Л. Брендайса про «право бути залишеним у спокої» (англ. right to be alone) була розвинута в судових рішеннях американських судів, зокрема, у справі *Katz v. U.S.*, де Верховний Суд США встановив, що фіксація поліцією розмови особи в таксофонній кабінці призвела до порушення Четвертої поправки, оскільки особа обґрунтовано розраховувала на приватність, а також у справі *Stanley v. Georgia*, де було встановлено, що володіння непристойними матеріалами, що зберігалися особою у власному будинку, не є злочином, оскільки особа розраховує на приватність [6, с. 8]. Таким чином, з огляду на особливості судової системи та застосування прецеденту як джерела права у США, прийнято вважати, що саме у 1928 р. вперше відбулося юридичне закріплення такого поняття як право на приватність, яке згодом було розвинуте у судових рішеннях.

Втім, з розвитком суспільних відносин обсяг інформації про особу постійно збільшувався, а концепція приватності, яку описали С. Уоррен і Л. Брендайс у науковій статті 1890 р. і яка була розвинута в окремій думці судді Л. Брендайса у справі *Olmstead v. U.S.*, набувала все більшої актуальності. З метою систематизації та більш чіткого визначення нового права на приватність, що виникло з деліктного права, американський юрист В. Проссер у роботі 1960 р. зазначив, що гарантування приватного життя зумовлені чотирма різними видами втручань. Не претендуючи на точне визначення та визнаючи існування плутанини та суперечливості у розвитку законодавства про захист приватності, В. Проссер все ж запропонував класифікацію чотирьох деліктів у сфері приватності: 1) втручання в право особи на усамітнення або в її приватні справи; 2) публічне розголошення незручних, приватних фактів про особу; 3) гласність, яка

висвітлює особу в хибному світлі в очах громадськості; 4) привласнення імені або зовнішності особи в корисливих цілях [7, с. 389].

Різноманіття наявних концепцій приватності в американській правовій системі дає змогу здійснити умовну класифікацію підходів щодо її визначення, розглядаючи приватність як: 1) сукупність майнових прав та права на тілесну недоторканність (Дж. Томсон); 2) право бути залишеним у спокої (С. Уоррен, Л. Брендайс); 3) контроль за персональною інформацією (А. Вестін, В. Перент, Р. Мерфі); 4) індивідуальну гідність та цілісність, особисту автономію та незалежність (Е. Дж. Блоустейн); 5) інтимність та близькість у спілкуванні та міжособистісних стосунках (Ч. Фрід, Р. Герштейн, Дж. Іеннес, Т. Джереті, Дж. Рейчелс); 6) обмежений доступ до особи (С. Бок, Р. Гавісон, А. Аллен, А. Мур); 7) секретність інформації (Р. Поснер, А. Етціоні) [8].

Визначаючи межі приватності дослідники Д. Банісар і С. Дейвіс виокремлюють такі її складові: 1) інформаційна приватність, що передбачає встановлення правил, які регулюють збір та обробку персональних даних, таких як кредитна інформація та медичні записи; 2) тілесна приватність, яка стосується захисту тілесної недоторканності особи від примусових процедур, таких як тестування на наркотики та огляд порожнин тіла; 3) приватність комунікацій, яка стосується безпеки та конфіденційності пошти, телефонного спілкування, електронної пошти та інших видів зв'язку; 4) територіальна приватність, яка стосується встановлення правових обмежень щодо втручання сімейну сферу та інше оточення особи, зокрема, робоче місце чи громадські місця [9, с. 6]. Таким чином, в американській правовій системі саме інформаційна приватність розглядається як право на захист персональних даних у сучасному розумінні, оскільки стосується правил, що регулюють обробку персональних даних. Така класифікація відповідає розумінню приватності у сучасній теорії прав людини, яка використовується й вітчизняними науковцями [10, с. 336; 11, с. 27-29].

Що стосується розвитку приватності в європейському контексті, то як зазначає дослідник С. Стромхольм, право на приватність, хоча є переважно американською концепцією, однак у країнах континентальної Європи приватність розвивалася перш за все у правових системах таких країн, як Франція (праці науковців Перро та Нерсона, які наприкінці XIX ст. розвивали концепцію «права особистості» (англ. rights of the

personality), що включає право на зображення та ім’я, право на конфіденційність листування та право на захист інформації про приватне життя) та Німеччина (роботи вчених Гарейза, який у 1877 р. вперше обґрунтував концепцію «права особистості», що включає право особи організовувати своє життя, як їй подобається, право на ім’я людини та право на честь, а також роботи Кохлера та Гірке, які у 1895 р. розвинули цю концепцію, як таку, що включає права особи на життя, свободу, честь, соціальне становище, вільну діяльність, комерційну сферу діяльності, ім’я та право використовувати знаки, становлячи частину загального права особи на визнання її як особисті) [12, с. 27-30].

У європейських підходах захист приватного життя є формою захисту права на честь та особисту гідність. Відтак основою європейського розуміння права на приватність є права на власний образ, ім’я та репутацію, а також те, що німецькі науковці називають правом на інформаційне самовизначення - правом контролювати види інформації, що поширюються про особу. Це тісно пов’язані форми основного права на приватність, що передбачає право особи контролювати публічну інформацію про неї в дозволеному такою особою обсязі та право на захист від небажаного публічного розголосу, збентеження чи приниження [13, с. 1161].

Відмінність між концепцією приватності в американській та європейській площинах зумовлена підходом до розуміння самої суті приватності – американська концепція приватності розглядається як свобода людини, в яку держава не може втручатися (негативна свобода), водночас європейська концепція спрямована на захист честі та гідності особи (позитивна свобода). Інша відмінність полягає в тому, що в США основним джерелом захисту приватного життя є деліктне законодавство, тоді як в Європі приватність насамперед розглядається як конституційна гарантія. Втім, ці відмінності є умовними та повинні розглядатися крізь призму історичного розвитку – європейські країни на конституційному рівні визнають права громадян на захист від свавільного втручання уряду в право на повагу до приватного і сімейного життя, недоторканність житла та таємницю кореспонденції, у той час, як в США право на приватність виникло з судових прецедентів.

Водночас у міжнародному праві захист приватності пов'язують з визнанням і закріпленням у міжнародних договорах права на захист приватного життя як одного з основоположних прав людини. Так, вперше на міжнародному рівні право на повагу приватного життя було закріплено у ст. 12 Загальної декларації прав людини 1948 р., яка гарантувала, що ніхто не може зазнавати свавільного втручання у приватне і сімейне життя, посягання на недоторканність житла, таємницю кореспонденції або на честь і репутацію особи, одночасно встановлюючи право кожного на захист від такого втручання [14]. Прийнята ГА ООН як резолюція (рекомендаційного характеру), Загальна декларація прав людини 1948 р. формально не є юридично обов'язковим документом. Однак саме на основі її положень та з метою подальшого розвитку основоположних прав були прийняті численні міжнародно-правові документи з прав людини як універсального, так і регіонального рівня.

Подальше закріплення на універсальному рівні право на приватність віднайшло у статті 17 Міжнародного пакту про громадянські та політичні права 1966 р. (далі – МПГПП) згідно з якою кожен має право на захист приватного та сімейного життя, недоторканність його житла і таємницю кореспонденції, а також його честі та гідності не лише від свавільних, але й незаконних посягань [15]. Задля подальшого контролю за реалізацією прав, гарантованих МПГПП, був створений Комітет з прав людини, який є одним з найважливіших договірних органів контролю у сфері прав людини на універсальному рівні.

Варто зазначити, що ст. 17 МПГПП хоча й закріплює право на повагу приватного та сімейного життя в його традиційному розумінні, проте не містить явного посилання на гарантії захисту персональних даних людини. У 1988 р. Комітет з прав людини у Загальному коментарі № 16: Стаття 17 (Право на приватність) Право на повагу до приватного життя, сім'ї, житла та кореспонденції, а також захисту честі та репутації розтлумачив, що ст. 17 МПГПП поширюється й на захист персональних даних. Водночас Комітет з прав людини наголосив на важливості дотримання низки сучасних принципів захисту даних, зокрема, запровадження правового регулювання збору, обробки та зберігання персональних даних, впровадження ефективних заходів забезпечення безпеки даних, гарантування права особи на доступ, виправлення та

видалення даних [16]. Крім того, Комітет з прав людини розглядаючи питання дотримання державами ст. 17 МПГПП дотримувався вказаного підходу та виніс низку рішень, які стосуються саме захисту персональних даних. Наприклад, порушення права на приватність у контексті захисту персональних даних було виявлено у справі *Sayadi and Vinck v. Belgium*, що стосувалася незаконного розповсюдження персональних даних двох заявників, а саме у зв'язку зі внесенням їх імен та контактних даних до списку Санкційного комітету ООН, який був у вільному доступі в Інтернеті. Так, бельгійська влада посилаючись на ймовірний зв'язок заявників з терористичною групою Аль-Каїда передала персональні дані заявників до списку Санкційного комітету Ради Безпеки ООН, незважаючи на те, що кримінальне провадження ще не було завершене і ця інформація все ще відображалась у санкційному списку навіть після припинення кримінального провадження. Відтак, Комітет з прав людини зауважив, що держава-відповідач несе відповідальність за розповсюдження даних заявників, що призвело до втручання у їхнє приватне життя та незаконного посягання на честь і репутацію заявників [17]. Окрім того, у нещодавній справі *Andrea Vandom v. Republic of Korea* було розглянуто питання захисту даних щодо ВІЛ позитивного статусу заявниці, що належить до категорії так званих чутливих персональних даних, при оформленні нею як іноземцем робочої візи. Так, Комітет з прав людини наголосив, що обов'язкова політика тестування на ВІЛ та наркотики щодо іноземців не тільки була дискримінаційною, але й становила свавільне та необґрунтоване втручання у право на приватне життя, оскільки: 1) від заявниці вимагали розкриття свого ВІЛ позитивного статусу (тобто інформації, що належить до чутливих даних) державі-відповідачу; 2) органи держави-відповідача чинили тиск на заявницю з метою проходження такого тестування та погрожували скасуванням візи, якщо вона не виконає вимоги; 3) такі тести становили особистий огляд заявниці [18]. Відтак, як свідчить практика Комітету з прав людини, ст. 17 МПГПП, яка гарантує право на приватність, поширюється і на правовідносини, пов'язані із захистом персональних даних.

Проте закріплення права на приватність в основних міжнародних договорах з прав людини не мало своїм прямим наслідком визнання та врегулювання захисту персональних даних. Для усунення розбіжностей, що існували в національних законах,

та з метою гармонізації положень у сфері захисту персональних даних у рамках Організації економічного співробітництва та розвитку (далі – ОЕСР) було розроблено Керівні принципи щодо захисту права на приватність і транскордонні потоки персональних даних, схвалені Рекомендацією Ради ОЕСР від 23 вересня 1980 р. (далі – Керівні принципи ОЕСР). Принципи, викладені в згаданому акті, характеризуються чіткістю і гнучкістю застосування, оскільки сформульовані таким чином, щоб забезпечити їх пристосування до технологічних та інформаційних змін [19]. Таким чином, Керівні принципи ОЕСР стали першим узгодженим на міжнародному рівні інструментом рекомендаційного характеру, що закріпили положення, спрямовані на гармонізацію принципів використання персональних даних у національному та міжнародному праві [20, с. 14]. Варто зазначити, що Керівні принципи ОЕСР були оновлені у 2013 році з метою удосконалення підходів ОЕСР у багатьох важливих аспектах, серед іншого, концепції національної стратегії приватності, програм управління приватністю і повідомлення про порушення безпеки даних, а також посилення співробітництва та взаємодії у сфері охорони правопорядку.

Водночас з метою гармонізації правового регулювання захисту персональних даних ГА ООН також ухвалила Керівні принципи щодо регулювання комп'ютеризованих файлів персональних даних, затверджені Резолюцією ГА ООН 45/95 від 14 грудня 1990 р. (далі – Керівні принципи ООН), які містять основні рекомендації для національних органів щодо принципів захисту персональних даних [21]. Втім, Керівні принципи ООН не визнаються міжнародною спільнотою як універсальні міжнародні стандарти, оскільки є занадто загальними і розраховані на застосування до персональних даних, що зберігаються урядовими міжнародними організаціями, включаючи органи самої ООН, і не поширюються на питання транскордонної передачі даних. Відтак Керівні принципи ООН, як і Керівні принципи ОЕСР, здебільшого мають значення як підстава для ухвалення інших актів у сфері захисту персональних даних, оскільки вони є актами рекомендаційного характеру. Ці рекомендаційні норми є узагальненим викладом основних принципів щодо автоматизованої обробки персональних даних, а відтак сприяють уніфікації норм у сфері захисту персональних даних.

Починаючи з 2013 року ГА ООН прийняла ще декілька резолюції щодо приватності в епоху цифрових технологій у відповідь на розвиток нових технологій та викриття фактів масового спостереження у світлі заяв зроблених Е. Сноуденом. У згаданих резолюціях було засуджено практики масового спостереження та закликано держави вжити заходи щодо захисту права на приватне життя, серед іншого, у контексті цифрових комунікацій, включаючи перегляд законодавства щодо масового спостереження, перехоплення комунікацій та збору персональних даних [22; 23]. Водночас переглянутий у 2016 році проєкт Резолюції наголошував не лише на необхідності обмеження повноважень державних органів, але й відповідальності приватного сектору щодо збору, використання, поширення і збереження персональних даних, а також запровадження прозорої політики обробки даних, а переглянутий у 2020 році проєкт Резолюції – на важливості приватності з огляду на технології штучного інтелекту або машинного навчання, які несуть ризики дискримінації [24; 25]. Все ж зауважимо, що на рівні ООН питання захисту персональних даних розглядається тільки як аспект права на приватне життя і норми щодо захисту даних ухвалені в рамках діяльності ООН не є зобов'язальними.

Що стосується захисту приватності на регіональному рівні, то у рамках діяльності РЄ право на приватне життя було деталізовано у ЄКПЛ, яка гарантує право на повагу до приватного та сімейного життя у частині 1 статті 8. Водночас частина 2 статті 8 ЄКПЛ регламентує виключні випадки втручання у право на повагу до приватного життя, що можуть бути здійснені згідно із законом та у випадках, необхідних у демократичному суспільстві в інтересах національної та громадської безпеки або економічного добробуту країни, з метою запобігання заворушенням і злочинам, для захисту здоров'я або моралі чи з метою захисту прав інших людей [26].

Звісно, право на приватність також гарантоване на рівні міжамериканської та африканської систем захисту прав людини. Так, право на приватність закріплене у ст. 11 Американської конвенції з прав людини 1969 р. згідно з якою ніхто не може зазнавати свавільного чи недобросовісного втручання в його приватне життя, сім'ю, житло або кореспонденцію, а також зазнавати незаконних нападів на його честь або репутацію [27]. Втім, на відміну від ЄКПЛ та Американської конвенції з прав людини, в Африканській

хартії прав людини та народів 1981 р. на момент її прийняття положення щодо захисту приватності були відсутні. Однак це право було проголошено у статті 4 Декларації Африканської комісії з прав людини і народів про принципи свободи вираження в Африці 2002 р., згідно з якою кожному гарантується право на доступ до інформації, що зберігається державними чи приватними органами, та право кожного на доступ та оновлення або іншим чином виправлення персональних даних щодо себе, незалежно від того, зберігаються вони державною чи приватною структурою [28]. У 2019 році була прийнята оновлена Декларація про принципи свободи вираження та доступу до інформації в Африці, яка удосконалила гарантії права отримувати інформацію, а також права на свободу вираження та поширювати інформацію, що гарантовано ст. 9 Африканської хартії прав людини та народів 1981 р. [29].

Право на приватність та захист персональних даних закріплено також і в інших міжнародно-правових актах у сфері прав людини, зокрема, ст. 18 Каїрської декларації прав людини в ісламі 1990 р., ст. 9 Африканської хартії про права і добробут дитини 1990 р., ст. 16 та 21 Арабської хартії прав людини 2004 р., ст. 21 Декларації прав людини Асоціації держав Південно-Східної Азії. Водночас принципи захисту приватності та персональних даних викладені у Системі норм щодо приватності Азійсько-Тихоокеанського економічного співробітництва, які хоч і не є юридично обов'язковими, все ж детально регламентують основні принципи захисту персональних даних в рамках діяльності держав Азійсько-Тихоокеанського регіону, зокрема, Австралії, Нової Зеландії, Японії, Таїланду, США, Канади [30].

Таким чином, вищезгадані міжнародно-правові акти узагальнили основи захисту приватного життя людини. Проте як видно зі змісту, зокрема, ст. 12 Загальної декларації прав людини, ст. 17 МПГПП та ст. 8 ЄКПЛ, право на захист персональних даних не було прямо визначено в цих міжнародних документах. До того ж норми універсальних міжнародних договорів містили доволі загальне визначення права на приватне життя, а регіональні договори, хоча й більш чітко визначали межі втручання у це право, проте не деталізували окремі аспекти приватності.

У цьому плані поділяємо думку С. Т. Мішуровської, яка зазначає, що міжнародно-правове закріплення права на приватне життя найбільш повноцінно втілено у

загальному міжнародному праві та у регіональних міжнародних договорах. Втім, у міжнародних договорах закріплено лише зміст права на приватне життя і відсутні положення щодо можливостей та шляхів його обмеження. Водночас характерною рисою регіональних договорів є те, що право за змістом може відрізнятися залежно від правових традицій регіону, що не вважається порушенням загального міжнародного права. Крім того, регіональні міжнародні договори, зокрема, ЄКПЛ 1950 р., Американська конвенція про права людини 1969 р., Африканська хартія прав людини 1981 р., деталізують положення щодо обмеження прав, що пов'язано з культурною єдністю держав, що уклали ці міжнародні договори, і, відповідно, надає можливість підвищити рівень міжнародного контролю за дотриманням закріплених у них прав людини [31, с. 14].

Досліджуючи еволюцію права на захист персональних даних у міжнародному праві, варто зазначити, що тривалий час воно розглядалося лише як складова права на повагу до приватного життя і було нерозривно пов'язане із захистом інших основоположних прав людини, зокрема, права на доступ до інформації і права на свободу думки. Вочевидь з розвитком суспільних відносин обсяг інформації про особу нестримно збільшувався, виникала необхідність у транскордонній передачі персональних даних, таким чином прогалина у міжнародно правовому регулюванні захисту персональних даних лише зростала. Окремим питанням постала й необхідність масової обробки та зберігання великої кількості даних про особу, а зважаючи на стрімкий розвиток науково-технічного прогресу та комп'ютеризацію основних сфер життя людини стало очевидним, що загальні норми щодо захисту права на приватне життя не здатні повноцінно забезпечити захист персональних даних про особу [32, с. 16].

Саме у цей період у рамках діяльності КМРЄ були прийняті Резолюція (73) 22 «Про захист недоторканості приватного життя осіб стосовно електронних банків персональних даних у приватному секторі» від 26 вересня 1973 р. та Резолюція (74) 29 «Про захист недоторканості приватного життя осіб стосовно електронних банків персональних даних у публічному секторі» від 20 вересня 1974 р. Ці резолюції встановили принципи у сфері захисту персональних даних при їх обробці у приватному та публічному секторах. Водночас згадані акти хоча і регламентували питання захисту

персональних даних, однак переважно лише доповнювали зміст права на приватність, гарантованого у ст. 8 ЄКПЛ, оскільки були нерозривно пов'язані з ним. Відтак, право на захист персональних даних у цей період беззаперечно розглядалося лише у безпосередньому взаємозв'язку із правом на приватне життя [33, с. 30-31].

Упродовж п'яти років після ухвалення другої Резолюції КМРЄ правові засади захисту персональних даних були закріплені у національному законодавстві європейських держав, зокрема, Німеччині, Швеції, Данії, Франції, Норвегії, Люксембургу. Крім того, питання захисту персональних даних було включене й до Основних Законів держав: ст. 35 Конституції Португалії 1976 р., ст. 18 Конституції Іспанії 1978 р., ст. 1 Австрійського закону про захист даних 1978 р. тощо [34].

Вочевидь первинні правові інструменти захисту персональних даних були прийняті для забезпечення права на приватність, а право на захист персональних даних розглядалося лише як один з його аспектів і не було чітко визначене, що створювало прогалину в правовому регулюванні. Водночас у національному законодавстві країн все ще прослідковувалася значна диференціація між нормами щодо захисту персональних даних, а у міжнародному праві рівень захисту персональних даних залишався не достатнім та створював ризики втручання у права людини, слугуючи передумовою для конфліктів між особою та державою чи міжнародною організацією, наприклад ООН, Інтерполом, що обробляють великі обсяги персональних даних. Як слушно зауважує вітчизняна дослідниця І. М. Сопілко, у цей період держави звернули увагу на питання правового регулювання обігу інформації про фізичну особу і фактично розробили нове суб'єктивне право фізичної особи на її персональні дані [35, с. 63]. Таким чином, можна стверджувати, що захист персональних даних розглядається у доктрині та практиці як сфера правового регулювання та як основоположне право людини.

Виникнення права на захист персональних даних як самостійного, основоположного права, відокремленого від права на захист приватного життя, частково також пов'язують із закріпленням основних правових засад захисту даних у національних законодавчих актах держав Північної Європи, а також публікацією у 1970-х рр. у США так званих принципів Справедливих інформаційних практик (англ. Fair Information Practices, FIPs), що були розроблені з огляду на виникнення «сучасних»

проблем захисту права на приватне життя у зв'язку з популяризацією використання автоматизованої обробки даних [36, с. 3-4]. Поширене використання великих баз даних спричинило низку проблем у застосуванні концепції права на приватне життя, яка спрямована на захист приватних інтересів громадян, серед іншого, шляхом надання їм права контролю над приватними та конфіденційними даними [33, с. 30; 37]. Водночас у 1960-1980-их рр. у США були прийняті низка нормативно-правових актів, що регулювали питання захисту персональних даних, а саме: Про свободу інформації 1966 р. (The Freedom of Information Act), Про надання кредитної інформації про покупця 1970 р. (The Fair Credit Reporting Act), Про приватність 1974 р. (The Privacy Act), Про право на фінансову приватність 1978 р. (The Right to Financial Privacy Act), Про захист конфіденційності відеоматеріалів 1980 р. (The Video Privacy Protection Act) та інші [38, с. 73-74]. У США захист персональних даних здійснюється через низку нормативно-правових актів, які детально регламентують питання приватності та захисту даних в окремих сферах суспільного життя, таким чином режим захисту даних у США дещо відрізнявся від підходів, притаманних європейському регіону.

Вважаємо, що закріплення основних міжнародних стандартів у сфері захисту персональних даних значною мірою відбувалося саме в рамках діяльності РЄ та ЄС. Зважаючи на те, що саме на РЄ покладено відповідальність за забезпечення розвитку права на повагу до приватного життя, яке гарантоване ст. 8 ЄКПЛ, Комітетом РЄ з правових питань у 1971 р. було сформовано Комісію експертів з приватності та комп'ютерів для розробки відповідних актів у сфері захисту персональних даних. Втім, неузгодженість національних підходів щодо захисту персональних даних призвела до труднощів у передачі персональних даних через кордони. Так, у 1978 р. влада Швеції відмовилася передати персональні дані до Великої Британії з огляду на те, що законодавство останньої на той час не містило положень, які б гарантували захист персональних даних. Відтак під час роботи Комісії експертів з приватності та комп'ютерів стало очевидним, що досягнення ефективності у захисті персональних даних нерозривно пов'язано з удосконалення національних правових актів шляхом використання міжнародних інструментів, а тому розпочалась робота над розробкою проєкту майбутньої конвенції РЄ щодо захисту персональних даних [39].

Власне, вже у 1981 р. у рамках РЄ була прийнята Конвенція про захист осіб у зв'язку з автоматизованою обробкою персональних даних 1981 р. (далі – Конвенція № 108), яка є першим міжнародним договором, що стосується права на захист персональних даних. Варто наголосити на визначальній ролі Конвенції № 108, спрямованої на правове забезпечення співробітництва не лише держав-членів РЄ, але й третіх країн, оскільки належить до розширених міжнародних договорів РЄ. Метою Конвенції № 108 є забезпечення кожному, незалежно від громадянства або місця проживання, дотримання його основоположних прав, зокрема права на недоторканість приватного життя, у зв'язку з автоматизованою обробкою персональних даних. Примітно, що саме Конвенція № 108 вперше на міжнародному рівні закріпила поняття персональних даних як відомості чи сукупність відомостей про особу, яка ідентифікована або може бути конкретно ідентифікована, а також встановила гарантії захисту особливої категорії даних, так званих чутливих даних, що включають відомості про расову приналежність, політичні, релігійні чи інші переконання, дані щодо здоров'я та статевого життя та дані щодо засудження. Крім того, Конвенція № 108 закріпила основні принципи захисту персональних даних, гарантії для осіб, дані яких обробляються, а також спеціальні правила щодо транскордонної передачі даних та механізми співробітництва і консультацій між державами-учасницями Конвенції [40]. Хоча у тексті Конвенції № 108 відсутні положення, що безпосередньо закріплюють право на захист персональних даних, саме із її прийняттям у міжнародному праві відбулося становлення стандартів захисту персональних даних. Це слугувало передумовою для подальшого визнання та гарантування права на захист персональних даних, яке раніше було закріплене опосередковано, виключно у світлі права на захист приватного життя.

Розглядаючи питання становлення права на захист персональних даних у рамках ЄС слід зазначити, що поштовхом до більш комплексного вивчення проблеми захисту персональних даних стали дві резонансні справи, пов'язані з проблемою транскордонної передачі даних як всередині Європи, так і при передачі даних за межі континенту. Першою з них була ситуація щодо заборони Французьким агентством із захисту персональних даних передачі інформації щодо французьких працівників автомобільної

компанії «Фіат» до головного офісу компанії в Італії. Основна проблема полягала в тому, що автомобільна компанія не могла забезпечити достатній рівень захисту персональних даних та водночас не погоджувалася із законодавством Франції про захист даних. Інша ситуація була пов'язана з відмовою німецького банку надати своєму підрозділу, що знаходився в Гонконзі, інформацію стосовно клієнтів банку, які були громадянами Німеччини [41, с. 87]. Відповідно, хоча національне законодавство держав закріплювало певні стандарти захисту персональних даних, різноманіття національних підходів у цій сфері призводило до відмови у міжнародному співробітництві.

Вказані випадки вимагали вжиття заходів задля забезпечення ефективності функціонування державного та приватного сектору, а також міжнародного співробітництва. Тому поступово Європейське Співтовариство почало залучатися до розробки принципів захисту персональних даних, що відрізнялися від підходів РЄ. У ЄС, основними завданнями якого є посилення та сприяння розвитку економічного ринку, обробка персональних даних частково належала до сфери економіки, позаяк головна увага у РЄ полягала у захисті прав людини на європейському континенті [37]. Відтак перешкоди, які виникли в економічному секторі, стали передумовою для розробки та подальшого затвердження основного правового інструменту ЄС у сфері захисту персональних даних, яким тривалий час залишалася прийнята у 1995 р. Директива 95/46/ЄС про захист фізичних осіб при обробці персональних даних і про вільне переміщення таких даних (далі – Директива 95/46/ЄС).

Директива 95/46/ЄС, метою якої була гармонізації національного законодавства у сфері захисту персональних даних, як і Конвенція № 108, гарантувала захист прав людини при обробці персональних даних, однак розглядала це питання в контексті права на захист приватного життя. Фактично у Директиві 95/46/ЄС було втілено два ключових аспекти – можливість вільного переміщення персональних даних, що сприяло розвитку економічних відносин, та чіткі гарантії захисту прав суб'єкта даних, включаючи вимоги щодо отримання поінформованої згоди на обробку персональних даних, обробку даних у чесний та законний спосіб, для встановлених, чітких і законних цілей та не довше, ніж це необхідно для цілей обробки. Водночас було наголошено, що персональні дані повинні бути достовірними і постійно оновлюватися, а у разі якщо потреба у їх обробці

відпала дані необхідно видалити. Понад те, Директива 95/46/ЄС закріпила розширений перелік відомостей, що становлять персональні дані, зокрема, до цієї категорії було віднесено ідентифікаційний код або один чи більше факторів, притаманних фізичним, фізіологічним, розумовим, економічним, культурним чи соціальній ідентичності, особи, яку ідентифікують. Важливою гарантією було також вимога створення незалежних національних органів з питань захисту персональних даних у державах-членах ЄС [42].

Аналізуючи положення Директиви 95/46/ЄС можна дійти висновку, що правовий захист персональних даних здійснюється на основі: *принципу персоноцентризму* (слугує перш за все для захисту прав людини), *принципу екстериторіальності* (контролери даних незалежно від національності чи місця проживання фізичних осіб повинні поважати їх права), а також *принципу субсидіарності* (обробка персональних даних у ЄС повинна відбуватись згідно із законодавством однієї з держав-членів; повноваження контролера даних, створеного у державі-члені ЄС, повинні визначатися національним законодавством; держави-члени за власним бажанням визначають ризики для прав суб'єктів даних у своєму законодавстві) [43, с. 59]. Таким чином, у рамках ЄС первинне правове регулювання захисту персональних даних розглядалося у його тісному взаємозв'язку з правом на приватність.

Щоправда, невдовзі право на захист персональних даних як самостійне право було закріплено у Хартії Європейського Союзу про основоположні права (далі – Хартія ЄС), яка у 2000 р. була проголошена як політична декларація, а з набранням чинності Лісабонським договором її адаптована редакція 2007 р. має юридичну силу установчих договорів ЄС [44, с. 905]. Відтак на рівні ЄС право на захист персональних даних визнане основоположним правом з набранням чинності Лісабонським договором у 2009 р., що вніс зміни до установчих договорів ЄС. Відповідно, право на захист персональних даних було закріплене у статті 16 Договору про функціонування Європейського Союзу (далі - ДФЄС) та гарантоване у статті 8 Хартії ЄС. Перший абзац статті 8 Хартії ЄС проголошує, що кожен має право на захист персональних даних, у той час, як другий абзац встановлює принципи обробки даних, а саме «дані повинні оброблятися справедливо, для конкретних цілей та на основі згоди зацікавленої особи або на основі будь-якої іншої основи, встановленої законом», і що «кожен має право доступу до даних,

які були зібрані стосовно неї чи нього, та право на їх виправлення». Нарешті, третій абзац ст. 8 Хартії ЄС додає, що «дотримання цих правил підлягає контролю незалежним органом» [45]. Відтак саме Хартія ЄС, з одного боку, вперше закріпила у статті 8 право на захист персональних даних як самостійне право, відокремлене від права на захист приватного життя, а, з іншого боку, гарантувала його захист як основоположного права у ЄС. Піднесення захисту персональних даних до категорії основоположних прав на рівні ЄС мало вирішальне значення задля посилення ефективності захисту, який фактично надається фізичним особам через право ЄС в процесах, пов'язаних з обробкою персональних даних [46].

Варто зазначити, що з метою узгодження стандартів захисту персональних даних у Європі, прослідковується й послідовність в адаптації положень Конвенції № 108. Зокрема, у 2001 році був прийнятий Додатковий протокол до Конвенції № 108, який узгодив низку її положень з Директивою 95/46/ЄС, включаючи вимоги до створення органів у сфері захисту даних та обмеження експорту даних на основі «адекватності», тобто для належного виконання заявленої мети. З часом стандарти захисту персональних даних, викладені у Конвенції № 108 та Директиві 95/46/ЄС, відставали від умов інформаційного та соціального розвитку суспільства, а тому потребували оновлення.

У світлі новітніх інформаційно-технологічних розробок Європейська Комісія розробила низку актів, що оновлюють систему захисту персональних даних в ЄС. Правовим актом, що оновив і деталізував засади захисту персональних даних, які були раніше викладені у Директиві 95/46/ЄС, є прийнятий 27 квітня 2016 р. Регламент ЄС 2016/679 про захист фізичних осіб під час обробки персональних даних та їх вільного обігу, та про скасування Директиви 95/46/ЄС (Загальний регламент про захист даних). Загальний регламент про захист даних 2016 р., на відміну від Директиви 95/46/ЄС, є актом прямої дії, що гарантує право на захист персональних даних на рівні основоположних прав людини та регламентує основні принципи захисту цього права. Водночас Загальний регламент про захист даних 2016 р. значно розширює права суб'єктів персональних даних, наділяючи їх правом на отримання інформації про обробку даних, право на доступ, виправлення та видалення даних, а також вперше закріплює положення, що спрямовані на захист персональних даних дітей. Окрім того,

даний правовий акт значно збільшує категорію відомостей, що становлять персональні дані, передбачивши, серед іншого, захист даних про місцеперебування, онлайн-ідентифікаторів (IP-адреса, «cookies»), генетичних та біометричних даних [47]. Важливим є й той факт, що Загальний регламент про захист даних 2016 р. має екстериторіальне застосування, адже спрямований на захист прав людини не тільки на території ЄС, але і поза його межами.

Крім того, у вересні 2009 р. також був ініційований процес оновлення Конвенції № 108 і хоча положення модернізованої Конвенції № 108 в основному були доопрацьовані у 2014 р., її завершення було відкладено до прийняття Загального регламенту про захист даних 2016 р. Основною причиною такої затримки, як стверджує Г. Грінліф, стало бажання забезпечити послідовність та узгодженість оновленої Конвенції № 108, яку зазвичай називають Конвенція № 108+, з правовою базою ЄС [48].

У 2018 р. текст Конвенції № 108 було оновлено Протоколом (CETS № 223) про внесення змін до Конвенції № 108 (далі – Протокол), який наразі відкритий для підписання. Передбачається, що Протокол набере чинності в одному з альтернативних випадків: 1) у разі його ратифікації усіма державами-учасницями Конвенції № 108, або 2) 11 жовтня 2023 р. за умови ратифікації Протоколу 38 державами-учасницями Конвенції № 108. Метою оновлення положень Конвенції № 108 було вирішення проблем, пов’язаних із приватністю, що виникають внаслідок використання новітніх інформаційно-комунікаційних технологій, та посилення механізму Конвенції № 108 для забезпечення її ефективного впровадження. Примітно, що оновлений текст Конвенції № 108+ у статті 3 гарантує право кожної особи на захист персональних даних. До нововведень також можна віднести запровадження поняття розпорядника персональних даних та введення уніфікованого терміну «обробка персональних даних», відповідно, Конвенція № 108+ поширюватиметься на випадки обробки даних, як за допомогою автоматизованих систем, так і вручну. Окрім того, Конвенція № 108+ встановлює особливий порядок обробки генетичних, біометричних даних, так званих «чутливих даних», що стосуються расової належності, політичних, релігійних чи інших переконань, а також даних, що стосуються здоров’я або статевого життя, вчинених правопорушень, кримінальних проваджень, судимостей та пов’язаних із ними заходів

безпеки. Водночас важливим положенням Конвенції № 108+ є встановлена у ст. 26 і 27 можливість приєднання до неї ЄС та інших міжнародних організацій, які у розмінні Конвенції № 108+ визначаються як організації, що керуються міжнародним публічним правом [49]. У пояснювальній доповіді до Конвенції № 108+ наголошується, що вона охоплює «прямо та опосередковано всі принципи та правила, викладені в праві ЄС, одночасно надаючи Сторонам певну свободу розсуду» [50]. Примітно, що оновлена Конвенція № 108+ повністю не копіює формулювання Загального регламенту про захист даних 2016 р., проте відображає подібні концепції і підходи щодо гарантування права на захист персональних даних.

Зауважимо, що сфера захисту персональних даних також невпинно розвивається на рівні Африканського Союзу, адже широке впровадження комп'ютерних технологій та Інтернету в Африці викликало занепокоєння щодо необхідності сприяння управлінню кібербезпекою та кіберстабільністю на всьому континенті, що призвело до прийняття у 2014 році Конвенції Африканського Союзу про кібербезпеку та захист персональних даних (далі – Конвенція Африканського Союзу) [51]. Згодом задля сприяння імплементації Конвенції Африканського Союзу основні її положення були розтлумачені у Керівних принципах щодо захисту персональних даних для Африки 2018 р., які втілюють 18 рекомендацій, розроблених спільно Комісією Африканського союзу у співробітництві з міжнародною професійною організацією Інтернет-суспільство (ISOC), яка створена з метою забезпечення відкритого розвитку, еволюції та використання Інтернету. Відзначимо, що положення Конвенції Африканського Союзу цілком відповідають основним регіональним та міжнародним стандартам у сфері захисту персональних даних, зокрема, праву ЄС та Конвенції № 108. Попри доволі прогресивні положення, викладені у Конвенції Африканського Союзу станом на початок жовтня 2023 року її ратифікувало лише 14 з 55 держав-учасниць Африканського Союзу, а для набрання нею чинності необхідна ратифікація щонайменше 15 держав [52]. Окрім того, Конвенція Африканського Союзу хоча і проголошує, що кожна держава-учасниця зобов'язується створити правову базу, спрямовану на зміцнення основоположних прав, зокрема захисту персональних даних, і покарати будь-яке порушення приватності, не завдаючи шкоди принципу вільного переміщення персональних даних (ст. 8), на

практиці ці положення не є дієвими. Хоча деякі держави Африканського Союзу й прийняли закони про кібербезпеку та захист персональних даних, існують випадки, коли такі закони сформульовані досить розмито і часто такі положення використовується для придушення політичного інакомислення, а не для захисту громадян [53, с. 9]. Незважаючи на певні недоліки, той факт, що Африканський Союз визнає важливість захисту громадян від кіберзлочинності та розробки сучасного законодавства щодо захисту персональних даних є позитивною рисою для забезпечення єдності правового регулювання у цій сфері в африканському регіоні. Крім того, закріплені Конвенцією Африканського Союзу стандарти захисту персональних даних узгоджуються з чинними міжнародними-правовими актами у цій сфері, зокрема європейськими стандартами захисту даних.

Враховуючи викладене, можна констатувати, що міжнародно-правове регулювання захисту персональних даних потребує удосконалення. Положення більшості договірних та інших актів, що регулюють питання обігу та обробки персональних даних є регіональними, водночас інші міжнародні інструменти захисту персональних даних не є юридично обов'язковими. Становлення права на захист персональних даних у міжнародному праві відбувалося разом зі стрімким технологічним розвитком, але донині у доктрині немає єдності щодо вичерпного визначення категорії персональних даних та чіткого розмежування між правом на приватність та правом на захист персональних даних [54, с. 65].

Таким чином, починаючи з середини XX століття із закріпленням у низці міжнародних договорів права на захист приватного життя як одного з основоположних прав людини, питання захисту персональних даних розглядалися виключно у світлі захисту права на приватність. Розвиток інформаційних технологій та їх активне впровадження у публічній і приватній сферах життя у другій половині XX – початку XXI століття зумовив зміну підходу до визнання права на захист приватного життя у зв'язку з обробкою персональних даних про особу та поступово призвів до становлення права на захист персональних даних як самостійного права. Право на захист персональних даних *sui generis* слід розглядати як тісно пов'язане та таке, що доповнює традиційні права, закріплені в ЄСПЛ та МПГПП, оскільки захист даних прагне забезпечити повне

та ефективне застосування основоположних прав людини у відносно новому цифровому контексті.

Утвердження права на захист персональних даних пов'язують саме з активною діяльністю РЄ та ЄС. Власне, саме Конвенція №108 та Директива 95/46/ЄС регламентували основні питання захисту персональних даних, створюючи основу дотримання права на захист приватного життя. Поступово питання захисту персональних даних набули своєї самобутності, що сприяло виникненню та закріпленню права на захист персональних даних. Сучасною тенденцією розвитку права на захист персональних даних у міжнародному праві є його закріплення як самостійного права, відокремленого від права на захист приватного життя. На рівні ЄС визнання та гарантування права на захист персональних даних на рівні основоположного права людини відбулося з набранням чинності Лісабонським договором у 2009 р. Прийняття Загального регламенту про захист даних 2016 р. сприяло подальшій деталізації права на захист персональних даних і визначення основних стандартів захисту у цій сфері на рівні ЄС. Втім, наразі єдиним юридично обов'язковим міжнародно-правовим актом глобального значення у сфері захисту персональних даних залишається Конвенція № 108. Незважаючи на динамічність процесу розвитку та модернізації положень Конвенції № 108, її оновлена редакція хоча і гарантує право на захист персональних даних, проте ще не набрала чинності, відтак процес визнання та закріплення права на захист персональних даних у міжнародному праві не є завершеним. Водночас на універсальному рівні ООН визнає та забезпечує захист персональних даних виключно крізь призму права на приватне життя, а прийняті на рівні ООН акти, що стосуються захисту персональних даних, мають рекомендаційний характер. Відповідно, питання розробки універсальних міжнародних договорів у сфері захисту персональних даних досі не втратило своєї актуальності.

1.2 Концептуальні підходи до права на захист персональних даних у сучасному міжнародному праві

Право на захист персональних даних виникло порівняно нещодавно у відповідь на виклики інформаційно-технологічного розвитку людства, але як у науці, так і в практиці

міжнародного права досі немає єдності щодо природи права на захист персональних даних, а також моделей захисту персональних даних. Дійсно, з моменту закріплення основоположних прав людини у міжнародних договорах питання, пов'язані із захистом персональних даних, розглядалися виключно у світлі права на приватність, а тому первинні міжнародно-правові акти – Загальна декларація прав людини 1948 р., МПГПП, ЄКПЛ та інші регіональні міжнародні договори – закріплювали гарантії від втручання у приватне життя особи і гарантії захисту персональних даних як аспект приватного життя. З розвитком інформаційних технологій, впровадженню комп'ютеризації та Інтернет-технологій питання захисту персональних даних та нових загроз для приватності вимагали якнайшвидшого розв'язання. Відтак почали розвиватися нові механізми захисту персональних даних, зокрема, Конвенція № 108 та Директива 95/46/ЄС, які наголошували на необхідності захисту права на повагу до приватного життя при обробці персональних даних і, таким чином, все ж надавали певної самостійності праву на захист персональних даних.

Сучасною тенденцією розвитку права на захист персональних даних у міжнародному праві є його закріплення як самостійного права, відокремленого від права на захист приватного життя. Більше того, право на захист персональних даних визнається основоположним правом на рівні ЄС та у сучасних конституціях європейських держав, зокрема, Австрії, Естонії, Іспанії, Литві, Нідерландах, Польщі, Португалії, Словаччині, Словенії, Угорщині, Фінляндії, Швеції та Чехії. Втім, як слушно зазначено у п. 4 Преамбули Загального регламенту про захист даних 2016 р.: «…Право на захист персональних даних не є абсолютним правом; воно повинне розглядатися у зв'язку з його функцією в суспільстві та бути збалансованим з іншими основоположними правами згідно з принципом пропорційності» [47].

У науці підходи до визначення права на захист персональних даних варіюються від визнання його аспектом права на приватне життя (К. С. Мельник, В. М. Брижко, В. Г. Пилипчук), визнання його як права, безпосередньо пов'язаного із захистом приватності (Т. І. Обуховська, А. В. Кардаш, А. В. Пазюк) і визнання його як основоположного права на рівні з правом на приватність (М. Тцану, Б. ван дер Слот, О. Лінскі, П. М.

Сухорольський). У цьому плані підтримуємо підхід щодо визнання відокремленості та самостійності права на захист персональних даних.

Нині також сформувався підхід за якого право на захист персональних даних, незважаючи на свій тісний зв'язок з правом на приватність, належить до новітніх прав людини (Ю. С. Размєтаєва, Г. Гонзалес Фустер, Р. Геллерт). Перш за все, виникнення новітніх прав, включаючи інформаційні права людини, пов'язане з неминучими процесами суспільного та технологічного розвитку. У цьому аспекті погоджуємося із Размєтаєвою Ю. С., що права людини розвиваються з плином часу та не зафіксовані навічно у якомусь еталонному вигляді, навпаки вони продовжують розвиватися та переглядатися, так само як розвивається людство [55, с. 31]. Відповідно, зміни в цифрову епоху безпосередньо впливають, серед іншого, на набуття приватністю ознак колективного явища та більш помітному впливі цифрового сліду на приватність [56, с. 13]. Важливо усвідомлювати, що закріплення права на захист персональних даних як новітнього права сприяє реалізації також таких його аспектів як, зокрема, право бути забутим, право знати логіку прийняття автоматизованих рішень чи права щодо профайлінгу, які не захищаються в рамках інших загальновизнаних прав [57, с. 20].

Безсумнівно, право на захист персональних даних та право на приватність є взаємопов'язаними, однак мають певні розбіжності. Тому все більша кількість науковців погоджується з тим, що право на захист даних не слід розглядати як елемент права на приватність або похідне від нього право, водночас наголошуючи на відмінностях між двома правами (Дж. Кокотт, К. Соботта, Г. Фустер, О. Лінскі, М. Тцану, П. М. Сухорольський).

Однією з відмінностей є сфера застосування та сутність права на приватність та права на захист персональних даних. З одного боку, захист персональних даних стосується такого аспекту приватності як контроль над інформацією про особу. Незважаючи на те, що право на захист персональних даних завжди пов'язане з інформацією про ідентифіковану особу або особу, яку можна ідентифікувати, право на приватність не обов'язково включає її. Щоправда, приватність є більш широкою правовою концепцією, яка втілює сукупність прав та цінностей, включаючи право бути залишеним в спокої, відокремленість, персональну автономію, розвиток особистості та

інші аспекти. Звісно, право на захист персональних даних спрямоване на захист приватності, але також захищає і інші цінності, що стосуються безпеки та якості даних, недискримінації та пропорційності. Водночас як право на захист персональних даних, так і право на приватність, не є абсолютним правом, і, відповідно, воно підлягає обмеженням, які встановлені законом, переслідують законну мету, є необхідними у демократичному суспільстві, пропорційними та поважають «сутність» права на захист даних [58, с. 91]. Порівнюючи обсяг обох прав, стає зрозумілим, що сфера захисту персональних даних є ширшою, оскільки пов'язана з будь-якою інформацією про особу, завдяки якій цю особу можна ідентифікувати, а не лише з інформацією про ідентифіковану особу, яка може виступати об'єктом захисту права на приватність.

Ще одна відмінність між цими двома правами стосується обов'язків, які покладаються на сторони правовідносин: право на приватність переважно стосується негативного обов'язку державних органів не втручатися у сферу приватного життя особи та позитивного обов'язку приймати необхідне законодавство для забезпечення відносин між приватними особами, а право на захист персональних даних покладає однакові зобов'язання у сфері захисту даних як на органи державної влади, так і на приватних осіб, зокрема, роботодавців, постачальників послуг або рекламодавців [59, с. 225-226].

Також стверджується, що право на захист персональних даних на відміну від права на приватність надає особі більше контролю над різними типами даних, не залежно від того чи була особа ідентифікована, чи ні. Відтак право на захист персональних даних слід розглядати як право, яке значною мірою збігається з правом на приватність і водночас забезпечує додаткові, відмінні можливості для фізичних осіб, зокрема, право на доступ до персональних даних, право на виправлення або видалення таких даних. Втім, основною відмінністю між правом на захист персональних даних та правом на приватність є концепція інформаційного самовизначення (англ. informational self-determination). Так, право на захист персональних даних надає людині більше інформаційних прав, ніж право на приватність, наприклад, право перенесення даних та право на забуття, які сприяють інформаційному самовизначенню особи та забезпечують вищий рівень контролю над своїми персональними даними [60, с. 595-596].

Окрім того, право на захист персональних даних регулює вертикальні і горизонтальні відносини, але не залежить повністю лише від осіб, які реалізують або забезпечують виконання своїх прав, а також ґрунтується на низці обов'язків, покладених на широке коло суб'єктів, долучених до процесу обробки персональних даних. Так, наприклад, дотримання правил захисту персональних даних повинно підлягати контролю з боку незалежного органу [61, с. 47].

Як зауважують дослідники П. де Херт та С. Гатвьорс право на приватність та право на захист персональних даних є двома різними юридичними механізмами, які мають різні та взаємодоповнюючі функції. Вони виокремлюють дві основні теорії співвідношення приватності та захисту персональних даних, які зводяться до наступного: приватність спрямована на захист людей від незаконного та надмірного використання влади (принцип невтручання), а захист персональних даних спрямований на контроль законного використання влади (принцип прозорості). Основні правові положення щодо захисту персональних даних, таким чином, виходять з того, що обробка персональних даних в принципі є дозволеною і законною, а правове регулювання захисту приватності першочергово спрямоване на забезпечення невтручання держави у приватне життя, хоча право на приватність покладає й позитивні зобов'язання щодо створення правової бази для захисту приватної сфери життя [62, с. 72-74].

Інший підхід запропонований науковцем Н. Н. Г. де Андраде, який наголошує на необхідності збалансування спільних та відмінних рис у підходах до визначення права на захист персональних даних, права на приватність та права на ідентичність, які є вирішальними для досягнення всебічного та надійного захисту всіх аспектів особистості людини. Так, поняття персональних даних визначається шляхом застосування критеріїв ідентифікації інформації про особу, серед яких чільне місце займають фактори, властиві для фізичної, психологічної, психічної, економічної, культурної чи соціальної ідентичності. Таким чином, ідентичність є одним із критеріїв визначення обсягу персональних даних. Однак право на ідентичність як право на визнання та повагу з боку інших рис або граней особистості, характерних або унікальних для конкретної людини (таких як зовнішність, ім'я, зображення, голос тощо) тісно пов'язано з правом на приватність як свободою від необґрунтованих обмежень на розвиток власної

ідентичності. На відміну від права на захист персональних даних, право на приватність та право на ідентичність спрямовані на захист конкретних інтересів особистості. Інша суттєва відмінність полягає в тому, що право на приватність та право на ідентичність є матеріальними правами (англ. substantive rights), тобто спрямовані на забезпечення захисту конкретних інтересів особистості, у той час, як право на захист персональних даних є процесуальним правом (англ. procedural right), тобто встановлює правові умови та процедури через які ці матеріальні права можуть бути ефективно забезпечені [63, с. 92-98].

Визнання відокремленості права на захист персональних даних у науковій та практичній площині поступово призвело до удосконалення правового регулювання у цій сфері. Як наслідок, право на захист персональних даних було закріплено в основних правових актах у сфері захисту даних - Загальному регламенті про захист даних 2016 р. та Конвенції № 108 +, які містять керівні принципи та стандарти захисту персональних даних. Втім, незважаючи на прийняття різноманітних міжнародно-правових актів у сфері захисту персональних даних та відносне узгодження основних принципів захисту даних та засобів їх реалізації, існують суттєві відмінності в тому, як вони застосовуються на практиці, що призводить до існування конкуруючих режимів захисту даних, тобто сукупності стандартів, принципів, норм, правил та процедур прийняття рішень, пов’язаних із захистом персональних даних.

Так, на практиці сформувалися різні підходи до правового регулювання захисту персональних даних, основними з яких є секторальний або галузевий підхід, який характерний для США та передбачає створення спеціальних федеральних законів та/або законів окремих штатів, які регулюють захист персональних даних у тій чи іншій галузі (телекомунікаційному секторі, банківській сфері тощо), та комплексний підхід, який є характерним для європейського регіону та передбачає створення єдиного, всеохоплюючого закону, який регулює питання захисту персональних даних у всіх сферах суспільного життя [64]. Для американської моделі захисту даних визначальною рисою є те, що право на приватність не належить до основоположних прав людини і Конституція США прямо не захищає право на приватність, а захист приватності забезпечується завдяки судовому тлумаченню кількох основних конституційних

гарантій, що походять з Першої, Третьої, Четвертої та П'ятої поправок та гарантують, відповідно, свободу слова, друку та зборів, заборону на розміщення солдатів у будь-якому домі в мирний час без згоди власника, захист від необґрунтованого обшуку і арешту, а також вилучення майна та свободу від самовикриття [65; 66, с. 422]. На відміну від американської, європейська модель захисту персональних даних характеризується визнанням та закріпленням на конституційному рівні права на приватне життя та права на захист персональних даних. Ця відмінність пояснюється перш за все тим, що у своїх конституціях молоді європейські демократії мають змогу відображати нові реалії і запроваджувати сучасні підходи до захисту прав людини, на відміну від Конституції США 1787 р.

Водночас для американської моделі також відмінною рисою є закріплення правових норм регулювання приватності та захисту персональних даних одночасно у законодавчих актах федерального рівня та законодавстві штатів. Так, існує понад 20 федеральних галузевих законів, що забезпечують захист приватності у різних галузях, однак вагому роль у регулюванні приватності відіграють закони штатів – наприклад, Каліфорнійський закон про захист прав споживачів (California Consumer Privacy Act або CCPA) - які у більшості випадків мають перевагу над федеральними законами. Також положення щодо приватності безпосередньо закріплені у конституціях десяти штатів: Аляски, Аризони, Каліфорнії, Флориди, Гаваїв, Іллінойсу, Лос Анджелесу, Монтани, Південної Кароліни та Вашингтону. Втім, неабиякий вплив на практику захисту приватності та персональних даних мають рішення Верховного Суду, який здійснює тлумачення правових норм або визнає їх недійсними [67, с. 5].

Таким чином, порівнюючи у практичній площині дві основні моделі захисту – європейську та американську – можна виокремити такі їхні основні риси:

1) для *європейської моделі* характерна наявність загального акту у сфері регулювання захисту персональних даних, а для *американської моделі* - наявність низки актів для різних галузей;

2) для *європейської моделі* характерне визнання та закріплення права на приватне життя та захист персональних даних на конституційному рівні, а для *американської*

моделі - визнання і тлумачення права на приватність, включаючи різні його аспекти, у судових прецедентах;

3) для *європейської моделі* характерна наявність єдиного контролюючого органу із захисту даних (Data Protection Authority), а для *американської моделі* - відсутність єдиного контролюючого органу та покладення функції з контролю на низку органів відповідних галузях, зокрема, Федеральна торгова комісія (FTC), яка має юрисдикцію щодо більшості комерційних організацій та вживає заходи для захисту споживачів від нечесної або оманливої практики у сфері торгівлі, включаючи захист приватності та персональних даних. Водночас низка органів, серед іншого, Федеральна комісія зв'язку (FCC), Комісія з цінних паперів та бірж (SEC), Міністерство охорони здоров'я та соціальних служб (HHS) та Бюро фінансового захисту споживачів (CFPB), мають повноваження із захисту даних згідно з секторальними законами. Крім того, на рівні штатів існують власні органи як, наприклад, Генеральний прокурор Каліфорнії, який має повноваження забезпечувати виконання Каліфорнійського закону про захист прав споживачів та більшості законів про приватність у Каліфорнії.

Щоправда, поділ на європейську та американську моделі не є виключним і у науці існують також й інші класифікації. Зокрема, вітчизняний науковець В. О. Серьогін, вивчаючи особливості захисту інформаційного прайвесі (інформаційної приватності, що регулює питання захисту персональних даних), виокремлює два підходи - універсальний, прийнятий у багатьох державах та наддержавних утвореннях, таких як ЄС, а також характерний для США - секторальний (галузевий) підхід. Водночас у межах секторального підходу науковцем пропонується поділ федеральних законів США у сфері захисту приватності (прайвесі) на окремі категорії: 1) прайвесі у фінансовій сфері (наприклад, Закон про чесну кредитну звітність 1970 р. щодо забезпечення приватності компаніями, які надають кредитні звіти); 2) прайвесі у сфері освіти (наприклад, Закон про сімейні освітні права та приватність 1974 р., який регулює захист освітніх записів, доступ до навчальних реєстрів та персональних даних студентів); 3) прайвесі у сфері охорони здоров'я (наприклад, Закон про мобільність і підзвітність медичного страхування 1996 р., який регулює приватність медичних записів); 4) прайвесі дітей (наприклад, Закон про захист приватності дітей в Інтернеті 1998 р., який регулює

використання персональних даних дітей в Інтернеті); 5) прайвесі споживачів (наприклад, Закон про політику в галузі кабельного зв'язку 1984 р. та Закон про захист приватності відео 1988 р., які встановлюють правила збирання та використання персональних даних операторами кабельного зв'язку та постачальниками відеопослуг) [68, с. 58-60].

Д. Банісар та С. Девіс, досліджуючи світові тенденції у сфері захисту даних, запропонували поділ на основні моделі захисту персональних даних у яких захист даних здійснюється за допомогою: комплексних законів, секторальних законів, спільного регулювання та саморегулювання. Так, більшість країн світу запроваджують комплексні закони, які регулюють питання збирання, використання та поширення персональних даних приватним та публічним сектором. Зазвичай у країнах, що запроваджують комплексні закони, існує наглядовий орган, який контролює виконання цих законів. Втім, для Канади та Австралії характерним є впровадження різновиду цих законів, який описується як модель спільного регулювання – галузі промисловості розробляють стандарти, які гарантують захист приватного життя, забезпечуються відповідною галуззю та контролюються агентством з питань захисту приватності. Водночас для галузевих законів є характерним регулювання захисту персональних даних через низку законодавчих актів та відсутність єдиного регуляторного органу. Незважаючи на різноманіття галузей регулювання, основним недоліком галузевого підходу є те, що він вимагає розробку нових законодавчих актів із впровадженням кожної нової технології у суспільне життя. У багатьох країнах галузеві закони використовуються як доповнення законодавства у сфері захисту даних, забезпечуючи більш детальний захист певних категорій інформації, таких як захист телекомунікації, поліцейських справ або записів споживчих кредитів. Як зазначають Д. Банісар та С. Девіс, принаймні теоретично захист персональних даних також можна здійснювати й за допомогою різних форм саморегулювання, за яких компанії та галузеві органи розробляють відповідні кодекси поведінки (кодекси практик). Розробка таких кодексів поведінки щодо захисту персональних даних є характерною для США, Японії та Сінгапуру. Втім, галузеві кодекси в багатьох країнах, як правило, забезпечують низький рівень захисту і не є широко впровадженими [9, с. 13-14].

Вивчаючи основні моделі захисту інформації про особу, В. М. Брижко, А. І. Радянська та М. Я. Швець, поряд із галузевим та комплексним підходами виокремлюють також змішаний підхід, який полягає у створенні базового (рамкового, системоутворюючого) закону про захист даних і розробку на його основі галузевих нормативно-правових актів. За таких умов, як стверджують дослідники, система захисту персональних даних залишатиметься незмінною при виникненні нових загроз і нових видів порушень, оскільки доповнення та зміни будуть вноситися до галузевого законодавства [69, с. 19]. Таку класифікацію пропонує і дослідниця А. В. Кардаш, стверджуючи, що для змішаного підходу характерним є існування одночасно загального закону у сфері захисту персональних даних та окреме, детальне регулювання у галузевих актах. Саме змішаний підхід, на думку дослідниці, є найбільш всеохопним та оптимальним у сфері захисту персональних даних [70, с. 118-119].

Водночас А. В. Пазюк пропонує поділ підходів щодо захисту персональних даних на: 1) ліберальний (ринковий), який покладений в основу законодавства у сфері захисту персональних даних у США; 2) соціально-захисний (загальноєвропейський) підхід, який засновується на повазі до прав людини; 3) змішаний підхід. Особливістю соціально-захисного підходу є наявність єдиного законодавчого акту, спеціального наглядового органу з захисту персональних даних та поширення правових норм щодо захисту персональних даних як у публічній, так і у приватній сферах. Для ліберального підходу принциповими рисами є відсутність загального закону у сфері захисту персональних даних, дотримання концепції невтручання держави у приватноправові відносини, а також наявність низки органів, які здійснюють загальний нагляд за дотриманням умов ліцензій у відповідних секторах. Водночас так званий змішаний підхід виник внаслідок широкого поширення соціально-захисного підходу у країнах, які традиційно вважаються ліберально-ринковими (Канада, Австралія) [41, с. 133-138].

Не можна залишити поза увагою й особливості регулювання захисту персональних даних у країнах Латинської Америки. Так, наприклад, у Бразилії, Парагваї, Перу, Аргентині, Еквадорі, Колумбії, модель захисту приватності та персональних даних включає також як самостійний елемент Habeas data (від лат. «мати дані»). Конституційне право особи на Habeas data від початку було притаманне лише публічним

організаціям і було своєрідною відповіддю диктаторським часам у Бразилії та по всій Латинській Америці, коли інформація про громадян зберігалася урядом у таємниці і використовувалася для придушення повстань населення. Нині Habeas data може використовуватися також для отримання інформації про персональні дані, які зберігаються чи обробляються приватними структурами, доки такі бази даних мають суспільний інтерес. Habeas data можна характеризувати як процесуальне конституційне право особи, що надає їй право подати індивідуальну скаргу до конституційного суду з метою отримання доступу, оновлення, виправлення, заперечення проти обробки даних або видалення чутливих персональних даних щодо особи, які можуть призвести до порушення права на приватність. Загалом Habeas data відповідають європейським стандартам захисту даних щодо прозорості, виправлення, оновлення, точності та цільового призначення, однак не всі варіації Habeas data, які закріплені у національних конституціях країн Латинської Америки, містять положення про забезпечення безпеки даних, і водночас жодна з них не обмежує передачу даних в інші країни. Відтак Habeas data без запровадження додаткових гарантій захисту персональних даних не може вважатися механізмом, який забезпечує належний рівень захисту даних [71, с. 5].

У порівнянні із персональними даними Habeas data є у вужчим поняттям, що розглядається як право особи на доступ до персональної інформації у режимі персональних даних. Проте Habeas data не вимагають від операторів даних забезпечення захисту персональних даних, що обробляються ними, а перш за все спрямовується на захист зображення особи, недоторканності приватного життя, честі, самовизначення та свободи інформації [72].

Вочевидь існування конкуруючих режимів захисту персональних даних в умовах відсутності універсального міжнародного договору у цій сфері має низку негативних наслідків, які зумовлені як різницею у трактуванні приватності, так і відмінностями у культурному сприйнятті захисту персональних даних. Такий стан речей мав наслідком низку торговельних конфліктів та суперечностей, які виникали, зокрема, при трансатлантичній передачі даних між США та ЄС.

Узагальнену думку з цього приводу у 1999 р. висловила Робоча група з питань захисту осіб при обробці персональних даних (більш відома як Article 29 Working Party),

яка була утворена згідно зі ст. 29 Директиви 95/46/ЄС як консультативний орган, зазначивши у своєму Висновку щодо рівня захисту даних у США: *«Приватність та захист даних у Сполучених Штатах є складною структурою, що включає галузеве регулювання як на федеральному рівні, так і на рівні штатів, у поєднанні з галузевим саморегулюванням […] Проте Робоча група вважає, що нинішнє розмаїття вузькоорієнтованих галузевих законів та добровільне саморегулювання у жодному разі не забезпечують належний захист персональних даних, переданих з Європейського Союзу»* [73].

Як наслідок, у 2000 р. Міністерство торгівлі США та Комісія Європейського Союзу уклали Угоду про безпечну гавань (Safe Harbor Agreement), яка включала ряд принципів щодо захисту персональних даних, які підприємства США можуть взяти на себе добровільно для участі у транскордонних передачах даних, а саме принципи щодо повідомлення осіб про збір даних, можливості передачі даних третім особам, вимог до захисту даних у разі їх подальшої передачі, вимог до захисту даних, забезпечення цілісності даних, доступу до даних та відповідальність за порушення вказаних принципів. Укладення цієї угоди мало на меті подолати розбіжності у режимах захисту персональних даних у ЄС та США, впорядкувати засоби для дотримання американськими організаціями Директиви 95/46/ЄС та захистити організації ЄС, що передають персональні дані організаціям США. Водночас принципи «безпечної гавані» згідно з цією Угодою могли бути обмежені в межах, необхідних для забезпечення інтересів національної безпеки, публічного інтересу чи інтересів правоохоронних органів. Втім, зроблені у 2013 р. Е. Сноуденом заяви щодо нагляду та збирання персональних даних Агентством національної безпеки США загострили занепокоєння щодо стандартів приватності та захисту даних у США. Як наслідок, низка угод між США та ЄС щодо обміну даними як у комерційному, так і в правоохоронному секторах потрапила під пильний контроль у Європі, а уже 6 жовтня 2015 р. розглядаючи справу *Maximillian Schrems v. Data Protection Commissioner* (далі – справа *Schrems*) Суд ЄС визнав недійсним рішення Європейської Комісії щодо затвердження Угоди про безпечну гавань між ЄС та США, зазначивши, серед іншого, що схема «безпечної гавані» застосовувалася виключно до підприємств США, які вирішили її дотримуватися

на добровільній основі, в той час, як органи державної влади США не підпадали під її дію. Крім того, виключення щодо забезпечення інтересів національної безпеки, публічних інтересів та інтересів правоохоронних органів мали перевагу над принципами «безпечної гавані», а відтак підприємства США зобов'язані були не обмежуючись ігнорувати правила щодо захисту даних, встановлених цими принципами, у разі якщо вони суперечили переліченим вище інтересам. Водночас угода не містила жодних висновків щодо існування у США норм, спрямованих на обмеження будь-якого втручання в основні права осіб, дані яких передаються з ЄС до США, втручання в які здійснюються державними структурами для переслідування законних цілей, таких як національна безпека, а також не розглядалася наявність ефективного правового захисту від такого втручання [74].

Задля врегулювання непорозумінь, що виникли у зв'язку з рішенням Суду ЄС у справі М. Шремса, у лютому 2016 р. було узгоджено положення оновленого правового режиму обміну приватними даними між США та ЄС, так званого EU-U.S. Privacy Shield або Щиту конфіденційності між ЄС та США, у якому було закріплено сім основних принципів: повідомлення про цілі обробки, повідомлення про вибір щодо подальшої обробки та передачі даних, відповідальність за подальшу передачу даних, безпека, цілісність даних та їх цільове обмеження, доступ до даних, а також звернення за захистом, забезпечення виконання та відповідальність за порушення принципів захисту даних. Щит конфіденційності між ЄС та США також регламентував додатковий набір принципів, що стосувалися обробки категорій чутливих даних, даних про людські ресурси, фармацевтичні і медичні продукти та загальнодоступних даних, а також деталізував норми щодо відповідальності за подальшу обробку персональних даних та ролі органів із захисту даних [75, с. 9-10]. Однак 16 липня 2020 р. Суд ЄС у справі *Data Protection Commissioner v. Facebook Ireland Ltd, Maximillian Schrems (Schrems II)* (далі – справа *Schrems II*), визнав недійсним рішення Європейської Комісії, яким було затверджено правовий режим Щиту конфіденційності між ЄС та США, вказавши серед іншого, що законодавство США не передбачає істотно рівноцінного (англ. essentially equivalent), а отже, достатнього рівня захисту даних, гарантованого на рівні ЄС. Водночас Суд ЄС наголосив на інвазивному характері програм спостереження для цілей

зовнішньої розвідки у США, які є непропорційними, оскільки недостатньо обмежують надані органам влади повноваження, а також не мають відповідних положень про мінімальні гарантії захисту [76]. Зауважимо, що 7 жовтня 2022 року президент США Дж. Байден підписав Виконавчий наказ про посилення заходів безпеки для розвідувальної діяльності США, у якому описано кроки, яких необхідно вжити для виконання зобов'язань Сполучених Штатів згідно з Рамковою угодою щодо конфіденційності даних між ЄС і США (далі – Рамкова угода). Рамкова угода призначена для забезпечення відповідного рівня захисту трансатлантичних потоків даних з ЄС після знакового рішення Суду ЄС у справі *Schrems II* [77].

Нині у відносинах з третіми країнами у рамках ЄС відповідно до Загального регламенту про захист даних 2016 р. використовуються й такі інструменти передачі даних як рішення про адекватність захисту даних, механізм сертифікації, кодекси практик, Стандартні договірні положення (Standard Contractual Clauses (SCC)), які використовують для обміну даними між ЄС та іншими країнами, та Обов'язкові корпоративні правила (Binding Corporate Rules (BCR)), за допомогою яких врегульовано передачу персональних даних у рамках діяльності транснаціональних компаній, а також як виключення використовуються відступи (дерогації) для конкретних ситуацій, регламентовані ст. 49 Загального регламенту про захист даних 2016 р. [78].

Відтак захист даних на міжнародному рівні залишається фрагментарним та слабким, що створює ризики для приватних осіб та проблеми для міжнародних організацій (таких як суб'єкти ООН та міжнародні гуманітарні організації), багато з яких обробляють значні обсяги персональних даних. Водночас міжнародне публічне право розглядає статус захисту персональних даних з незмінною невизначеністю, враховуючи, що: 1) міжнародні договори про права людини забезпечують захист приватного життя в широкому сенсі і не визначають особливостей права на захист персональних даних; 2) інші міжнародні документи, що стосуються захисту персональних даних, є або регіональними, або рекомендаційними; 3) існує відсутність міжнародного консенсусу щодо сфери приватності та захисту персональних даних, зумовлена, серед іншого культурним і правовим сприйняттям приватності; 4) існує суттєва фрагментація норм щодо захисту персональних даних у національних та регіональних правових системах.

Стверджується, що майбутніх зрушень у галузі захисту персональних даних у міжнародному праві можна досягти шляхом розробки єдиного універсального міжнародного договору або використання досвіду ЮНСІТРАЛ для вирішення питань захисту персональних даних шляхом прийняття міжнародного типового закону про захист даних, який забезпечить прогресивне узгодження та уніфікацію норм у цій сфері [79]. Водночас серед науковців висловлюються також думки, що саме прийнята в рамках РЄ Конвенція № 108 повинна бути прийнята ООН як глобальний договір, враховуючи, що до неї вже приєдналися країни, які не є членами РЄ, і тому вона має потенціал для набуття статусу універсального міжнародного договору про захист персональних даних [80; 81]. Вважаємо, що положення Конвенції № 108+ нині найбільш повно відображають сучасні реалії розвитку та найбільш прогресивні підходи у сфері захисту персональних даних, а відтак поділяємо думку науковців, які підтримують прийняття цього міжнародно-правового договору як універсального міжнародного договору у цій сфері.

Таким чином, відмінність у культурному та правовому сприйнятті права на приватність та права на захист персональних даних, а також різноманіття підходів щодо захисту персональних даних, породжують низку непорозумінь та неузгодженостей у правовому регулюванні у цій сфері. Навіть із прийняттям основних правових та інших рекомендаційних актів, порушення приватності та захисту персональних даних залишається актуальною проблемою перш за все через різні підходи до визначення права на захист персональних даних, яке розглядається і як основоположне, самостійне право людини, і як аспект права на приватність. Водночас сприяє фрагментації захисту персональних даних також існування конкуруючих режимів захисту даних: у деяких країнах закони не відповідають сучасним реаліям та існуючим механізмам захисту персональних даних, в той час, як в інших існують суттєві винятки із законів про захист персональних даних для правоохоронних та розвідувальних органів, що також створює загрози для забезпечення адекватного рівня захисту персональних даних. Досвід ЄС та США щодо врегулювання можливості транскордонної передачі даних ілюструє ризики та недоліки з якими стикаються країни за відсутності єдиного міжнародно-правового акту універсального значення у сфері захисту персональних даних. Врешті решт, без належного нагляду та імплементації основних принципів захисту даних на практиці,

саме існування правових актів може не забезпечити особам належного захисту їх права на захист персональних даних. Відтак для гарантування та забезпечення подальшого розвитку права на захист персональних даних виключно важливим є прийняття універсального міжнародного договору у цій сфері, що забезпечив би єдність наявних підходів до захисту даних.

1.3 Понятійно-категоріальний апарат у світлі європейських стандартів у цій сфері

Визначальним у процесі визначення підходів щодо правового регулювання та формування принципів захисту персональних даних є понятійно-категоріальний апарат. Зважаючи на те, що сфера захисту персональних даних невпинно розвивається, так само інтенсивно формується відповідна термінологія, поняття та категорії. Провідне місце в міжнародному механізмі правового регулювання захисту персональних даних займають стандарти захисту персональних даних, що розглядаються як «найбільш узагальнені, загальновизнані на міжнародному рівні, фундаментальні правові засади у сфері відносин, безпосередньо пов'язаних із персональними даними» [82].

Як відзначає Г. Грінліф, можна стверджувати про існування двох поколінь стандартів захисту персональних даних, які характеризуються різним рівнем захисту. До першого покоління відносяться Керівні принципи ОЕСР, як перший міжнародний документ рекомендаційного характеру, який став передумовою закріплення стандартів захисту персональних даних, та Конвенція № 108 у її редакції 1981 р. Водночас провідну роль у забезпеченні формування стандартів захисту персональних даних відіграла Директива 95/46/ЄС, адже після її прийняття у 2001 р. було оновлено й Конвенцію № 108 з метою її увідповіднення найбільш важливим положенням Директиви 95/46/ЄС, серед іншого, щодо створення наглядового органу. Вважається, що з цього моменту європейські стандарти захисту персональних даних, завдяки їх широкому впровадженню державами та наданню вищого рівня захисту, набули ролі універсальних стандартів і завершили формування другого покоління стандартів захисту персональних даних [80]. Погоджуємося із зазначеною класифікацією, але вважаємо за необхідне її доповнення третім поколінням, що нині закріплені у Загальному регламенті про захист

даних та оновленій Конвенції № 108+ зі змінами, внесеними Протоколом CETS № 223, які визначають провідні європейські стандарти захисту персональних даних.

Таким чином, за відсутності універсального міжнародного договору, основні стандарти захисту персональних сформувалися в рамках діяльності РЄ та ЄС, а згодом поступово були прийняті глобально. Відтак у науці та практиці дедалі частіше використовується саме термін «європейські стандарти захисту персональних даних», оскільки спостерігається тенденція наближення світових стандартів захисту даних до стандартів, закріплених у Конвенції № 108+ та Загальному регламенті про захист даних.

Вочевидь основою правового регулювання захисту персональних даних є термін «персональні дані», який відносно однаково визначений у Керівних принципах ОЕСР, Конвенції № 108 та її оновленій версії, Директиві 95/46/ЄС та Загальному регламенті про захист даних, а саме як будь-яка інформація про ідентифіковану особу або особу, яку можна ідентифікувати прямо чи опосередковано. Визначення персональних даних як у праві РЄ, так і у праві ЄС, є достатньо широким, щоб охопити всі можливі варіанти ідентифікації. Як зазначають науковці М. В. Бем та І. М. Городиський, визначальним у згаданому визначенні є поняття «ідентифікована особа», тобто особа, яку можна безпомилково виокремити з-поміж інших осіб завдяки наявній у розпорядженні інформації про неї. Зазвичай особу можна вважати ідентифікованою використовуючи її ім’я, прізвище, по батькові та реквізити документа, який посвідчує особу або цифровий номер, що присвоюється особі, зокрема, ідентифікаційний номер фізичної особи. Водночас Загальний регламент про захист даних надає найбільш вичерпне визначення «особи, яку можна ідентифікувати», зазначаючи, що таку особу можна ідентифікувати прямо чи опосередковано, зокрема завдяки таким ідентифікаторам, як ім’я, ідентифікаційний номер, дані щодо місцеперебування, онлайн ідентифікатор чи інші особливості фізичної, фізіологічної, генетичної, духовної, економічної, культурної чи соціальної ідентичності такої фізичної особи [83, с. 10-11]. Відтак ідентифікувати особу можна за однією ознакою (прізвище або, наприклад, псевдонім у відомих людей, адреса проживання), але зазвичай ідентифікація пересічної особи відбувається одночасно за декількома ознаками, сукупність яких є достатньою для точної ідентифікації конкретної особи.

Загалом вважається, що інформація містить персональні дані про особу у разі якщо особа є ідентифікованою або може бути ідентифікованою завдяки такій інформації, або якщо особа, яка хоч і не є ідентифікованою, однак може бути виділена завдяки цій інформації тією мірою, що використовуючи додаткову інформацію є можливість достовірно встановити хто є цією особою. Обидва види інформації захищені в однаковий спосіб відповідно до європейських стандартів захисту персональних даних. Таким чином, ідентифікація потребує елементів, які описують особу у спосіб, що дозволяє відрізнити її від всіх інших осіб та впізнати як індивіда. Водночас питання щодо прямої чи опосередкованої можливості ідентифікації особи потребує оцінки з огляду на впровадження нових технологій та постійний технологічний розвиток, а тому для визначення ймовірності ідентифікації особи необхідно враховувати всі об'єктивні фактори, наприклад, витрати та період часу, необхідний для ідентифікації, технології, наявні станом на момент обробки, технологічні розробки тощо. Втім, особа не буде вважатися «ідентифікованою», якщо її ідентифікація потребує необґрунтовано тривалого часу, зусиль чи ресурсів, наприклад, надмірно складних, тривалих та коштовних операцій [84, с. 99-102; 34, с. 3].

У науці виділяють два типи ідентифікації особи - об'єктивно можлива ідентифікація, яка передбачає використання виключно уже наявної інформації, та суб'єктивно можлива ідентифікація, яка передбачає додатковий аналіз та пошук іншої інформації, одержання якої потребує «розумних зусиль» чи доступ до якої може отримати особа, відповідальна за обробку даних [85, с. 46]. У будь-якому разі саме ознака ідентифікації особи є ключовою для визначення питання застосування положень про захист персональних даних щодо певної інформації.

Примітно, що Конвенція № 108 (ст. 6), Директива 95/46/ЄС (ст. 8) та Загальний регламент про захист даних (ст. 9) виділяють як особливу категорію так звані чутливі персональні дані, обробка яких дозволяється лише у чітко визначеному порядку, до таких даних відносяться, зокрема, дані про расове або етнічне походження; політичні, релігійні чи світоглядні переконання; членство у політичних партіях чи професійних спілках; про засудження до кримінального покарання; дані про здоров'я чи статеве життя, а також біометричні та генетичні дані [40; 42; 47].

Досліджуючи європейські стандарти захисту персональних даних необхідно також визначити основні поняття та терміни, зокрема ті, що позначають учасників правовідносин, пов'язаних із захистом персональних даних, а саме суб'єкта даних, контролера (володільця), оператора (розпорядника) та одержувача даних. Окрім того, необхідно проаналізувати терміни, безпосередньо пов'язані з обробкою даних, такі як автоматизована обробка, база даних, згода суб'єкта даних, транскордонна передача, а також основні принципи обробки персональних даних.

Ключовим учасником правовідносин у сфері захисту персональних даних безсумнівно є саме суб'єкт даних. Основні правові акти, що закріплюють європейські стандарти захисту персональних даних надають визначення суб'єкта даних опосередковано, крізь термін «персональні дані» як особу, персональні дані якої обробляються. Щоправда, якщо Керівні принципи ОЕСР, Директива 95/46/ЄС і Загальний регламент про захист даних як суб'єкта даних розглядають виключно фізичну особу, то Конвенція № 108 від початку визначала суб'єкта персональних даних як особу, без уточнення фізична чи юридична особа, і не виключала застосовування її положень у визначених у пункті (б) ч. 2 ст. 3 випадках до інформації «яка стосується груп осіб, асоціацій, фондів, компаній, корпорацій та будь-яких інших організацій, що безпосередньо чи опосередковано складаються з окремих осіб, незалежно від того, мають чи не мають такі установи статус юридичної особи» [40]. Вочевидь норми Конвенції № 108 надають дискрецію національним органам у визначенні питання поширення правового регулювання захисту персональних даних на організації, включаючи юридичних осіб. Однак оновлена Конвенція № 108+ надає визначення суб'єкта даних однозначно наголошуючи, що ним може бути лише фізична особа. Водночас Конвенція № 108+ наділяє держави правом надати суб'єктам даних ширший захист, ніж передбачений Конвенцією № 108+, і поширити положення національного законодавства на дані, що стосуються юридичних осіб, з метою захисту їх законних інтересів [49; 50, с. 6].

Наголосимо, що положення європейських стандартів захисту персональних даних поширюються тільки на живих осіб [86, с. 22]. Однак положення оновленої Конвенції № 108+ (ст. 13), як і Загальний регламент про захист даних (п. 27 Преамбули) наділяють

держави повноваженнями розширювати межі захисту персональних даних, в тому числі на померлих осіб. В цілому питання захисту персональних даних померлих осіб є доволі дискусійним у науці. У цьому плані дослідниця Ю. Д. Бєлова, яка виділяє два підходи щодо захисту персональних даних померлих осіб – негативний підхід, за якого законодавство про захист персональних даних не поширюється на відомості про померлу особу, та позитивний підхід, який допускає поширення дії законодавства у сфері захисту персональних даних на відомості про померлих осіб [85, с. 61-62]. Вважаємо, що саме другий підхід є найбільш прогресивним і відповідає сучасним реаліям, однак він вимагає деталізації положень національного законодавства щодо захисту персональних даних померлої особи, зокрема, в частині наділення суб'єкта даних за життя можливістю висловити волевиявлення щодо обробки його даних після смерті, можливості отримання чи відкликання згоди на обробку даних померлої особи з боку членів сім'ї або близьких родичів, а також наділення останніх правами суб'єкта даних (померлої особи).

Окрім суб'єкта даних безпосередніми учасниками відносин у сфері захисту персональних даних також виступають контролер та оператор даних. Так, контролером даних є фізична чи юридична особа, державний орган, установу чи будь-який інший орган, який самостійно або разом з іншими уповноважений приймати рішення щодо цілі та процедури обробки персональних даних. Водночас фізичні особи, які здійснюють обробку персональних даних під час діяльності суто особистого чи побутового характеру, не вважаються контролерами відповідно до положень Директиви 95/46/ЄС (ст. 3), Конвенції № 108+ (ст. 3) та Загального регламенту про захист даних (ст. 2). Оператором даних може бути фізична чи юридична особа, державний орган, установа чи будь-який інший орган, який обробляє персональні дані від імені контролера [42; 47; 49]. Головною характеристикою оператора даних є те, що він самостійно не встановлює мету обробки персональних даних, а лише здійснює їх обробку від імені контролера.

Окрім того, учасником правовідносин у сфері захисту даних виступає також одержувач даних, яким є будь-яка фізична чи юридична особа, державний орган, установа чи будь-який інший орган, якому персональні дані були розкриті чи стали доступні [42; 47; 49]. Водночас Директива 95/46/ЄС (ст. 2) та Загальний регламент про

захист даних (ст. 4) також надають визначення такого учасника як третя особа, якою є будь-яка особа, яка не є суб'єктом даних, контролером, оператором, а також особою, яка під безпосереднім підпорядкуванням контролера чи оператора, уповноважена обробляти дані. Різниця між категоріями одержувача даних та третьої особи стосується здебільшого їхнього зв'язку з контролером і, як наслідок, їхнього права на доступ до персональних даних, які є в контролера. Втім, поняття «одержувач даних» є ширшим, оскільки ним може виступати будь-яка особа, незалежно від того, чи є вона третьою стороною. Відмінність між одержувачами і третіми особами має принципове значення лише у зв'язку з умовами законного оприлюднення персональних даних. Зокрема, співробітники контролера чи оператора даних можуть без будь-яких законних вимог бути одержувачами персональних даних, якщо беруть участь у їхніх операціях з обробки. Водночас третя особа, яка є юридично самостійною від контролера чи оператора, не має права використовувати оброблені контролером персональні дані, за винятком, коли є особливі юридичні підстави, виправдані у конкретній ситуації [84, с. 121-123].

Що стосується безпосередньо використання персональних даних, то визначальну роль має термін «обробка персональних даних» під якою розуміють будь-які операції з персональними даними з використанням автоматизованих засобів чи без них. Щоправда, з розвитком технологій значно збільшилась кількість операцій, пов'язаних з персональними даними, які можуть становити обробку даних. Відповідно, у міжнародно-правових актах, які закріплюють європейські стандарти захисту персональних даних, обсяг визначення терміну обробка даних постійно розширювався, незважаючи на свій невичерпний характер. Розглянувши визначення «обробка даних», які закріплені у Конвенції № 108, Директиві 95/46/ЄС та Загальному регламенті про захист даних, можна надати таке найбільш повне визначення обробки персональних даних – це будь-яка операція або низка операцій з персональними даними з використанням автоматизованих засобів або без них, включаючи, але не обмежуючись, такі операції як збирання, реєстрація, організація, структурування, зберігання, адаптація чи зміна, пошук, ознайомлення, упорядкування чи комбінування, використання, розкриття через передавання, розповсюдження чи надання іншим чином, стирання або

знищення, а також виконання логічних та/або арифметичних дій. Примітно, що Конвенція № 108+ також надає автономне визначення обробки даних без використання автоматизованих засобів, зазначаючи, що така обробка означає операцію чи набір операцій, що виконуються над персональними даними у межах структурованого набору таких даних, які є доступними чи можуть бути виокремлені за певними критеріями [49]. Водночас Загальний регламент про захист даних також надає окреме визначення терміну «профайлінг», який є однією з форм автоматизованої обробки персональних даних, тобто використання персональних даних для оцінювання окремих персональних аспектів, що стосуються фізичної особи, зокрема, для аналізу або прогнозування аспектів, що стосуються продуктивності суб'єкта даних на роботі, економічної ситуації, здоров'я, особистих переваг, інтересів, надійності, поведінки, місцезнаходження або пересування [47]. Необхідно також відмежовувати поняття «захист персональних даних», який з урахуванням усталеної європейської практики, не є елементом обробки, адже не передбачає вчинення окремих дій з персональними даними, а є окремим від обробки комплексом дій [82].

Зауважимо, що важливе практичне значення для захисту персональних даних має також терміни «псевдонімізація» та «знеособлення» (або «анонімізація») персональних даних, які використовуються задля захисту персональних даних та унеможливлення безпосередньої ідентифікації суб'єкта даних. Псевдонімізацією є зміна персональних даних таким чином, щоб вони не могли бути віднесені до конкретного суб'єкта без використання додаткової інформації, яку зберігають окремо [47]. Водночас знеособлення персональних даних полягає у вилученні відомостей, які дають змогу прямо чи опосередковано ідентифікувати особу. Цей спосіб не обов'язково передбачає повне видалення даних, за допомогою яких можна ідентифікувати суб'єкта, хоча і така операція охоплюється терміном знеособлення, оскільки законодавство у сфері захисту персональних даних не застосовуються до цілком анонімних даних, що викладені у спосіб за допомогою якого не можливо ідентифікувати суб'єкта даних [83, с. 14; 84, с. 105-106]. Згадані терміни юридично закріплені лише в Загальному регламенті про захист даних, а також розтлумачені у пояснювальній записці до Конвенції № 108+, але ці

техніки захисту даних широко використовується на практиці контролерами та операторами задля забезпечення адвекватного рівня безпеки даних.

Обробка персональних даних ґрунтується на сукупності принципів, які визначають правові засади її здійснення. Оскільки найбільш повно принципи викладені у європейських стандартах захисту персональних даних, пропонуємо дослідити принципи обробки персональних даних з огляду на їх поступове закріплення та здійснити більш ґрунтовний аналіз саме принципів, закріплених у третьому поколінні європейських стандартів, а саме у Конвенції № 108+ та Загальному регламенті про захист персональних даних.

Першим міжнародно-правовим актом, який містив перелік основних принципів захисту персональних даних, були Керівні принципи ОЕСР, які закріпили низку основних принципів обробки даних, до яких належать: 1) принцип обмеження збору даних, згідно з яким дані збираються законними методами та з відома або за згодою суб'єкта даних; 2) принцип якості даних, тобто відповідності персональних даних цілі для якої вони збираються, а також їх точність, повнота та оновлення; 3) принцип цільового використання, передбачає, що цілі для яких збираються дані повинні бути повідомленні на момент збору даних; 4) принцип обмеження у використанні, згідно з яким персональні дані повинні використовуватися лише для цілей, для яких вони зібрані; 5) принцип гарантії безпеки даних, що передбачає захист від ризків втрати чи несанкціонованого доступу, знищення, використання, зміни або розголошення даних; 6) принцип відкритості, що передбачає можливість встановлення характеру персональних даних, що обробляються, основних цілей їх використання, а також особи та місцезнаходження контролера даних; 7) принцип індивідуальної участі, що гарантує права суб'єктів даних; 8) принцип відповідальності контролера щодо дотримання заходів захисту персональних даних [87]. Втім, Керівні принципи ОЕСР мають рекомендаційний характер, а відтак вони не були здатні забезпечити уніфікацію норм щодо захисту даних на міжнародному рівні, оскільки вони є мінімальними стандартами, що відображають найбільш загальні правила, застосовні у цій сфері.

Подальшого розвитку та деталізації принципи обробки персональних даних набули при прийнятті Конвенції № 108 (ст. 5) та Директиві 95/46/ЄС (ст. 6), які закріпили

принцип чесності та законності, принцип цільового обмеження, принцип адекватності, відповідності та достовірності даних, принцип точності даних, принцип обмеження зберігання. Примітно, що у ст. 7 Директиви 95/46/ЄС були деталізовані критерії законності обробки, а саме, що: 1) обробка даних допускається тільки за умови, що суб'єкт даних недвозначно надав свою згоду, 2) обробка необхідна для виконання контракту, стороною якого є суб'єкт даних чи для вжиття заходів на прохання суб'єкта даних до підписання контракту, 3) обробка необхідна для дотримання правового зобов'язання контролера, 4) обробка необхідна для захисту життєво важливих інтересів суб'єкта даних, 5) обробка необхідна для виконання завдання, метою якого є задоволення суспільних інтересів, чи для виконання офіційних повноважень, якими наділений контролер чи третя сторона, якій передаються персональні дані, 6) обробка необхідна в цілях законних інтересів, що переслідуються контролером чи третьою стороною або сторонами, яким надаються дані [42]. Водночас у ст. 9 Конвенції № 108 закріплені випадки, за яких дозволяється відступ від основних принципів щодо обробки даних, коли це необхідно задля захисту державної та громадської безпеки, фінансових інтересів держави чи боротьба з кримінальними правопорушеннями, а також захисту суб'єкта даних або прав інших осіб [40]. Окрім зазначених випадків Директива 95/46/ЄС у ст. 13 також закріплює можливість відступу від основних принципів обробки даних з метою захисту національної безпеки, оборони, суспільної безпеки, запобігання, розслідування, виявлення і судове переслідування кримінальних злочинів чи порушень етики визначених професій, захисту важливого економічного чи фінансового інтересу держави-члена ЄС, включаючи монетарні, бюджетні і податкові питання, а також моніторинг, перевірку чи регулятивну функцію, пов'язану з виконанням офіційних повноважень.

Варто зазначити, що у Конвенції № 108 та Директиві 95/46/ЄС також були детально регламентовані права суб'єкта даних, зокрема: 1) право встановити факт обробки персональних даних, основні цілі обробки, категорії даних, а також особу, місце проживання або основне місце роботи контролера файлу; 2) право отримати інформацію про обробку, зберігання персональних даних, що стосуються суб'єкта даних, а також надання цих даних у доступній для розуміння формі; 3) право на виправлення або

видалення даних, якщо вони були оброблені всупереч положенням, що регламентують основні принципи обробки даних; 4) право мати засоби правового захисту у разі невиконання прохання про підтвердження або у відповідних випадках про надання, виправлення або знищення персональних даних. Важливим положенням, закріпленим у вищезгаданих міжнародно-правових актах, є створення наглядового органу із захисту персональних даних [40; 42].

Власне, еволюція європейських стандартів захисту персональних даних втілилася в основоположних засадничих принципах, що закріплені в оновленій Конвенції № 108+ та Загальному регламенті про захист даних 2016 р. Примітно, що ці міжнародно-правові акти спрямовані на забезпечення права на захист даних кожної особи, незалежно від її національності чи місця проживання, що свідчить про персоноцентризм та екстериторіальність застосування їх норм. Відповідно, положення Конвенції № 108+, і Загального регламенту про захист даних 2016 р. поширюються на державний та приватний сектори, забезпечуючи тим самим право на захист своїх персональних даних, однак обробка даних, що здійснюється особою під час суто особистої чи побутової діяльності становить виключення і у такому разі положення згаданих міжнародно-правових актів не застосовуються.

Обидва міжнародно-правові документи у статті 5 визначають основні принципи захисту персональних даних [47; 49], що зводяться до наступних:

1) принцип законності, справедливості та прозорості - персональні дані повинні бути отримані відповідно до мети, передбаченої законом, оброблятися у законний спосіб, справедливо і відкрито, тобто бути у доступній для суб’єкта даних формі;

2) принцип цільового обмеження - персональні дані повинні збиратися для певної, конкретної і законної цілі та не піддаватися додатковій обробці, яка не сумісна з початковою ціллю; як виключення, дозволяється подальша обробка для цілей архівування у суспільних інтересах, для наукових чи історичних досліджень і статистичних цілей;

3) принцип мінімізації даних – персональні дані повинні бути адекватними, відповідати початковій цілі та обмежуватися тими даними, які відповідають і необхідні для досягнення цілей, для яких вони обробляються;

4) принцип точності – персональні дані мають бути точними, повними та актуальними і, за необхідності, постійно оновлюватися, а неточні персональні дані, з урахуванням цілей обробки, повинні бути видалені або виправлені без затримки;

5) принцип обмеження зберігання – персональні дані повинні зберігатися у формі, що дозволяє ідентифікувати суб'єкта даних не довше, ніж це необхідно для цілей, для яких вони обробляються; як виключення, дозволяється зберігати персональні дані протягом тривалішого періоду виключно для цілей архівування у суспільних інтересах, для наукових чи історичних досліджень і статистичних цілей;

6) принцип цілісності та конфіденційності – персональні дані обробляються у спосіб, що забезпечує їх належний захист, включаючи захист від несанкціонованої або незаконної обробки, випадкової втрати, знищення або пошкодження, з використанням відповідних технічних або організаційних заходів, включаючи використання механізмів шифрування, аутентифікації та авторизації;

7) принцип підзвітності контролера – контролер несе відповідальність за дотримання принципів обробки персональних даних і повинен продемонструвати свою відповідність їм.

Зауважимо, що інші положення щодо обробки даних, закріплені у Конвенції № 108+ та Загальному регламенті про захист даних 2016 р., фактично є деталізацією і подальшим розвитком основних принципів обробки даних і, відповідно, розглядаються у їх світлі. Зокрема, положення щодо інформування суб'єкта про обробку персональних даних, а також його право отримувати інформацію про те, чи обробляються його персональні дані, хто їх обробляє та який порядок їх обробки фактично є деталізацією принципу справедливості обробки. Водночас право суб'єкта даних вносити зміни до персональних даних, що обробляються контролером, наприклад, у разі їх неактуальності, а також порядок реалізації цього права є втіленням принципу точності та актуальності. Положення, що стосуються підстав обробки даних є логічним продовженням принципу законності [88, с. 32]. Примітно, що обидва міжнародно-правові акти також розширюють перелік прав суб'єкта даних, серед іншого, гарантуючи право на отримання від контролера підтвердження факту обробки даних, право на доступ до персональних даних, право на виправлення та видалення даних, право не

підлягати рішенням, що ґрунтуються на автоматизованій обробці, включаючи профайлінг, право на заперечення проти обробки даних та право на мобільність даних.

Щоправда, хоча положення Конвенції № 108+ та Загального регламенту про захист даних 2016 р. повністю узгоджуються між собою, проте вони не є ідентичними. Зокрема, у ст. 5 Конвенції № 108+ втілений принцип пропорційності, що відповідає усталеній практиці ЄСПЛ щодо питань захисту персональних даних, згідно з яким обробка даних повинна бути пропорційною щодо законної мети, що переслідується, і відображати на всіх етапах обробки справедливий баланс між державними, приватними інтересами, правами особи, що знаходяться під загрозою [49]. При цьому, згідно зі ст. 5 Конвенції № 108+ обробка даних здійснюється на основі вільної, конкретної, поінформованої та однозначної згоди суб'єкта даних або іншої законної підстави. Відповідно до пояснювальної записки до Конвенції № 108+ поняття «законної підстави» передбачає, зокрема, обробку для виконання договору, для захисту життєво важливих інтересів суб'єкта даних або інших осіб, а також обробку для виконання юридичного зобов'язання контролера даних та обробку у випадку задоволення суспільних інтересів або переважання законних інтересів контролера чи третьої сторони. Водночас згода на обробку персональних даних повинна відображати вільне вираження власного вибору особи у письмові або усній формі, вона повинна становити чітку, стверджувальну дію, що однозначно вказує на прийняття конкретного механізму обробки персональних даних. Саме тому попередньо затверджені форми згоди, просте мовчання або бездіяльність суб'єкта даних щодо надання своєї згоди, не є згодою у розумінні Конвенції № 108+ [34].

Зауважимо, що Загальний регламент про захист даних 2016 р. у ст. 6 також визначає згоду як законну підставу для обробки персональних даних, а у ст. 7 чітко встановлює умови надання та відкликання згоди. У цьому аспекті право ЄС також вимагає, щоб згода була добровільною, поінформованою, чітко визначеною та однозначною [47]. Згода не вважатиметься добровільно наданою, якщо суб'єкт даних не має справжнього чи вільного вибору, або неспроможний відмовити в наданні згоди або її відкликанні без негативних наслідків. Визначальною рисою Загального регламенту про захист даних 2016 р. є те, що у ньому закріплені критерії перевірки того, чи є згода

вільно наданою, що здійснюється, зокрема, шляхом оцінки залежності виконання договору від згоди на обробку даних, що не є необхідною для виконання такого договору. Водночас детально регламентовані питання отримання згоди дитини у сфері послуг інформаційного суспільства – обробка персональних даних дитини є законною, якщо згода отримана від дитини, яка досягла щонайменше 16 років, а у разі якщо дитина не досягла цього віку обробка вважатиметься законною, коли згоду надано чи її надання санкціоновано носієм батьківської відповідальності щодо дитини (ст. 8). На додаток до згоди суб'єкта даних, ст. 6 Загального регламенту про захист даних 2016 р. встановлює ще п'ять законних підстав обробки даних, зокрема якщо обробка необхідна: 1) для виконання договору стороною якого є суб'єкт даних або для укладення договору; 2) для виконання іншого встановленого законом зобов'язання; 3) для захисту життєво важливих інтересів суб'єкта даних або іншої особи; 4) для виконання завдання в інтересах суспільства або здійснення офіційних повноважень контролера; 5) для законних інтересів контролера або законних інтересів третьої сторони, окрім випадків, коли переважають права суб'єкта даних, що вимагають охорони, особливо, якщо суб'єктом даних є дитина, однак ці положення не застосовуються, якщо обробка здійснюється державним органом, який обробляє дані для виконання своїх офіційних повноважень [47].

Отже, сучасною тенденцією європейської системи захисту персональних даних є формування взаємоузгоджених, єдиних стандартів у цій сфері. Ці стандарти сформувалися з огляду на популяризацію транскордонного обміну персональними даними, задля досягнення єдності в правовому регулюванні, яке узгоджувало б фундаментальні цінності поваги до недоторканості приватного життя особи й безперешкодний обмін інформацією між державами та втілилися у Загальному регламенті про захист даних та Конвенції № 108+. Однак, процес формування стандартів захисту персональних даних не можна вважати завершеним. Перш за все тому, що Загальний регламент про захист даних є актом регіонального значення, оскільки першочергово спрямований на захист даних громадян ЄС в межах ЄС, хоча він і може застосовуватися екстериторіально. Водночас Конвенція № 108+, положення якої узгоджуються з Загальним регламентом про захист даних, ще не набрала чинності. Все

ж можна стверджувати, що у сфері захисту персональних даних прослідковується уніфікація європейських стандартів захисту даних і їх широке впровадження на глобальному рівні. Крім того, у загаданих міжнародно-правових актах визнається та гарантується право на захист персональних даних як самостійне право людини, відокремлене від права на захист приватного життя.

Висновки до Розділу 1

За результатами дослідження засад виникнення, становлення та розвитку права на захист персональних даних у доктрині та практиці міжнародного права, здійсненого у першому розділі дисертації, було сформульовано такі висновки.

Виникнення і закріплення приватності як правової категорії пов'язують із публікацією у США статті «Право на приватність» С. Уоррена і Л. Брендайса. Згодом категорія приватності була розтлумачена у судових прецедентах і було виокремлено такий її елемент як інформаційна приватність, що передбачає встановлення правил, що регулюють збір та обробку персональних даних. У міжнародному праві захист приватності пов'язаний із визнанням і закріпленням права на захист приватного життя як одного з основоположних прав людини в універсальних та регіональних міжнародних договорах.

Ґенеза права на захист персональних даних свідчить, що його виникнення безумовно пов'язане із закріпленням та визнанням права на захист приватного життя як основоположного права людини і тривалий час право на захист персональних даних розглядалося лише як один з його аспектів та не було чітко визначене, що створювало прогалину в правовому регулюванні. Поступовому виокремленню та закріпленню як самостійного основоположного права людини на захист персональних даних сприяла широкомасштабна комп'ютеризація всіх сфер суспільного життя, впровадження новітніх технологічних розробок і необхідність у транскордонній передачі великих обсягів даних.

Формування підходів до захисту права та приватне життя і права на захист персональних даних перебуває у взаємозв'язку із національним, культурним, історичним та ідеологічним сприйняттям приватності та такого її аспекту як інформаційна приватність. Як наслідок, сформувалися декілька режимів захисту

приватності та персональних даних, що характерні для європейського регіону (так звана європейська модель захисту даних), США та, зокрема, країн Латинської Америки (так звана американська модель захисту даних).

Водночас у міжнародному праві прослідковується значна фрагментація норм щодо захисту персональних даних, що зумовлено відсутністю універсального міжнародного договору у цій сфері, відмінностями у сприйнятті приватності та персональних даних і, відповідно, існування конкуруючих правових режимів захисту даних. За відсутності універсального міжнародного договору стандарти захисту персональних даних в основному сформувалися в рамках діяльності саме РЄ та ЄС. У зв'язку з чим у доктрині та практиці використовують категорію «європейських стандартів захисту персональних даних», які можна охарактеризувати як найбільш узагальнені, керівні положення, принципи, основоположні правові засади у цій сфері.

В умовах глобалізаційного розвитку європейські стандарти захисту персональних даних поступово набули значного поширення по всьому світу і сприяли уніфікації норм щодо захисту даних на міжнародному рівні. З огляду на еволюційний розвиток європейських стандартів захисту даних виправданою є їх класифікація на: перше покоління (Керівні принципи ОЕСР 1980 р. та Конвенції № 108 у її первинній редакції 1981 р.), друге покоління (Конвенція № 108, оновлена Додатковим протоколом 2001 р., та Директива 95/46/ЄС) та третє покоління (оновлена Конвенція № 108+ зі змінами, внесеними Протоколом CETS № 223, та Загальний регламент про захист даних 2016 р.).

Сучасною тенденцією європейської системи захисту персональних даних є формування взаємоузгоджених, єдиних стандартів у цій сфері, що сформувалися з огляду на популяризацію транскордонного обміну персональними даними, з метою досягнення єдності в правовому регулюванні, що узгоджувало б фундаментальні цінності поваги до недоторканості приватного життя особи й безперешкодний обмін інформацією між державами. Можна стверджувати, що у сфері захисту персональних даних прослідковується уніфікація європейських стандартів захисту даних і їх широке впровадження на глобальному рівні.

Оновлена Конвенція № 108+ та Загальний регламент про захист даних спрямовані на забезпечення права на захист даних кожної особи, як самостійного основоположного

права, відокремленого від права на захист приватного життя, незалежно від національності чи місця проживання особи, що свідчить про персоноцентризм та екстериторіальність застосування їх норм.

Хоча право на захист персональних даних виникло порівняно нещодавно, це нове *sui generis* право завжди слід розглядати як таке, що тісно пов'язане та доповнює традиційні права, закріплені, зокрема, в ЄСПЛ та МПГПП, оскільки право на захист персональних даних прагне забезпечити повне та ефективне здійснення традиційних прав у відносно новому цифровому контексті.

РОЗДІЛ 2. ОСОБЛИВОСТІ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ В ЄВРОПЕЙСЬКОМУ СУДІ З ПРАВ ЛЮДИНИ

2.1 Правові засади регулювання захисту персональних даних у Раді Європи

Консолідація зусиль міжнародної спільноти задля координації діяльності у сфері захисту прав людини першочергово втілена у діяльності міжнародних організацій. Чільне місце серед таких міжнародних організацій займає РЄ, яка була створена після закінчення Другої світової війни у 1949 р. задля забезпечення стабільності на європейському континенті. РЄ є політичною регіональною міжнародною міжурядовою організацією, що забезпечує співробітництво держав у найважливіших сферах, за винятком національної оборони, становлячи інституційну основу європейського міжнародного права [89, с. 661]. Як зазначає вітчизняна дослідниця Л. Г. Фалалєєва, багатогранна діяльність РЄ сприяє утвердженню європейської ідентичності (у широкому сенсі) та формуванню культури толерантності, взявши за відправну точку міжнародні стандарти поваги до прав людини як однієї з основоположних цінностей демократичного суспільства, заснованого на верховенстві права. РЄ заохочує комплексне та системне вдосконалення законодавчого забезпечення зважаючи на динаміку розвитку європейських та інших міжнародних стандартів, спонукаючи керуватися ними під час правозастосування, а також забезпечувати своєчасне оновлення законодавства [90, с. 54-55].

Найбільш визначальним документом, прийнятим в рамках РЄ і підписаним усіма державами-членами, є ЄКПЛ, яка закріплює основоположні права людини та встановлює механізм їх захисту у ЄСПЛ. Прийняття ЄКПЛ стало визначною подією в міжнародному праві, оскільки вона не лише встановлювала перелік основоположних прав, наприклад, як Загальна декларація прав людини 1948 р., але створила й спеціальні установи із повноваженнями здійснювати судовий та квазісудовий контроль за дотриманням її положень. Однак від початку повноваження конвенційних контрольних органів щодо розгляду індивідуальних заяв були факультативними, що залишало за державами право визнавати юрисдикцію ЄСПЛ чи ні [91, с. 19].

Зауважимо, що право на захист персональних даних, хоча виникло після прийняття ЄКПЛ, проте питання захисту персональних даних, комп'ютеризації та використання новітніх технологій, викликали стурбованість на національному рівні, а відтак сприяли розробкам РЄ у цій сфері.

Вперше ПАРЄ відзначила питання, пов'язані із захистом даних, у 1968 р., коли звернулася до КМРЄ із Рекомендацією 509 (1968) Права людини та сучасні науково-технічні розробки з проханням вивчити, чи забезпечують ЄКПЛ та національне законодавство держав-членів належний захист права на приватне життя *vis-à-vis* сучасною наукою і технікою. Дослідження, проведене за вказівкою КМРЄ у відповідь на цю рекомендацію, показало, що чинне на той час національне законодавство не забезпечувало достатнього захисту приватності та інших прав та інтересів осіб щодо автоматизованих банків даних. На основі цих висновків КМРЄ у 1973 та 1974 рр. прийняв дві резолюції щодо захисту персональних даних: Резолюція (73) 22 та Резолюція (74) 29, які встановлювали принципи захисту даних для приватного сектору та, відповідно, державного сектору [34].

Необхідність узгодження правового регулювання захисту персональних даних сприяла прийняттю у 1980 р. ПАРЄ Резолюції 721 (1980) Обробка даних та захист прав людини, в якій наголошувалось на необхідності об'єднання зусиль держав задля зміцнення принципів та положень, які мають бути втілені в конвенції про захист даних РЄ, і якнайшвидшого укладення та набрання чинності майбутньою конвенцією РЄ у цій сфері [92]. Водночас на виконання згаданої резолюції ПАРЄ було також прийнято Рекомендацію 890 (1980), у якій наголошено на необхідності впровадження ефективного захисту персональних даних, а також запропоновано внести зміни до ЄКПЛ для забезпечення захисту персональних даних або шляхом внесення змін до ст. 8 чи ст. 10 ЄКПЛ, або шляхом доповнення ЄКПЛ новою статтею [93].

Уже 1981 р. в рамках діяльності РЄ було прийнято Конвенцію № 108 як основний документ, що визначав принципи та стандарти захисту прав людини, зокрема права на недоторканність приватного життя, у зв'язку з автоматизованою обробкою персональних даних. Як зазначає А. В. Пазюк, однією з підстав чому положення щодо захисту персональних даних не було включено до ЄКПЛ було те, що жодна редакція

такого доповнення не змогла б охопити всіх принципів щодо захисту персональних даних, які могли бути врегульовані за допомогою спеціальної конвенції [39]. Водночас прийняття окремого протоколу до ЄКПЛ, який би гарантував право на захист персональних даних не було б здатне забезпечити адекватний рівень захисту даних, оскільки додаткові протоколи до ЄКПЛ, які гарантують нові права людини не включені до основного тексту ЄКПЛ, обов'язкові тільки для тих держав, що їх підписали. Відтак було б вкрай тяжко забезпечити право на захист персональних даних, зокрема, при передачі даних між державою, яка ратифікувала б відповідний протокол до ЄКПЛ щодо захисту персональних даних, а також державою, яка його не ратифікувала.

Додамо, що прийняття спеціальної конвенції щодо захисту персональних даних було також обумовлено важливістю забезпечення безперешкодної транскордонної передачі персональних даних та поширення стандартів захисту персональних даних у країни поза межами європейського регіону. Як зазначено у пояснювальній записці до Конвенції № 108, у питаннях, пов'язаних із захистом персональних даних, недоцільно покладатися виключно на ЄКПЛ, зокрема, тому що вона є «закритим» інструментом, який не дозволяє участь неєвропейських держав та інших держав, які не є членами РЄ. Саме для того, щоб наголосити, що Конвенція № 108 є відкритою для приєднання не європейських держав було також вирішено уникнути словосполучення «Європейська Конвенція» у назві майбутнього міжнародного інструменту із захисту персональних даних [34].

Все ж навіть після прийняття Конвенції № 108 у науці міжнародного права виникали дискусії з приводу гарантування права на захист персональних даних у рамках ЄКПЛ. Беручи до уваги походження та еволюцію права на захист персональних даних, ЄКПЛ від початку не сприймалася як інструмент для належного захисту даних, оскільки концепція права на захист персональних даних виникала після її прийняття, і існували спеціальні міжнародно-правові акти, що детально регулюють цю сферу. Втім, ЄСПЛ зробив значний внесок у розвиток права на захист персональних даних, надавши широке тлумачення права на повагу до приватного життя та розширивши сферу дії статті 8 ЄКПЛ до питань захисту персональних даних.

Щоправда, після прийняття Конвенції № 108, яка детально регулювала основні принципи та керівні положення у сфері захисту даних, у науці висловлювалися думки щодо розробки окремого протоколу до ЄКПЛ, який би гарантував основопложне право на захист персональних даних у рамках конвенційної системи. Такий підхід, як зазначає дослідниця Н. Бистром, перш за все пояснюється внутрішнім та зовнішніми чинниками. Що стосується внутрішніх чинників, то посилання на статтю 8 та гарантоване нею право на повагу до приватного життя, згідно з тлумаченням ЄСПЛ, в цілому не здатне забезпечити достатній рівень захисту суб'єкта даних та його основних прав щодо захисту персональних даних. Відсутність єдиного, чіткого підходу призводить до фундаментальних суперечностей, коли у рішеннях ЄСПЛ інколи право на захист даних гарантується в рамках ст. 8 ЄКПЛ, а у деяких випадках основні права суб'єкта даних, такі як доступ до власних даних, право на виправлення чи видалення даних не гарантуються чи не визнаються ЄСПЛ. Водночас застосування ЄСПЛ у своїх рішеннях *доктрини еволюційного тлумачення* до справ, пов'язаних із гарантуванням права на захист персональних даних може підірвати юридичну точність, визначеність, рівність та передбачуваність у відношенні до суб'єкта даних, а застосування ЄСПЛ *доктрини свободи розсуду*, зокрема, у справах щодо захисту національної безпеки, має наслідком заперечення права на захист персональних даних. Більше того, саме зовнішні чинники, зокрема, цифрова революція, призводять до визнання персональних даних у цифровому суспільстві як абсолютно нової політичної та економічної цінності, що робить особу безпрецедентно вразливою. Відтак саме прийняття окремого протоколу вважається найкращим способом зміцнення конвенційної системи і гарантування права особи на захист персональних даних [94]. В цілому погоджуємося із зазначеною позицією, адже Конвенція № 108 не передбачає створення самостійного контрольного механізму для захисту гарантованого нею права на захист персональних даних, а зважаючи на багатогранність захисту персональних даних вважаємо, що існує необхідність у гарантуванні права на захист персональних даних як самостійного права в рамках конвенційної системи шляхом прийняття окремого протоколу, що забезпечило б належний захист таких аспектів права на захист персональних даних як право на забуття, право на заперечення проти обробки чи права на мобільність даних [95, с. 56-57].

Наголосимо, що окрім ЄКПЛ та Конвенції № 108 у рамках РЄ також прийнято низку інших міжнародно-правових договорів, які стосуються питань захисту персональних даних. Вочевидь міжнародні договори РЄ сприяють гармонізації та вдосконаленню національного законодавства держав-учасниць на засадах спільних правових стандартів [89, с. 662]. У цьому аспекті Фалалєєва Л. Г. наголошує, що: *«договірна практика Ради Європи та прецедентна практика ЄСПЛ заклали підвалини становлення і розвитку права Ради Європи як сукупності норм обов'язкового та рекомендаційного характеру, що регулюють міжнародні відносини в її рамках відповідно до основних принципів міжнародного права»* [82, с. 60]. Попри те, що Конвенція № 108, як і її оновлена версія, регулює всі сфери обробки персональних даних загалом у рамках РЄ також були розроблені низка міжнародно-правових документів, які детально регламентували питання захисту персональних даних у різних сферах, зокрема інформаційному секторі та сфері поліцейської діяльності і кримінального правосуддя. Такими документами є, серед іншого, Європейська конвенція про взаємну допомогу в кримінальних справах 1959 р., Конвенція про кіберзлочинність 2001 р., Конвенція про доступ до офіційних документів 2009 р.

Так, прийнята у РЄ Європейська конвенція про взаємну допомогу в кримінальних справах 1959 р. є основоположним документом у сфері кримінального правосуддя, який регулює питання взаємної допомоги у провадженні стосовно правопорушень, покарання яких на момент прохання про надання допомоги підпадає під юрисдикцію судових органів запитуючої Сторони. У аспекті захисту персональних даних вагому роль відіграє саме Другий додатковий протокол до Європейської конвенції про взаємну допомогу у кримінальних справах 2001 р., який у статті 26 визначає основні принципи захисту даних. Особливості принципу захисту даних у сфері кримінального правосуддя обумовлені специфічними цілями, а відтак у статті 26 визначено, що використання персональних даних здійснюється тільки: a) для цілей провадження, до якого застосовується ця Конвенція чи Протоколи до неї, b) для інших судових й адміністративних проваджень, безпосередньо пов'язаних із провадженням, зазначеним у підпункті «a», c) для запобігання безпосередній та серйозній загрозі суспільній безпеці. Персональні дані можуть бути використані з іншою метою за умови отримання згоди на

це Стороною, яка передала ці дані, або суб'єкта даних. У статті 26 також встановлено право держави відмовитися передавати персональні дані у випадках, коли такі дані не захищені у її національному законодавстві або Сторона, якій мають бути передані такі дані, не є зобов'язаною Конвенцією № 108 та не може забезпечити належний рівень захисту даних. Крім того, встановлюється право держави вимагати в іншої сторони надання інформації про те, як були використані передані персональні дані [96].

Водночас сфера захисту даних і сфера кримінального правосуддя також безпосередньо пов'язана із явищем кіберзлочинності. У цьому аспекті важливу роль для захисту персональних даних відіграє Конвенція про кіберзлочинність 2001 р., яка є зобов'язальним міжнародно-правовим документом РЄ, що стосується боротьби зі злочинами, вчиненими проти і за допомогою електронних мереж, а також вона стосується розслідування злочинів, де фігурують електронні докази [84, с. 296]. Примітно, що у преамбулі Конвенції про кіберзлочинність 2001 р. наголошено на необхідності забезпечення балансу між правоохоронними інтересами та основоположними правами людини, зокрема, й правом на захист персональних даних, як це передбачено Конвенцією № 108. Хоча у Конвенції про кіберзлочинність 2001 р. не вживається поняття «персональні дані», але використовується поняття «інформація про користувача послуг», що визначено як будь-яка інформація у формі комп'ютерних даних чи в іншій формі, яка знаходиться у постачальника послуг, належить до користувачів його послуг, не є даними про рух даних або власне даними змісту інформації, та за допомогою якої можна встановити a) тип комунікаційної послуги, яка використовувалася, її технічні положення і період користування, b) особистість користувача послуг, поштову або географічну адресу, телефони та інший номер доступу, інформацію про рахунки та платежі, яку можна отримати за допомогою угоди або домовленості про постачання послуг, c) будь-яку іншу інформацію про місце встановлення комунікаційного обладнання, яку можна отримати за допомогою угоди або домовленості про постачання послуг [97]. Відтак інформація про користувача послуг містить доволі детальну інформацію за допомогою якої можна ідентифікувати особу, зокрема, встановити її адресу, номери телефонів, номери рахунків тощо, а тому в розумінні європейських стандартів захисту персональних даних така інформація є

персональними даними. До того ж, до такої інформації належить й IP-адреса користувача послуг, яка є інформацією, що дозволяє ідентифікувати користувача і встановити адресу, звідки було здійснене з'єднання. Відтак, хоча Конвенція про кіберзлочинність 2001 р. безпосередньо не є інструментом захисту персональних даних, проте при вчиненні кіберзлочинів існує ризик витоку персональних даних, серед іншого, й чутливих даних, а тому стандарти кібербезпеки разом із європейськими стандартами захисту персональних даних значно підвищують рівень захисту персональних даних у цифровому просторі. Відповідно, імплементація міжнародно-правових у сфері кібербезпеки сприяє не тільки зменшенню кіберзлочинності, але й забезпечує додатковий рівень захисту персональних даних у мережі. Зауважимо, що розвиток інформаційних технологій та глобалізація комп'ютерних мереж мали безумовний вплив на процес модернізації Конвенції про кіберзлочинність 2001 р., яка у 2003 р. була оновлена Додатковим протоколом, який стосується криміналізації дій расистського та ксенофобного характеру, вчинених через комп'ютерні системи.

Також важливим міжнародно-правовим договором РЄ є Конвенція про доступ до офіційних документів 2009 р., яка регулює питання реалізації загального права на доступ до офіційних документів, що перебувають у розпорядженні державних органів. Як наголошено у Пояснювальній записці до Конвенції про доступ до офіційних документів 2009 р. дія цієї Конвенції поширюється на документи, що містять персональні дані, однак у разі надання доступу до таких документів, використання наявних у них персональних даних регулюється Конвенцією № 108 [98]. Таким чином, застосування Конвенції про доступ до офіційних документів 2009 р. сприяє забезпеченню справедливого балансу між правом на доступ до офіційних документів і правом на захист персональних даних, перш за все, шляхом вилучення з офіційних документів персональних даних чи іншої інформації, що може призвести до ідентифікації осіб, і позначення відповідних пропусків у документі. Водночас у разі якщо після вилучення такої інформації версія офіційного документа вводить в оману, є беззмістовною чи покладає явно необґрунтоване навантаження на державний орган щодо оприлюднення решти документа, то у наданні доступу до документа може бути відмовлено.

Щоправда, вагому роль у забезпеченні дотримання стандартів захисту персональних даних, викладених у Конвенції № 108 та інших міжнародних договорах РЄ, відіграють також рекомендаційні норми, ухвалені РЄ, які хоча й не є обов'язковими, проте сприяють узгодженню керівних принципів захисту даних зі специфікою певних сфер діяльності або технологічними розробками. До таких норм належать, зокрема, рекомендації, що стосуються використання і обробки даних у певних сферах чи визначених цілях, як от у статистичних цілях (Рекомендація № R (83) 10, згодом замінена Рекомендацією № R (97) 18 стосовно сфери статистики), для цілей прямого маркетингу (Рекомендація № R (85) 20); для цілей соціального забезпечення (Рекомендація № R (86) 1); у поліцейському секторі (Рекомендація № R (87) 15); для цілей працевлаштування (Рекомендація № R (89) 2); у сфері телекомунікаційних послуг (Рекомендація № R (95) 4); в Інтернеті (Рекомендація № R (99) 5); для цілей страхування (Рекомендація Rec (2002) 9); пов'язані з профайлінгом (Рекомендація CM/Rec (2010) 13); при використанні пошукових систем (Рекомендація CM/Rec (2012)3); та послуг соціальних мереж (Рекомендація CM/Rec (2012), а також при використанні алгоритмічних систем (Рекомендація CM/Rec (2020)1). Низка рекомендацій стосується обробки певних категорій даних, як от медичні дані (Рекомендація № R (81) 1 та Рекомендація № R (97) 5); ДНК (Рекомендація № R (92) 1); дані, отримані в результаті генетичних тестів (Рекомендація CM/Rec (2016)8); дані, пов'язані зі здоров'ям (Рекомендація CM/Rec (2019)2) [99].

Окрім того, утвердженню та уніфікації стандартів захисту персональних даних у праві РЄ сприяє й Парламентська Асамблея РЄ шляхом ухвалення резолюцій у цій сфері, зокрема, Резолюції 721, Обробка даних та захист прав людини (1980), Резолюції 1604, Відеоспостереження у громадських місцях (2008), Резолюції 1797, Необхідність глобального розгляду наслідків біометрії для прав людини (2011), Резолюції 1843, Захист конфіденційності та особистих даних в Інтернеті та онлайн-медіа (2011), Резолюції 1986, Покращення захисту користувачів та безпеки у кіберпросторі (2014), Резолюції 2342 (2020) Справедливість за алгоритмом - роль штучного інтелекту у системах поліції та кримінального правосуддя [99].

Зауважимо, що право РЄ у сфері захисту персональних даних продовжило свій розвиток з огляду на загрози та ризики, пов'язані із захистом даних, які були зумовлені початком світової пандемії COVID-19, оскільки остання не тільки порушила питання, пов'язані із захистом прав на здоров'я, а й вплинула на інші основоположні права людини, включаючи, зокрема, право на приватність та право на захист персональних даних. Задля боротьби з пандемією низка держав-учасниць РЄ оголосила на національному рівні надзвичайний стан, який є винятковим станом, що дає право уряду запровадити політику захисту безпеки своїх громадян шляхом обмеження певних основоположних прав людини. Враховуючи, що з початку глобальної пандемії уряди запровадили різноманітні надзвичайні заходи для боротьби з поширенням та передачею COVID-19, включаючи спеціальні програми для мобільних телефонів та засоби спостереження, право на приватність та право захист персональних даних були піддані високому ризику втручання. Варто зазначити, що з початку пандемії дев'ять держав-учасниць ЄКПЛ використали механізм «відступу у надзвичайних ситуаціях», передбачений статтею 15 ЄКПЛ, включаючи відступ від зобов'язань за статтею 8 ЄСПЛ, яка забезпечує право на приватне життя і право на захист персональних даних у рамках конвенційної системи [100].

Вочевидь заходи, прийняті державами для боротьби зі світовою пандемією, несуть загрозу серйозних втручань і можуть бути надмірними, а тому такі заходи мають бути критично оцінені через їх потенційний руйнівний вплив на приватність та захист даних. Так, надзвичайні заходи у різних країнах включали, наприклад, використання безпілотників для моніторингу руху осіб (Греція, Франція), використання спеціальних програм для COVID-19 на мобільних телефонах, які мали бути встановлені добровільно, для відстеження близькості та контактів між особами (Словенія, Україна), а також додатки для самоізоляції, які були обов'язковими для встановлення на мобільний телефон (Туреччина) [101]. Ці заходи безумовно впроваджувалися державами для відстеження та стримання розповсюдження COVID-19, але більшість з цих заходів безпосередньо ґрунтувалася на збиранні та використанні персональних даних про особу. Більшість держав, які запровадили подібні заходи, є сторонами Конвенції № 108, а також ЄСПЛ, а відтак при запровадженні таких заходів повинні бути дотримані керівні

принципи захисту даних, а саме наявність конкретної правової основи, яка б уповноважувала державні органи обробляти персональні дані, законної мети та конкретної цілі збору та обробки персональних даних, забезпечення відкритості та прозорості їх обробки, мінімізації даних, обмеження строків їх зберігання та вжиття заходів для захисту даних. Таким чином, така діяльність повинна підлягати контролю з боку органу захисту даних та повинні бути вжиті відповідні гарантії захисту даних.

Дотримання основних принципів захисту персональних даних в умовах кризи COVID-19 становить серйозну проблему для урядів. Найбільш поширеною проблемою є сумісність із принципом цільового обмеження збору даних. У ході пандемії у багатьох країнах були прийняті нормативні акти, які давали їм широку свободу розсуду, це призвело до ситуацій, коли персональні дані збиралися медичними працівниками з однією ціллю (у деяких випадках збір дозволявся без згоди пацієнта), а пізніше ці дані були використані або оброблені іншими органами влади для інших цілей. Наприклад, в деяких країнах медичні працівники надали список пацієнтів правоохоронним органам (Словенія, Греція, Угорщина), а в інших місцеві органи мали доступ до даних пацієнтів, оскільки вони відповідають за надання послуг тим, хто перебуває на карантині (Австрія, Нідерланди). Також деякі країни публікували дані про пацієнтів або померлих осіб, які не були анонімізовані або включали повне ім’я пацієнта, а отже, особу можна було безпосередньо ідентифікувати (Чорногорія, Чехія, Словаччина, Португалія, Румунія та Угорщина, Україна). Враховуючи, що персональні дані зберігаються кількома органами влади одночасно, терміни зберігання таких даних зазвичай не визначаються і становлять ще одну проблему. Втім, безстрокове зберігання персональних даних може призводити до непропорційного втручання у основоположні права особи, а отже, уряди повинні прийняти відповідні запобіжні заходи проти зловживання та інших негативних наслідків [102, с. 145-146].

Іншим викликом для урядів стало забезпечення дотримання принципу пропорційності, який є надзвичайно важливим для забезпечення балансу прав і інтересів, про які йдеться. Наприклад, на початку карантину дані про трафік та місцеперебування використовувалися для запобігання поширенню COVID-19 незалежно від стану здоров’я окремої людини. Використання таких даних передбачає,

що постачальники телекомунікаційних послуг надають такі дані державним органам, що дозволяє їм відстежувати переміщення осіб. Проте дані про трафік дозволяють владі обробляти контакти інфікованої особи та, відповідно, ідентифікувати діяльність такої особи та ролі людей, з якими вона контактує, інформувати про соціальні контакти інфікованого з іншими особами, які вимагають від вжиття відповідних заходів безпеки (карантин або добровільна ізоляція контактних осіб), а також забезпечувати регулярний моніторинг контактів для відстеження поширення симптомів та проведення тестування на ознаки інфекції [103, с. 383]. Вочевидь, деякі з цих заходів призводять до надмірного втручання, і пропорційність таких заходів можна оцінити лише в безпосередньому зв'язку з його ефективністю на практиці.

Додатковою перешкодою є питання відповідальності контролера або оператора персональних даних. Беручи до уваги те, що постачальники медичних послуг або інші органи, ймовірно, нададуть іншим органам доступ до персональних даних, важливо встановити достатні гарантії, які забезпечуватимуть права суб'єкта даних отримати інформацію про те, які дані збираються та хто саме їх обробляє, зберігає чи збирає.

Ще однією поширеною проблемою у світлі світової пандемії є використання персональних даних померлих осіб. Хоча європейські стандарти захисту персональних даних поширюються лише на живих осіб, проте оновлена Конвенція № 108, як і Загальний регламент про захист даних, дозволяють державам поширювати межі захисту персональних даних на померлих осіб. Незважаючи на те, що питання захисту персональних даних померлих осіб досить суперечливе як у теорії, так і на практиці, пандемія змушує держав приймати найбільш прогресивний та найбільш узгоджений із сучасними реаліями підхід, який вимагає деталізації законодавства щодо захисту персональних даних померлого, зокрема регулює питання щодо згоди суб'єкта даних на обробку його дані після смерті, можливість отримати або відкликати згоду на обробку даних від членів сім'ї або близьких родичів, а також наділити останніх правами суб'єкта даних (померлої особи), включаючи право на доступ, видалення або виправлення відповідних даних. Наразі лише деякі європейські країни, а саме Данія, Франція, Угорщина, Італія, Словаччина та Іспанія, прийняли законодавчі положення про захист персональних даних померлих осіб, але з точки зору боротьби з COVID-19 це питання є

надзвичайно важливим і вимагає детального регулювання [104]. Оскільки ЄСПЛ не трактував це питання у своїй судовій практиці, це може призвести до розвитку підходів щодо визначення меж та обсягу права на захист персональних даних і створення нових принципів у цьому аспекті.

Таким чином, надзвичайні заходи, прийняті урядами у відповідь на глобальну пандемію, створили численні загрози для права на приватність та права захист даних. Держави повинні дотримуватися основних стандартів та керівних принципів захисту даних навіть під час пандемії. Безперечно, невизначені цілі та необмежене зберігання даних впливає на прозорість обробки даних, але також порушує права суб'єкта даних, такі як право доступу до файлу даних, право на видалення чи виправлення даних. Відповідно, будь-яке втручання у право на захист даних має бути необхідним у демократичному суспільстві, пропорційним законній меті, що переслідується, та суті основоположних прав. Більш того, руйнівний вплив на право на захист персональних даних може бути значно зменшений шляхом запровадження інструментів, що забезпечують ефективний нагляд за надзвичайними заходами, запобігають свавіллю та запроваджують у цьому відношенні відповідні гарантії. Можна зробити висновок, що пандемія сприяла закріпленню та розвитку стандартів захисту даних і створила перспективи для тлумачення окремих аспектів права на захист персональних даних у судовій практиці ЄСПЛ.

Зауважимо також, що в рамках діяльності РЄ 28 травня 2021 р. було затверджено проєкт Другого додаткового протоколу до Конвенції про кіберзлочинність щодо посилення співробітництва та розкриття електронних доказів (далі – Другий додатковий протокол), який був розроблений у відповідь на збільшення кіберзлочинності, включаючи атаки на медичні заклади, державні органи та об'єкти критичної інфраструктури під час пандемії COVID-19, викрадення та використання персональних даних, збільшення онлайн насильства, втручання у вибори або зловживання технологіями в терористичних цілях. У проєкті Другого додаткового протоколу ст. 14 присвячується захисту персональних даних і містить, серед іншого, наступні принципи захисту даних, а саме: 1) використання персональних даних у визначених у ст. 2 цілях, а саме у конкретних кримінальних розслідуваннях або провадженнях щодо кримінальних

правопорушень, пов’язаних із комп’ютерними системами та даними, та до збору доказів у електронній формі, 2) забезпечення точності, повноти та оновлення персональних даних, 3) обробка чутливих даних виключно за відповідних гарантій для запобігання необґрунтованого непоправного впливу від використання таких даних, зокрема проти незаконної дискримінації, 4) обмеження періоду зберігання даних із передбаченням у національному законодавстві конкретних періодів зберігання або періодичного перегляду необхідності подальшого зберігання, 5) заборона отримання персональних даних на підставі рішень, що ґрунтуються виключно на основі автоматизованої обробки даних, 6) забезпечення безпеки даних, 7) ведення обліку або інші засоби демонстрації того, як здійснюється доступ, використання та розкриття персональних даних, 8) подальший обмін даних виключно у разі забезпечення ефективного рівня захисту даних, 9) прозорість обробки та повідомлення суб’єкта даних про законну мету, цілі обробки, строки обробки, одержувачів даних, право на доступ і виправлення даних та право на відшкодування. Водночас передбачається створення одного або декількох органів задля здійснення нагляду за додержанням вказаних принципів обробки даних [105]. Безумовно, світова пандемія COVID-19 мала наслідком перехід до використання цифрових інструментів практично у всіх сферах суспільного життя, включаючи роботу та освіту, що об’єктивно зумовило поширення кіберзлочинності. Розвиток глобальних комп’ютерних технологій та перехід суспільства у цифрову площину має значні ризики для забезпечення захисту персональних даних осіб, а тому боротьба із кіберзлочинністю вимагає більш жорсткого регулювання обробки персональних даних й більш деталізований виклад основних принципів їх захисту. Зауважимо, що положення Другого додаткового протоколу до Конвенції про кіберзлочинність 2001 р. враховують основні європейські стандарти захисту персональних даних, встановлюючи додаткові вимоги щодо захисту даних зумовлених ризиками сфери кіберзлочинності. Другий додатковий протокол до Конвенції про кіберзлочинність був прийнятий 17 листопада 2021 р. і відкритий для підписання з 12 травня 2022 р. та набере чинності після його ратифікації 5 державами. Зауважимо, що станом на жовтень 2023 року 40 країн підписали цей протокол, серед яких й Україна, включаючи 13 країн, які не є державами-

членами РЄ, а також двоє держав, а саме Сербія та Японія, ратифікували цей протокол після підписання [106].

Зауважимо, що вагому роль у розвитку європейських стандартів захисту даних мають ухвалені в рамках діяльності РЄ акти, спрямовані на врегулювання використання штучного інтелекту (ШІ) та забезпечення основоположних прав людини. Примітно, що в рамках РЄ було ухвалено низку актів м'якого права у цій сфері, включаючи, серед іншого, Рекомендацію CM/Rec(2020) Комітету міністрів державам-членам щодо впливу алгоритмічних систем на права людини, Рекомендацію 2102 (2017) ПАРЄ щодо технологічної конвергенції, штучного інтелекту та прав людини, а також Керівні принципи щодо штучного інтелекту та захисту даних T-PD (2019) 01, які наголошують на важливості забезпечення людської гідності, запобігання дискримінації та гарантування основоположних прав людини, зокрема права на захист персональних даних, при використанні технологій штучного інтелекту. Понад те, КМРЄ, застосовуючи наскрізний підхід до штучного інтелекту в різних секторах РЄ, було створено ad hoc Комітет зі штучного інтелекту, який діяв у 2019-2021 роках, наступником якого став чинний Комітет зі штучного інтелекту (Committee on Artificial Intelligence (CAI)), який займається розробкою [Рамкової] Конвенції про штучний інтелект, права людини, демократію та верховенство права [107].

Таким чином, право РЄ у сфері захисту персональних даних послідовно розвивається та є доволі деталізованим, включає міжнародно-правові акти як обов'язкового, так і рекомендаційного характеру, які відповідають сучасному розвитку суспільства і відповідним ризикам, пов'язаним із нестримним розвитком інформаційних технологій. Гарантування і ефективна реалізація на практиці основоположних прав забезпечується саме завдяки міжнародно-правовим договорам РЄ, які деталізують особливості захисту закріплених у ЄКПЛ основоположних прав і свобод у відповідних сферах діяльності. Водночас розвиток рекомендаційних норм, ухвалених у рамках дільяності РЄ, викликаний необхідністю забезпечення постійного оновлення положень міжнародно-правових договорів РЄ, зокрема, задля забезпечення тлумачення керівних принципів захисту персональних даних, закріплених у Конвенції № 108, з огляду на новітні технологічні розробки у світлі умов сьогодення. Втім, з огляду на усталеність

норм, закріплених у міжнародних договорах РЄ, найбільш дієво норми щодо захисту персональних даних оновлюються саме завдяки рекомендаціям та резолюціям, прийнятим у рамках діяльності РЄ, які інтерпретують питання застосування керівних принципів захисту даних у світлі новітніх змін в інформаційному середовищі.

2.2 Сучасні підходи до захисту персональних даних в Європейському суді з прав людини

Безсумнівно, у міжнародних нормативно-правових актах не можливо передбачити всю багатогранність аспектів, пов'язаних із захистом персональних даних з огляду на об'єктивні чинники такі, як постійний технологічний розвиток та розвиток суспільних відносин. Відтак, значний вплив як на розвиток європейських стандартів захисту персональних даних, так і на вдосконалення правових засад регулювання обробки та використання персональних даних, має розвиток практики міжнародних судових органів, зокрема ЄСПЛ. ЄСПЛ здійснює тлумачення відповідних конвенційних норм, використовуючи низку інтерпретаційних технік і принципів. Зауважимо, що професор С. Б. Карвацька наголошує на відсутності єдиного підходу до визначення терміну «принципи інтерпретації» (доктрини, концепти, концепції, теорії) [108, с. 275]. Таким чином, доволі часто вищезазначені терміни вживаються як синонімічні, взаємозамінні.

Особливості захисту персональних даних у ЄСПЛ пов'язані перш за все із відсутністю чітких положень щодо гарантування права на захист персональних даних безпосередньо у тексті ЄКПЛ чи Протоколах до неї. Вважаємо виправданим підхід (Л. А. Биграве, Б. Ван дер Слот) за якого презюмується, що право на захист персональних даних у конвенційній системі сформувалося внаслідок застосування ЄСПЛ *доктрини «живого інструменту» або доктрини еволюційного тлумачення* (англ. living instrument doctrine or evolutive interpretation doctrine) до статті 8 ЄКПЛ, яка гарантує право на захист приватного життя [109; 110]. Ця концепція виникла у 1978 році, коли у справі *Tyrer v. the United Kingdom,* яка стосувалась питання смертної кари, ЄСПЛ вперше зазначив, що «Конвенція є живим інструментом, яку слід тлумачити з урахуванням умов сьогодення» (§31) [111]. Власне, з прийняттям рішення у цій справі ЄСПЛ згодом дійшов важливого висновку, що положення ЄКПЛ повинні тлумачитися динамічно і відображати поточні реалії, виклики та загрози змін суспільства. З цих причин, як наголосив ЄСПЛ у рішенні

Airey v. Ireland, права та свободи, перелічені у ЄКПЛ, щоб вони були «практичними та ефективними, а не теоретичними та ілюзорними», не слід вважати вичерпними (§24) [112]. *Доктрина еволюційного тлумачення (або принцип еволюційного тлумачення)*, як зазначає Ю. С. Размєтаєва, включає два основні фактори: 1) невичерпний характер, закріпленого в ЄКПЛ, каталогу прав людини, який еволюціонує з розвитком суспільних відносин, та 2) цільове тлумачення положень ЄКПЛ задля забезпечення реального захисту прав людини [55, с. 142]. Як стверджує А. Моубрей, у своїй інтерпретаційній діяльності ЄСПЛ керується й *принципом дотримання прецеденту*, а відтак неухильно і переконливо дотримується своїх попередніх підходів та інтерпретації та відступає від них лише за наявності належної причини [113]. Зауважимо, що хоч рішення ЄСПЛ і мають прецедентний характер, все ж кожне рішення ухвалюється з урахуванням застосування ЄКПЛ до конкретних обставин кожної справи, а тому попередні прецеденти у певній сфері відіграють важливу, хоч і не вирішальну роль, і ЄСПЛ відступає від них за наявності відповідної необхідності.

У контексті захисту персональних даних, як зауважує Б. Ван дер Слот, саме розуміння ЄКПЛ як живого документа дозволило ЄСПЛ тлумачити її положення у світлі сучасних умов та створювати нові права людини, що відповідають розвитку суспільства і реаліям сьогодення. Наслідком застосування еволюційного тлумачення було розширення сфери більшості положень ЄКПЛ, але у цьому процесі основну функцію виконувала саме стаття 8 ЄКПЛ, сприяючи прийняттю нових прав у рамках конвенційної системи [114, с. 39-40]. Відтак саме завдяки *доктрині еволюційного тлумачення* стаття 8 ЄКПЛ розширила сферу свого застосування, що поступово призвело до визнання та гарантування права на захист персональних даних.

Ілюстрацією застосування ЄСПЛ *доктрини еволюційного тлумачення* у справах, пов’язаних із захистом персональних даних, є динамічне тлумачення статті 8 ЄКПЛ, наприклад, у справі *Leander v. Sweden* та *Amann v. Switzerland*, де прослідковується зміна підходу ЄСПЛ до визначення поняття приватне життя і поступове його наближення до поняття персональних даних, закріпленого у Конвенції № 108.

Так, у справі *Leander v. Sweden*, яка була однією з перших справ ЄСПЛ, що стосувалися питання захисту персональних даних, ЄСПЛ проаналізував законність

ведення таємного реєстру поліції та здійснення перевірки особи перед зайняттям певних посад за наявною у реєстрі інформацією. Хоча в даній справі не було встановлено порушення статті 8 ЄКПЛ, проте ЄСПЛ вперше зазначив, що зберігання і розповсюдження державними органами інформації про особу у поєднанні з відмовою надати можливість заявнику спростувати таку інформацію становило втручання у його право на повагу до приватного життя (§48) [115].

Згодом у справі *Amann v. Switzerland*, що стосувалася перехоплення телефонних розмов, створення та зберігання файлу про особу з цього приводу за допомогою заходів таємного спостереження, ЄСПЛ підтвердив свої попердні висновки і наголосив, що гарантії частини 1 статті 8 ЄКПЛ застосовуються до питань зберігання персональних даних, що стосуються приватного життя особи. Належну увагу було приділено Конвенції № 108 під час оцінки чи було втручання органів державної влади, шляхом збору та обробки персональних даних заявника, неправомірним. Водночас у цій справі ЄСПЛ наголосив, що в контексті персональних даних термін «приватне життя» не слід тлумачити обмежувально. Понад те, використання широкого тлумачення терміну «приватне життя» повністю відповідає положенням Конвенції № 108, яка визначає персональні дані як «будь-яку інформацію, яка стосується ідентифікованої особи, або особи, яку можна ідентифікувати» (§§65-67). Відтак, ЄСПЛ дійшов висновку, що дані про те, що заявник підтримував контакт з Російським посольством та вів справи з компанією А. беззаперечно становили дані, що відносяться до його приватного життя у розумінні ст. 8 ЄКПЛ [116].

Надалі у своїй практиці ЄСПЛ визнав, що під дію статті 8 ЄКПЛ підпадають, зокрема, обробка, зберігання і використання персональних даних, таких як: ім’я особи (Garnaga v. Ukraine, §36), інформація про дитинство особи (Odièvre v. France, §§28-29), медичні дані (L.H. v. Latvia, §47-60), генетичні та біометричні дані (S. and Marper v. the United Kingdom, §§70-77, 84), зображення особи (Von Hannover v. Germany (no. 2), §§95-99), дані про попередню професійну діяльність особи (Sõro v. Estonia, §§ 49, 56), дані щодо сексуальної орієнтації (Drelon v. France, §96) [117-123]. Враховуючи ключові принципи захисту персональних даних, викладені у статті 5 Конвенції № 108, ЄСПЛ також поступово дійшов висновку, що персональні дані можуть збиратися лише для

конкретних і законних цілей, що зумовлює виникнення позитивних зобов'язань держав встановлювати відповідні правила захисту даних.

Разом з тим, оскільки в ЄСПЛ спостерігається тенденція до розширення прав людини, то важливу роль також відіграє *принцип правової визначеності* відповідно до якого практика ЄСПЛ розвивається послідовно і має прецедентний характер, а відтак аналогічні справи не можуть вирішуватися по-різному. Такий підхід відповідає інтересам правової визначеності як такої та послідовного розвитку прецедентного права ЄКПЛ, проте не заважає ЄСПЛ відступити від попереднього рішення у разі якщо це виправдано для забезпечення тлумачення ЄКПЛ у світлі соціальних змін і якщо це відповідає сучасним умовам [55, с. 146]. Зауважимо, що *принцип правової визначеності* безпосередньо пов'язаний із забезпечення верховенства права, а тому положення ЄКПЛ варто тлумачити крізь призму її преамбули, в якій підкреслено, що верховенство право є частиною спільної спадщини Договірних сторін [24].

Крім того, зауважимо, що у 1980-х роках у практиці ЄСПЛ виникла доктрина, яка вимагала, щоб національні закони були доступними та передбачуваними. Відповідно до *доктрини доступності та передбачуваності* (англ. accessibility and foreseeability doctrine) ЄСПЛ має розглядати текст закону, сферу, яку він охоплює, а також кількість і статус тих, кому він адресований, щоб оцінити його чіткість та точність. Цю вимогу можна визначити як вимогу «доступності» закону. З одного боку, це означає, що норма повинна регулювати конкретну ситуацію, яка має значення для справи; з іншого боку, що з суб'єктивної точки зору громадянин повинен доступ до відповідних правових норм, які є достатніми та застосовуються до конкретної справи. Інший аспект, безпосередньо пов'язаний з попереднім, стосується передбачуваності наслідків власної поведінки: закон має бути сформульований з достатньою чіткістю, щоб громадянин міг передбачити обставини, в яких застосовується закон, та міг регулювати свою поведінку відповідно до положень закону [124, с. 37-38]. Як наголошує, Б. ван дер Слот, від початку ЄСПЛ нерішуче застосував *доктрину доступності та передбачуваності* до права на приватність та захисту персональних даних, особливо тому, що було б вкрай важко забезпечити дотримання цих принципів у справах, що стосувалися таємного

нагляду та спеціальних поліцейських розслідувань, де секретність та непередбачуваність складають фундаментальну основу [125].

ЄСПЛ неодноразово наголошував на важливості застосування *доктрини доступності та передбачуваності* у справах пов'язаних із захистом персональних даних. Однією з таких справ була *Malone v. the United Kingdom*, яка стосувалася законності перехоплення кореспонденції та телефонних дзвінків заявника. ЄСПЛ зазначив, що втручання повинно відповідати закону, який передбачає наявність у внутрішньому законодавстві підстав, сумісних із верховенством права. Таким чином, закон має бути належним чином доступним та передбачуваним, тобто сформульований з достатньою точністю, щоб давати можливість особі - за необхідності з відповідними порадами - регулювати свою поведінку. Щоб внутрішнє законодавство відповідало цим вимогам, воно повинно забезпечувати належний правовий захист від свавілля і з достатньою чіткістю вказувати на обсяг дискреційних повноважень, наданих компетентним органам, та спосіб їх здійснення (§§66-68) [126].

Згодом ЄСПЛ застосував *доктрину доступності та передбачуваності* у справі *Rotaru v. Romania*, де ЄСПЛ оцінив законність зберігання Службою розвідки Румунії файлу, що містив персональні дані заявника (включно інформацію про навчання, його громадську активність, публікації, участь в політичних організаціях тощо). ЄСПЛ у своєму рішенні наголосив, що національне законодавство не визначало межі реалізації владних повноважень щодо збору інформації, вид інформації, що може зберігатися, категорії осіб, щодо яких вона може збиратися, а також обставини, що зумовлюють збір інформації, чи процедуру збору. Понад те, національний закон не визначав конкретні строки зберігання такої інформації, коло осіб, що мають доступ до файлів, спосіб, у який дані можуть використовуватися та характер цих файлів. ЄСПЛ також зазначив, що зберігання та використання такої інформації не супроводжувалося гарантіями від зловживань з боку Служби розвідки Румунії. Зважаючи на зазначені факти ЄСПЛ визнав, що відповідне законодавство Румунії не було достатньо передбачуваним, а тому втручання у права заявника не було законним і порушувало ст. 8 ЄКПЛ. До того ж, у вказаному рішенні ЄСПЛ наголосив, що навіть публічна інформація може потрапляти у сферу приватного життя, у разі якщо вона систематично збирається та зберігається у

файлах, що знаходяться у володінні органів влади. Ці принципи мають навіть більше значення, коли така інформація стосується далекого минулого людини (§§48-63) [127].

Наголосимо, що у своїй практиці, зокрема у справі *Weber and Saravia v. Germany* щодо перехоплення повідомлень у рамках кримінального розслідування, ЄСПЛ розробив такі мінімальні вимоги, які повинні бути викладені в законі, щоб уникнути зловживання з боку органів влади: 1) характер правопорушень, які можуть стати підставою для наказу про перехоплення даних; 2) визначення категорій осіб, комунікації яких можуть бути перехоплені; 3) обмеження тривалості перехоплення даних; 4) процедура, якої слід дотримуватися для вивчення, використання та зберігання отриманих даних; 5) запобіжні заходи, які слід вжити при передачі даних іншим сторонам; та 6) обставини, за яких перехоплені дані можуть або повинні бути стерті або знищені (§95) [128].

Щоправда, у справі *Roman Zakharov v. Russia* ЄСПЛ розвинув і узагальнив принципи захисту персональних даних відносно інформації, отриманої за допомогою заходів таємного спостереження, які дозволяли перехоплювати телефонні комунікації. Таким чином, ЄСПЛ сформулював детальні критерії захисту персональних даних, які зводяться до наступних вимог: 1) дані слід збирати на основі закону; 2) положення закону повинні відповідати вимогам доступності, ясності та передбачуваності; 3) рішення про введення заходів таємного спостереження повинно підлягати судовому перегляду або контролю іншим органом; 4) такий контроль повинен надавати особі можливість викласти свої аргументи; 5) рішення суду має бути обґрунтованим для запобігання свавільному втручанню; 6) вказівки у рішенні суду щодо того, до яких даних (документів) можна отримати доступ, мають бути максимально зрозумілими; 6) особа, щодо якої дані збираються таємно, повинна мати ефективні засоби захисту, які передбачали б можливість оскаржити законність та обґрунтованість рішення про доступ до такої інформації, а також отримати компенсацію у разі порушення; 7) доступ повинен надаватися лише до інформації, необхідної для цілей розслідування; 8) отримана інформація повинна бути належним чином зафіксована, збережена та захищена з метою запобігання її зміні, незаконному знищенню та розповсюдженню; 9) отриману інформацію слід негайно знищити у разі зникнення подальшої потреби в ній (§§227-

305). ЄСПЛ підсумував, що недотримання цих правил призведе до порушення прав особи, гарантованих ст. 8 ЄКПЛ [129].

Стверджується, що визначальну роль для розвитку права на захист персональних даних у конвенційній системі мала також *доктрина свободи розсуду* (англ. margine of appreciation doctrine). Як зауважує Андрущенко К. А., «*хоча щодо «margin of appreciation» вживаються поняття «концепція», «доктрина», суть цих понять, тобто їх правовий зміст, роз'яснюється тотожно*» [130, с. 40]. *Доктрина свободи розсуду* втілює принцип пропорційності, однак не зводиться лише до нього. ЄСПЛ застосовує *доктрину свободи розсуду* до питань захисту персональних даних, надаючи державі свободу дій щодо виконання своїх зобов'язань за ЄКПЛ та відображаючи допоміжну роль ЄСПЛ. Проте водночас вона вимагає, щоб держави досягли балансу між конкуруючими приватними/суспільними інтересами та конвенційними правами і свободами, а також передбачили відповідні гарантії у національному законодавстві, щоб особа не підлягала свавільному поводженню [124, с. 45]. Як зазначає дослідниця Н. Бистром, хоча саме теорія еволюційного тлумачення дозволяє ЄСПЛ розглядати дедалі складніші справи щодо захисту персональних даних у цілому і щодо прав суб'єкта даних, але доктрина свободи розсуду також є дієвою у цій сфері у переважній більшості справ. Втім, доктрину свободи розсуду як правило критикують через залежність від європейського консенсусу щодо обсягу свободи розсуду держави в тому чи іншому питанні [131, с. 219, 239]. Так, у рішенні *Hämäläinen v. Finland* ЄСПЛ зазначив, що при визначенні свободи розсуду необхідно враховувати низку факторів: у справах, де на кону постає особливо важливе питання існування чи ідентичності особи, свобода, надана державі, буде обмежена, а у справах, де європейські країни не мають єдиної думки (консенсусу) щодо відносної важливості певного інтересу або щодо найкращих засобів його захисту, особливо, коли справа порушує делікатні моральні чи етичні питання, свобода розсуду буде ширшою. Так само широкою буде свобода розсуду у разі якщо від держави вимагається знайти баланс між конкуруючими приватними та публічними інтересами або правами, гарантованими ЄКПЛ (§67) [132]. Відповідно, саме юридична ясність, визначеність та передбачуваність у поєднанні з відносно невеликою свободою дій держави здатна забезпечити послідовний та ефективний захист

персональних даних. Водночас у разі з якщо свобода дій держави є широкою, законодавство повинно передбачати належні гарантії для суб'єкта даних від свавільної поведінки органів влади, наділених широкими повноваженнями щодо збору та обробки персональних даних.

У цьому аспекті на увагу заслуговують висновки ЄСПЛ у справі *M. K. v. France*, де ЄСПЛ наголосив, що держава вийшла за межі наданої свободи розсуду і не дотималася балансу інтересів особи та суспільства, що призвело до порушення ст. 8 ЄКПЛ. У цій справі було розпочато розслідування щодо заявника за крадіжку книг, слідчі органи відібрали у нього відбитки пальців і внесли їх у національну базу даних відбитків пальців. Пізніше заявник звернувся із вимогою видалити його відбитки пальців з цієї бази даних, однак йому відмовили. Національні суди посилалися на те, що збереження відбитків пальців відповідало інтересам слідчих органів з огляду на необхідність накопичення більшої кількості зразків відбитків для їх порівняння у ході розслідування. ЄСПЛ вкотре наголосив, що свобода розсуду, ступінь якої змінюється в залежності від низки факторів, включаючи характер діяльності, що обмежується, та цілей, які переслідуються цими обмеженнями, в принципі, повинна бути залишена державам (§34). Однак ЄСПЛ визнав, що у справі за цілі обробки відбитків пальців у базі даних, вказані національними органами, були настільки широкі, що дозволяли збирати дані практично щодо всього населення. Водночас національне законодавство не передбачало належного захисту прав осіб, дані яких збиралися, оскільки можливість видалення даних, яка насправді не була правом таких осіб, була скоріше «теоретичною та ілюзорною», а не «практичною та ефективною». Крім того, строки зберігання хоча і були обмежені у часі, проте могли продовжуватися до двадцяти п'яти років, а відтак такий термін на практиці дорівнює безстроковому зберіганню (§39-47) [133].

З особливою увагою та обачністю ЄСПЛ застосовує *доктрину свободи розсуду*, а також *доктрину доступності та передбачуваності* до справ, пов'язаних із масовим перехопленням даних з метою захисту національної безпеки. Визначальними справами, що узагальнюють ключові підходи у цьому аспекті, є *Big Brother Watch and Others v. the United Kingdom* та *Centrum för rättvisa v. Sweden*, які були розглянуті Великою Палатою ЄСПЛ 25 травня 2021 року. В обох справах Велика Палата ЄСПЛ наголосила, що на

відміну від цільового перехоплення, яке було предметом більшої частини практики ЄСПЛ і яке в основному використовується для розслідування злочинів, масове перехоплення також – можливо, навіть переважно – використовується для збору іноземної розвідувальної інформації та виявлення нових загроз з боку як відомих, так і невідомих акторів. Діючи в цій сфері, Договірні Держави мають законну потребу в секретності, що означає, що лише невелика частина інформації про функціонування цієї схеми буде загальнодоступною, але навіть доступна інформація може бути викладена в термінології, яка є неясною та яка може значно відрізнятися від однієї держави до іншої. Зважаючи на зазначене, у цих справах ЄСПЛ визначив основні етапи масового перехоплення: (a) перехоплення та початкове збереження комунікацій та пов'язаних комунікаційних даних (тобто даних про трафік, що належать до перехопленого зв'язку); (b) застосування специфічних селекторів до збережених комунікаційних/пов'язаних даних зв'язку; (c) аналіз вибраних комунікацій/ пов'язаних комунікаційних даних аналітиками; (d) подальше збереження даних та використання «кінцевого продукту», включаючи обмін даними з третіми сторонами [134; 135].

Водночас Велика Палата ЄСПЛ в обох справах зазначила, що як і у випадку з будь-яким режимом перехоплення, звичайно, існує значний потенціал для зловживання масовим перехопленням таким чином, що негативно впливає на право осіб на повагу до приватного життя. Хоч ст. 8 ЄКПЛ не забороняє використання масового перехоплення для захисту національної безпеки та інших суттєвих національних інтересів від серйозних зовнішніх загроз, і держави мають широкий розсуд у вирішенні того, який тип режиму перехоплення необхідний для цих цілей, але під час роботи з такою системою свобода розсуду, що надається їм, повинна бути вужчою, і необхідно передбачити низку запобіжних заходів. Оцінюючи, чи діяла держава у межах наданої свободи розсуду, потрібно враховувати ширший діапазон критеріїв, ніж встановлений у попередній практиці ЄСПЛ у справі *Weber and Saravia v. Germany*. Також ЄСПЛ наголосив, що вирішуючи питання відповідності критеріям «згідно з законом» та «необхідності» одночасно потрібно розглянути питання, які повинні бути з достатньою чіткістю передбачені у національному законодавстві, а саме: 1) підстави, за яких може бути дозволено масове перехоплення; 2) обставини, за яких можуть бути перехоплені

комунікації окремої особи; 3) порядок надання дозволу для перехоплення; 4) процедури, яких слід дотримуватись для відбору, вивчення та використання перехопленого матеріалу; 5) запобіжні заходи, які слід вживати при передачі матеріалів іншим сторонам; 6) обмеження тривалості перехоплення, зберігання перехопленого матеріалу та обставин, за яких такий матеріал має бути стертий та знищений; 7) процедури та умови здійснення нагляду незалежним органом за дотриманням вищезазначених гарантій та його повноважень щодо вирішення питань у разі їх недотримання; 8) процедури незалежного *ex post facto* контролю відповідності вказаним умовам та повноваження, якими наділений компетентний орган щодо вирішення випадків невідповідності [134; 135].

У справі *Big Brother Watch and Others v. the United Kingdom* Велика Палата ЄСПЛ встановила, що режим масового перехоплення у Великобританії не містив достатніх «наскрізних» гарантій, щоб забезпечити адекватні та ефективні гарантії від свавілля та ризику зловживань, що мало наслідком порушення статей 8 та 10 ЄКПЛ. Водночас режим, згідно з яким Великобританія могла запитувати розвідувальні дані від іноземних урядів та/або розвідувальних органів, закріплював належні гарантії, і тому не призвів до порушення статті 8 або 10 ЄКПЛ [134]. Що стосується справи *Centrum för rättvisa v. Sweden*, то Велика Палата ЄСПЛ наголосила на наступних недоліках у системі масового перехоплення: 1) відсутність чітких правил щодо знищення перехопленого матеріалу, який не містить персональних даних; 2) відсутність у відповідному законодавстві вимоги про те, що під час прийняття рішення про передачу розвідувальних матеріалів іноземним партнерам враховуються інтереси приватності осіб; 3) відсутність ефективного *ex post facto* контролю. Таким чином, шведський режим масового перехоплення, якщо розглядати його в цілому, не містив достатніх «наскрізних» гарантій, щоб забезпечити адекватні та ефективні гарантії проти свавілля та ризику зловживань, що призвело до порушення статті 8 ЄКПЛ [135]. Вочевидь навіть у справах, де превалюють певні національні інтереси, ЄСПЛ оцінює втручання з позиції того чи є національне законодавство якісним та доступним і, чи містить воно гарантії щодо запобігання свавільному втручанню у право на захист персональних даних.

Іншим важливим принципом забезпечення ефективної реалізації права на захист персональних даних є виконання державою кореспондуючих обов'язків. Відповідно, при розгляді справ ЄСПЛ застосовує *доктрину позитивних зобов'язань*, яка передбачає, що держава повинна забезпечити найбільш повне дотримання як позитивних, так і негативних прав і вживати розумних та належних заходів для їх реального здійснення. Екстраполюючи вказане на сферу захисту персональних даних, зауважимо, що ЄСПЛ розглядає два основних аспекти – дотримання державою позитивних зобов'язань, тобто наявність гарантій дотримання права на захист персональних даних, а також негативних зобов'язань, тобто утримання від свавільного втручання в це право з боку держави.

Зауважимо, що межа між позитивними та негативними зобов'язаннями держави за ЄКПЛ не піддається точному визначенню, але принципи, які застосовуються, однак, є подібними. В обох контекстах ЄСПЛ, зокрема у справах *Gaskin v. the United Kingdom* (§42) та *Palomo Sánchez and Others v. Spain* (§62), зазначив, що слід враховувати справедливий баланс, який має бути досягнутий між конкуруючими інтересами окремої особи та суспільства в цілому, який у будь-якому випадку залежить від свободи розсуду, якою користується держава [136; 137].

З урахуванням *доктрини еволюційного тлумачення* ЄКПЛ, обсяг та зміст позитивних зобов'язань держави щодо забезпечення відповідних прав може розширюватися і зазнавати змін. Все ж певні фактори вважаються релевантними для оцінки змісту позитивних зобов'язань держав. У справі *Sõro v. Estonia* (§67) було зауважено, що вони стосуються важливості поставлених на карту інтересів і того, чи йдеться про «фундаментальні цінності» чи «основні аспекти» приватного життя, або ж про вплив на заявника невідповідності між соціальною реальністю та законом, узгодженості адміністративної та юридичної практики у національній системі, що розглядається як важливий фактор у справах за статтею 8 ЄКПЛ [122]. Таким чином, позитивні зобов'язання держави за ст. 8 ЄКПЛ не будуть виконані належним чином, у разі якщо на практиці держава не забезпечує повагу до приватного життя у відносинах між особами шляхом створення законодавчої бази з урахуванням різних інтересів, які підлягають захисту в конкретному контексті.

На увагу заслуговують також висновки ЄСПЛ у справі *Liebscher v. Austria*, яка стосувалася вимоги до заявника надати всю угоду про розлучення (а не витяг з неї) для того, щоб внести ці дані до державного земельного кадастру, який є відкритим для громадськості, з метою передачі частки нерухомого майна колишній дружині заявника. Вказана угода про розірвання шлюбу містили прізвища та місця проживання неповнолітніх дітей, розміри аліментів, домовленості щодо батьківської опіки, угоду про поділ майна (крім нерухомого) та перелік доходів та майна заявника. ЄСПЛ вирішив, що ця справа має розглядатися з позиції позитивного зобов'язання держави вжити заходів, спрямованих на забезпечення поваги до приватного життя, включаючи як забезпечення нормативної бази, так і впровадження, у разі необхідності, конкретних заходів (§§60-61) [138].

Позитивні зобов'язання щодо забезпечення ефективного захисту гарантованих ЄКПЛ прав можуть включати, зокрема, зобов'язання забезпечити особі право на доступ до її персональних даних чи отримати доступ до інформації про себе, яка збирається і зберігається державними органами. Так, у справі *Gaskin v. the United Kingdom* ЄСПЛ встановив порушення ст. 8 ЄКПЛ у зв'язку з обмеженням доступу заявника до документів, які зберігалися соціальними службами та стосувалися його раннього дитинства і виховання. Окрім того, порушення прав заявника були зумовлені і відсутністю незалежного органу, який би розглядав клопотання щодо надання доступу до персональних даних. ЄСПЛ також наголосив, що надаючи доступ до такої інформації, необхідно водночас забезпечити конфіденційність захисту даних третіх осіб (§49) [136]. Водночас у справі *Ciubotaru v. Moldova*, яка стосувалася запису в офіційних реєстрах даних щодо етнічного походження заявника, ЄСПЛ, наголошуючи на дуже чутливому характері таких даних, визнав наявність позитивного зобов'язання держави щодо запровадження процедури, яка дозволить суб'єкту даних змінити запис про його/її етнічну приналежність на основі об'єктивно підтверджених доказів (§§52-53) [139].

Примітно, що у рішенні *Bărbulescu v. Romania* ЄСПЛ зазначив, що хоча основним завданням ст. 8 ЄКПЛ є захист осіб від свавільного втручання у їх право на повагу до їхнього приватного та сімейного життя, житла та кореспонденції з боку державних органів чи приватних організацій, яким держава делегувала певні обов'язки, вона також

може покладати на державу певні позитивні зобов'язання щодо забезпечення ефективного дотримання цих прав. У цій справі ЄСПЛ зазначив, що захід, на який скаржився заявник, а саме моніторинг його комунікацій в Yahoo Messenger, що призвів до дисциплінарного провадження проти нього з подальшим звільненням за порушення внутрішніх правил трудового розпорядку компанії, був прийнятий не державним органом, а саме приватною комерційною компанією. ЄСПЛ зазначив, що моніторинг повідомлень заявника та перевірка їх змісту роботодавцем з метою обґрунтування його звільнення не може розглядатися як «втручання» в його право з боку державного органу. Втім, вжиті роботодавцем заходи були визнані правомірними національними судами. Відтак, моніторинг повідомлень заявника хоча й не був результатом прямого втручання з боку органів влади, але відповідальність держави виникає у разі, якщо факти, на які скаржиться заявник, випливають із нездатності з органів влади забезпечити заявнику реалізацію права, закріпленого у ст. 8 ЄКПЛ (§§109-111) [140].

Відтак, аналізуючи практику ЄСПЛ, у разі якщо захід, що перешкоджає захисту персональних даних, впроваджується фізичною чи юридичною особою виключно в приватному секторі, то ЄСПЛ розглядатиме справу з точки зору позитивних зобов'язань держави. Однак, якщо захід було запроваджено державним органом або приватним органом, якому держава делегувала свої зобов'язання, ЄСПЛ розгляне справу з точки зору негативного зобов'язання держави.

У контексті дотримання державами негативних зобов'язань ЄСПЛ застосовує трискладовий тест та вирішує, чи було втручання «передбачено законом», чи переслідувало воно законну мету та, чи було «необхідним у демократичному суспільстві». Класичною справою, що стосувалася питання дотримання негативних зобов'язань держави щодо зберігання інформації про особу в державному реєстрі вважається справа *Leander v. Sweden*, яка стосувалася зберігання інформації про приватне життя заявника в секретному поліцейському реєстрі [115]. Пізніше ЄСПЛ також досліджував питання порушення негативних зобов'язань держави у справах, що стосувалися: 1) публікації районною радою записів з камери відеоспостереження, розташованої в публічному місці, без дозволу заявника і без маскування його обличчя (Peck v. the United Kingdom, §60-63), 2) збирання інформації правоохоронними органами

в рамках кримінального провадження, зокрема GPS даних (Uzun v. Germany, §52), відбитків пальців, ДНК профілів та зразків клітин (S. and Marper v. the United Kingdom, §§ 67-69), IP-адрес (Benedik v. Slovenia, §120), 3) розголошення медичних даних заявника у судовому рішенні, яке було поширене у пресі (Z v. Finland, §§95-96), 4) розголошення чутливих персональних даних, а саме інформації про ВІЛ позитивний статус заявниці (M. K. v. Ukraine, §§41-61) [120; 141-145].

Водночас наголосимо, що питання щодо відповідальності держави може виникати та у разі коли приватні компанії чи не державні органи діють в інтересах держави. Зокрема, питання щодо відповідальності за стеження за телефонними дзвінками, електронною поштою та підключенням до Інтернету працівника школи було досліджено у справі *Copland v. the United Kingdom*. ЄСПЛ дійшов висновку, що питання, яке підлягає аналізу, стосувалося саме негативного зобов'язання держави не втручатися в приватне життя та кореспонденцію заявника, оскільки школа розглядалася як державний орган, за дії якого у цілях ЄКПЛ відповідав Уряд (§39) [146]. Так само у справі *Vukota-Bojić v. Switzerland* ЄСПЛ дійшов висновку, що держава несе відповідальність за збирання та зберігання персональних даних приватною страховою компанією, яка діяла в рамках схеми державного страхування, а відтак фактично була публічним органом (§47) [147].

Зауважимо також, що у своїх рішеннях ЄСПЛ також наголошує на важливості *принципу неілюзорності прав та забезпечення їх практичності та ефективності (принцип ефективності гарантованих прав)*, який є наскрізним принципом для всіх положень ЄКПЛ, оскільки вона гарантує не теоретичні та ілюзорні права, а права, які є практичними і є ефективними. Саме з огляду на цей принцип при розгляді справ ЄСПЛ не обмежується тільки формальною перевіркою чи закріплено відповідне право у національному законодавстві [148, с. 9]. У цьому аспекті також погоджуємося з професором С. Б. Карвацькою, що «*необхідність практичного й ефективного захисту прав прав і свобод людини сприяла виробленню ЄСПЛ унікального інтерпретаційного підходу для конвенційних норм, оскільки він надавав можливість не обмежуватися гарантіями, вже зафіксованими в ЄКПЛ, а постійно їх розширювати*» [108, с. 279]. Таким чином, забезпечення і гарантування права на захист персональних даних сприяє наповненню змістом та виконанню першочергової мети ст. 8 ЄКПЛ, а саме захисту

права на приватність. Проте, саме завдяки еволюційному тлумаченню ЄСПЛ здатен потенційно розширювати можливості для ефективної практичної реалізації прав, гарантованих ЄКПЛ, та забезпечувати ефективність нових прав, що виникають з огляду на нестримний розвиток людства.

У контексті захисту персональних даних *принцип ефективності гарантованих прав* був застосований ЄСПЛ у справі *K. H. and Others v. Slovakia,* яка стосувалася питання незабезпечення права заявниць отримати копії власних медичних документів. ЄСПЛ наголосив, що оскільки реалізація права на повагу до приватного та сімейного життя, гарантованого статтею 8, повинна бути практичною й ефективною, то позитивні зобов'язання держави мають поширюватися, зокрема, на надання суб'єкту даних копій документів, що містять його чи її персональні дані (§§47-48). Також ЄСПЛ зазначив, що власник файлу може визначити порядок копіювання файлів персональних даних і чи повинен суб'єкт даних нести витрати на це, проте суб'єкти даних не зобов'язані конкретно обґрунтовувати запит на надання копії документів, що містять їх персональні даних. Крім того, у цій справі національні суди і Уряд-відповідач наполягали на тому, що заборона виготовлення копій документів, що містили медичні дані заявниць, була обґрунтована необхідністю захисту відповідної інформації від зловживань, але, на переконання ЄСПЛ, такі аргументи не є достатньо переконливими та не можуть більш вагомими, ніж право заявників на отримання копій їхніх медичних карт (§§53-54) [149].

На відміну від попередньої справи, у справі *Dalea v. France*, яка стосувалася довгострокової реєстрації персональних даних заявника в Шенгенській інформаційній системі, ЄСПЛ визнав, що держава забезпечила право заявника на доступ до персональних даних про себе. Хоча заявник не був у змозі ознайомитися з точними підставами його включення до Шенгенської бази даних, йому було надано доступ до всіх інших його персональних даних і він був поінформований, що підстава внесення його даних до Шенгенської бази даних стосується державної безпеки, оборони та громадської безпеки. ЄСПЛ зазначив, що відсутність у заявника особисто повного доступу до інформації, яку він запитував, не може порушити право на повагу до його приватного життя, беручи до уваги необхідність захисту національної безпеки [150].

Оскільки, як зазначено вище, право на захист персональних даних фактично виникло внаслідок застосування *доктрини еволюційного тлумачення* до статті 8 ЄКПЛ, переважна більшість підходів ЄСПЛ щодо захисту даних сформовані та викладені у його судових рішеннях саме в рамках розгляду порушень цієї статті. Втім, питання захисту персональних даних не обмежуються лише статтею 8 ЄКПЛ та можуть стосуватися здійснення й інших гарантованих ЄКПЛ прав, зокрема права на справедливий суд, права на свободу думки, совісті та релігії чи права на свободу вираження поглядів [151, с. 54].

У цьому контексті зазвичай ЄСПЛ використовує *принцип пропорційності та забезпечення рівноваги інтересів (принцип пропорційності)* задля урівноваження конкуруючих прав і свобод, гарантованих ЄКПЛ, більшість з яких не є абсолютними, а відтак можуть підлягати обмеженням за певних умов. Зауважимо, що *принцип пропорційності* у практиці ЄСПЛ щодо захисту персональних даних фактично передбачає, що обробка персональних даних має здійснюватися відповідно до засад адекватності, відповідності та ненадмірності стосовно цілей, задля яких вони збираються. У цьому аспекті ЄСПЛ розглядає й питання забезпечення рівноваги між правами та інтересами окремих осіб або питання забезпечення балансу між приватними та публічними інтересами. У низці справ ЄСПЛ аналізував заходи, вжиті органами влади в процесі судового розгляду, що призвели до розкриття персональних даних сторін судового провадження чи третіх осіб внаслідок відтворення судом у рішенні про розлучення медичних даних заявника, отриманих без його дозволу і згоди (L. L. v. France, §46), розголошення в публічному судовому засіданні конфіденційної інформації про стан психічного здоров'я і психіатричне лікування заявника (Panteleyenko v. Ukraine, §57), нездатність національних судів надати належні причини для відхилення вимог заявника у судовому провадженні проти його роботодавця щодо захисту персональних даних (Surikov v. Ukraine, §102-103) [152-154].

Примітно, що ЄСПЛ досліджував також випадки порушення ст. 9 ЄКПЛ, яка гарантує свободу думки, совісті та релігії, в контексті захисту персональних даних особи. Зокрема, на увагу заслуговують висновки у справі *Sinan Işık v. Turkey*, яка стосувалася питання зазначення — в обов'язковому чи добровільному порядку — даних про релігію в посвідченні особи. На думку ЄСПЛ, факт необхідності письмового

звернення до органів влади щодо зміни даних про релігію у реєстрі та в посвідченнях особи, а також сам факт наявності у посвідченні особи поля «релігія», зобов'язував особу розкривати, проти її волі, інформацію, що стосується її релігійних чи особистих переконань. Понад те, оскільки посвідчення особи використовується у повсякденному житті, воно *de facto* є документом, що вимагає від заявника розкривати дані про свої релігійні переконання проти його волі щоразу, коли цей документ використовується. З цих міркувань, ЄСПЛ визнав порушення ст. 9 ЄКПЛ, повторивши, що свобода сповідувати свою релігію або переконання також має негативний аспект, а саме право особи не бути зобов'язаною розголошувати свою релігію або діяти таким чином, щоб це було можливо зробити висновок, що він чи вона дотримуються, чи не дотримуються таких переконань. Попри те, що поле з релігією можна було залишити порожнім, сам факт його наявності має особливий підтекст, оскільки він неминуче дозволяє провести відмінність між носіями посвідчень особи, які містять дані про релігію, і тими, хто вирішив не вказувати ці дані (§§49-53) [155].

Крім того, питання свободи релігії та захисту персональних даних також було досліджено ЄСПЛ стосовно вимоги розкрити власні релігійні переконання у суді, щоб не складати релігійну присягу. Так, у справі *Alexandridis v. Greece* заявник, який був адвокатом у суді першої інстанції м. Афін, вимушений був під час складання присяги викрити свої релігійні переконання і вказати або те, що не належить до православних християн (§§38-41) [156]. Водночас справа *Dimitras and Others v. Greece* стосувалася складання присяги свідками у кримінальному провадженні. ЄСПЛ дійшов висновку, що положення національного законодавства, які передбачали, що з метою підтвердження своєї особи всі свідки повинні були, крім іншої інформації, вказати інформацію про віросповідання перед наданням показань, призвели до порушення права заявників на свободу віросповідання (§88) [157].

Також ЄСПЛ досліджував питання захисту персональних даних в аспекті реалізації свободи вираження поглядів. Однією з таких справ є справа *Biancardi v. Italy,* яка стосувалася притягнення журналіста до цивільної відповідальності за відмову деіндексувати, тобто заборонити видачу результату пошуку в пошуковій системі, опубліковану в Інтернеті статтю, що стосувалася чутливих даних про приватну особу, а

саме даних про відкрите кримінальне провадження. У цій справі ЄСПЛ в контексті так званого «права на забуття», тобто права вимагати видалення своїх даних, запропонував нові критерії для оцінки необхідності втручання у свободу вираження, які зводяться до наступного: 1) час, протягом якого стаття була розміщена в Інтернеті, особливо з урахуванням цілей, для яких персональні дані першочергово оброблялися, 2) чутливість таких персональних даних, 3) тяжкість накладених санкцій (§§64-71) [158]. На увагу заслуговують і висновки ЄСПЛ у справі *Centre for Democracy and the Rule of Law v. Ukraine*, яка стосувалася відмови Центральної виборчої комісії надати громадській організації-заявнику доступ до інформації про освіту та трудову діяльність лідерів політичних партій, яка містилася в їх автобіографіях, поданих ними під час парламентської виборчої кампанії, на тій підставі, що вона є конфіденційною та може бути оприлюднена в повному обсязі лише за згоди зацікавлених осіб. ЄСПЛ наголосив, що хоча запитувана інформація і становила персональні дані, оскільки стосувалася освіти та професійної діяльності політичних лідерів, але ці особи були доволі відомими громадськими діячами і подавши власні автобіографії під час національних парламентських виборів вони неминуче піддали свою кваліфікацію та документи ретельній перевірці з боку громадськості (§§115-121) [159].

Зазначимо, що ЄСПЛ відіграє важливу роль у визначенні обсягу змісту «персональних даних», тобто віднесенні певної інформації до категорії персональних даних, а також тлумаченні основоположних принципів захисту даних та прав суб'єкта даних. Крім того, у справах пов'язаних із захистом права на приватність і права на захист персональних даних ЄСПЛ наголошував, що приватне життя не підлягає вичерпному визначенню. У цьому аспекті вочевидь важливу роль відіграє *принцип автономних понять (або принцип автономного тлумачення)*. Згідно з цим принципом у певних випадках ЄСПЛ надає автономний зміст терміну, що використовується у ЄКПЛ, незалежно від його значення на національному рівні. Основним завданням принципу автономного тлумачення є досягнення першочергової мети ЄКПЛ, яка полягає у захисті прав особи від порушення державами-членами. Саме принцип автономного тлумачення допомагає тлумачити певні терміни у світлі об'єкта та мети відповідної статті ЄКПЛ, яка гарантує те чи інше право [160, с. 12-17]. Складність у застосуванні цього принципу в

аспекті захисту права на захист персональних даних полягає в тому, що це право, попри його визнання в рамках конвенційної системи у судових рішеннях ЄСПЛ, не закріплено безпосередньо в ЄКПЛ чи протоколах до неї. З огляду на те, що європейські стандарти захисту даних не закріплюють вичерпний перелік категорії «персональних даних» і держави мають право закріплювати на національному рівні власний перелік, тому ЄСПЛ цілком виправдано міг би застосовувати *принцип порівняльного тлумачення* у справах щодо захисту права на захист персональних даних, звертаючись до європейських стандартів у цій сфері та практики держав-членів РЄ.

Підсумовуючи, зазначимо, що право на захист персональних даних виникло у конвенційній системі внаслідок застосування ЄСПЛ доктрини еволюційного тлумачення до ст. 8 ЄКПЛ. Попри те, що це право безпосередньо пов'язане з правом на приватне життя, вочевидь ці два права є різними, що, зокрема, підтверджується тим, що право на захист персональних даних може стосуватися здійснення й інших гарантованих ЄКПЛ прав, як от права на свободу вираження чи права на свободу віросповідання. В аспекті еволюційного розвитку права на захист персональних даних в судовій практиці ЄСПЛ важливу роль відіграли доктрина доступності та передбаченості, доктрина свободи розсуду та доктрина позитивних та негативних зобов'язань держави. Крім того, вагоме значення для забезпечення реалізації права на захист персональних даних мають принцип правової визначеності та принцип неілюзорності прав та забезпечення їх практичності та ефективності.

2.3 Практика Європейського суду з прав людини щодо втручання в право на захист персональних даних

Безумовно вагому роль ЄСПЛ відіграє у тлумаченні основоположних категорій і принципів захисту персональних даних, а також прав суб'єкта даних. Саме завдяки судовій інтерпретації ключових принципів захисту персональних даних ЄСПЛ сприяє становленню, розвитку та ефективному впровадженню на практиці європейських стандартів захисту персональних даних.

Важливим в аспекті здійснення права на захист персональних даних є визначення категорії персональних даних. У своїх рішеннях ЄСПЛ неодноразово наголошував, що інтерпретація терміну «приватне життя», що використовується у статті 8 ЄКПЛ, має

відповідати Конвенції № 108, метою якої є захист прав людини, і, зокрема, права на приватність в контексті автоматичної обробки персональних даних. ЄСПЛ також чітко вказав, що з урахуванням ст. 2 Конвенції № 108 поняття персональних даних визначається як «будь-яка інформація, що стосується ідентифікованої особи або особи, що може бути ідентифікована» (Amann v. Switzerland, §65, Haralambie v. Romania, §77, та P. G. and J. H. v. the United Kingdom, §46) [115; 161; 162]. ЄСПЛ також підкреслював, що захист персональних даних має фундаментальне значення для здійснення особою права на повагу до приватного життя (Peck v. the United Kingdom, §78, Benedik v. Slovenia, §95) [140; 142].

Зауважимо, що з урахуванням європейських стандартів захисту даних найчастіше персональні дані поділяють на дві традиційні категорії – загальні та чутливі персональні дані. Цей поділ перш за все зумовлений необхідністю забезпечення підвищеного рівня захисту тих персональних даних, які стосуються більш інтимних сфер приватного життя особи, тобто чутливих персональних даних. Втім, зважаючи на те, що Конвенція № 108 вказує на невичерпний характер поняття персональних даних у своїй прецедентній практиці ЄСПЛ також дотримується такої позиції, що дозволяє йому тлумачити ЄКПЛ в умовах сьогодення і, відповідно, адаптувати термін «персональні дані» до сучасних реалій, розширюючи його сферу не лише на категорії персональні дані у їх традиційному розумінні, але й на так звані «нові» категорії даних, що виникають із розвитком інформаційного суспільства.

У своїх рішеннях ЄСПЛ неодноразово розглядав питання щодо захисту традиційних категорій персональних даних, до яких відносять, зокрема, дані про ім’я, по батькові та прізвище особи (Garnaga v. Ukraine, §36, Bulgakov v. Ukraine, §42), дані про дату і місце народження чи дитинство особи (Odièvre v. France, §§28-29), дані про місце проживання (Alkaya v. Turkey, §30) чи зображення особи (Von Hannover v. Germany (no. 2) [GC], §§95-99, Antović and Mirković v. Montenegro, §§ 40-45, 55) [116; 117; 120; 163-165].

Технологічний розвиток та активне використання Інтернету зумовило розширення категорії загальних персональних даних та включення до неї й інших даних, які можуть призвести до ідентифікації особи, до яких входять, зокрема: зразки голосу (P.

G. and J. H. v. the United Kingdom, §59), дані про користувача Інтернету, серед іншого, IP адреса (Benedik v. Slovenia, §§108-109), дані, що обробляються провайдерами телекомунікаційних послуг, наприклад, щодо реєстрації користувачів мобільних SIM карт (Breyer v. Germany, §80), дані про зайняття певним видом діяльності або участі у певних організаціях (Khelili v. Switzerland, § 56, Association "21 December 1989" and Others v. Romania, §§ 161-168), дані про особу, отримані з банківських документів (M. N. and Others v. San Marino, §51; G. S. B. v. Switzerland, § 51; Brito Ferrinho Bexiga Villa-Nova v. Portugal, §42), інформація про спортсменів, зокрема дані про місцеперебування та щоденні заняття, навіть у вихідні дні, зібрана у рамках державних антидопінгових заходів у спорті (National Federation of Sportspersons' Associations and Unions (FNASS) and Others v. France, §§ 155-159) [142; 162; 163; 166-172].

При визначенні того, чи мало місце порушення захисту персональних даних ЄСПЛ наголошував, що опублікована інформація про особу має бути деталізована настільки, щоб уможливити ідентифікацію особи [173]. У цьому аспекті на увагу заслуговують висновки ЄСПЛ у справі *L. B. v. Hungary*, яка стосувалася публікації на сайті національного податкового та митного органу персональних даних заявника у списку боржників, зокрема його імені, адреси, податкового номера та суми несплачених податків. Перш за все ЄСПЛ дійшов висновку, що публікація інформації щодо виконання податкових зобов'язань з огляду на потенційний вплив на ведення бізнесу та функціонування економіки переслідувала законну мету і була предметом публічного інтересу. ЄСПЛ також звернув увагу, що в контексті дотримання принципів захисту персональних даних, тривалість обробки не була надмірною, оскільки дані видаляли з сайту одразу після сплати податкових зобов'язань. Крім того, ЄСПЛ проаналізував чи достатньою була сукупність ідентифікаторів вказаних на сайті та дійшов висновку, що публікація імені та прізвища особи була б не достатньою для розрізнення платників податків від інших осіб з подібними даними, а тому виникала необхідність у публікації додаткових персональних даних (§§51-52) [174]. Варто зауважити, що 9 березня 2023 року Велика Палата ЄСПЛ ухвалила остаточне рішення за результатами розгляду справи *L. B. v Hungary* та дійшла протилежного висновку, встановивши порушення статті 8 ЄКПЛ через відсутність оцінки необхідності оприлюднення домашньої адреси заявника,

а також з огляду на те, що, попри певну свободу розсуду, законодавча влада не вжила всіх заходів для розробки належних адаптованих відповідей у світлі принципу мінімізації даних. Понад те, Велика Палата ЄСПЛ сформулювала критерії, які мають бути враховані при публікації персональних даних, а саме: 1) суспільний інтерес у поширенні інформації, 2) характер розкритої інформації та чи вона стосувалася найінтимніших аспектів особистості, як от стан здоров'я, відношення до релігії чи сексуальна орієнтація, 3) наслідки публікації для приватного життя заявника, такі як наступне відчуття незахищеності, публічне приниження та відсторонення від суспільного, і можливі перешкоди для ведення заявником нормального способу життя, 4) тип носія (матеріальний носій чи Інтернет), який використовується для розкриття відповідних даних, 5) ключові принципи захисту персональних даних (§§118-128, 139) [175].

Водночас у справі *Kırdök and Others v. Turkey* ЄСПЛ встановив порушення ст. 8 ЄКПЛ з огляду на відмову державних органів у поверненні або знищенні копії електронних даних, вилучених в юридичній фірмі в рамках розслідування, порушеного проти третьої особи, які мали статус адвокатської таємниці, хоч такі дані не були розшифровані, переписані чи офіційно прив'язані до заявників (§36) [176].

Що стосується категорій чутливих персональних даних, обробка яких здійснюється в особливому порядку, то ЄСПЛ неодноразово наголошував у своїх рішеннях, що варто проявляти особливу ретельність при вирішенні питань, які, хоча і опосередковано, стосуються розкриття чутливих даних (Rodina v. Latvia, §112) [177]. Зауважимо, що до категорії чутливих персональних даних відносяться, серед іншого:

- біометричні або генетичні дані, зокрема, зразки клітин, ДНК профілі та відбитки пальців (S. and Marper v. the United Kingdom), зразки слини (Dragan Petrovic v. Serbia), відбитки долонь (P. N. v. Germany), зразки голосу (Wisse v. France, Doerga v. the Netherlands), біологічні зразки (Aycaguer v. France);

- дані про расове або етнічне походження (Ciubotaru v. Moldova);

- політичні, релігійні або світоглядні переконання (Sinan Işık v. Turkey щодо внесення даних про релігію в посвідчення особи, Catt v. the United Kingdom щодо політичних переконань заявника, який брав участь у протесті);

- членство в політичних партіях та професійних спілках (Segerstedt-Wiberg and Others v. Sweden);

- дані засудження до кримінального покарання (Gardel v. France, Catt v. the United Kingdom);

- дані, що стосуються здоров'я (M. S. v. Sweden щодо поширення медичних даних про проведений аборт, Armonas v. Lithuania та Biriuk v. Lithuania щодо поширення в пресі даних про ВІЛ позитивний статус заявників);

- дані щодо статевого життя чи сексуальної орієнтації (P. and S. v. Poland та Delcour v. France);

- дані щодо делікатних родинних взаємовідносин (Rodina v. Latvia) [178, с. 12-14].

Вищезгадані категорії даних розкривають найбільш інтимні сфери приватного життя, а відтак їх обробка має бути чітко визначеною законом, виключно необхідною за конкретних обставин та пропорційною. У цьому аспекті погоджуємося із М. В. Бемом та І. М. Городиським, які стверджують, що обробка чутливих персональних даних має здійснюватися лише в особливих випадках з одночасним забезпеченням найвищих стандартів як захисту, так і дотримання прав суб'єктів персональних даних, адже ці категорії даних містять чутливу інформацію, що може мати наслідком дискримінаційне ставлення до відповідних суб'єктів даних [88, с. 22]. Такий підхід відображений і у судовій практиці ЄСПЛ, зокрема, у справі *S. and Marper v. the United Kingdom* було наголошено, що: «*Дані викликають особливе занепокоєння, якщо вони можуть призвести до встановлення етнічного чи іншого походження людини, беручи до уваги швидкі темпи розвитку в області генетики та інформаційних технологій*». Заразом біометричні та генетичні дані містять унікальну інформацію про відповідну особу та дозволяють її/його точну ідентифікацію за доволі широкого кола обставин, дозволяють встановлювати генетичні зв'язки між окремими особами та оцінювати їх ймовірне етнічне походження (§§71-85) [119]. Водночас на увагу заслуговують висновки у справі *Willems v. the Netherlands* щодо обов'язку заявника надати під час оформлення нового паспорту біометричні дані (відбитки пальців), які мали бути оцифровані та збережені в його паспорті та у відповідній базі даних. ЄСПЛ визнав, що обов'язок надати відбитки пальців при оформленні нового паспорту переслідував законну мету та був необхідним

у демократичному суспільстві, оскільки він спрямований на дотримання відповідного права ЄС і забезпечення загального публічного інтересу (§§22-23) [179]. Відповідно, у цій справі публічні інтереси переважали над правами і інтересами заявника щодо відмови у розголошенні чутливих персональних даних.

Наголосимо, що у своїй практиці ЄСПЛ також розмежовує дані, про ідентифіковану особу, та дані, які можуть призвести до ідентифікації особи. Так, ЄСПЛ розглянув це питання у справі *Cakicisoy and Others v. Cyprus*, що стосувалася ситуації, коли органи влади взяли зразки крові у заявників, щоб отримати їх ДНК профіль для програми ексгумації з метою ідентифікації останків їхніх померлих родичів. ЄСПЛ звернув увагу на той факт, що ці зразки були знищені після закінчення терміну дії згоди на обробку, а тому такі дії не мали наслідком втручання у право заявників на повагу до їхнього приватного життя (§§50-52) [180]. Протилежних висновків дійшов у справі *Mehmedovic v. Switzerland*, яка стосувалася розслідування, проведеного щодо заявника приватною страховою фірмою, яке містило частину даних, що стосувалися заявниці. ЄСПЛ звернув увагу, що невелика частина даних щодо заявниці, яка була зібрана випадково і не мала значення для розслідування, жодним чином не становила систематичний або постійний збір даних. До того ж за допомогою цих даних заявницю було важко ідентифікувати й можна було лише частково впізнати, а відтак збір даних щодо заявниці не призвів до порушення статті 8 ЄКПЛ (§§4, 18) [181].

Підсумовуючи, зазначимо, що ЄСПЛ оцінює кожну конкретну справу крізь призму європейських стандартів захисту персональних даних, встановлюючи чи мала місце обробка персональних даних та одночасно застосовуючи «трискладовий тест» для вирішення того чи було втручання в право на захист персональних даних виправданим, тобто чи відповідало втручання закону, чи переслідувало воно законну мету і, чи було воно необхідним для досягнення цієї мети.

Доволі часто на практиці питання захисту персональних даних виникають і у ситуаціях, коли органи влади правомірно обробляють персональні дані. ЄСПЛ наголошував, що попри те, що в рамках кримінального розслідування органи влади можуть правомірно збирати та обробляти персональні дані про особу, але при інформуванні громадськості про хід кримінального провадження органи влади повинні

бути вкрай обережними. У справі *Khadija Ismayilova v. Azerbaijan* ЄСПЛ дійшов висновку, що розкриття органами прокуратури персональних даних заявниці, професійної журналістки, у пресрелізі, в якому викладено звіт про хід кримінального розслідування мало наслідком порушення ст. 8 ЄКПЛ. У своєму звіті органи влади вказали інформацію про заявницю, включаючи чутливі приватні деталі життя заявниці, такі як її адресу, інформацію про особу її хлопця, його повне ім'я та рід занять, а також повні імена її орендодавця, членів сім'ї, імена та рід занять її друзів і колег. Крім того, звіт містив інформацію про осіб, яким заявниця здавала квартиру в суборенду і деталі фінансових домовленостей між ними (§§ 142-150) [182]. Відповідно, з огляду на висновки у цій справи, можна стверджувати, що органи влади мають бути вкрай обережними при інформуванні громадськості та вживати заходів для захисту персональних даних про особу.

Що стосується тлумачення терміну «суб'єкт даних» зауважимо, що основні міжнародно-правові акти у сфері захисту персональних даних поширюють свої положення на захист даних приватних осіб, але ЄСПЛ сформував дещо інший підхід у цьому аспекті. ЄСПЛ визнає, що гарантії захисут персональних даних можуть поширюватися на юридичних осіб у разі, якщо їх права прямо порушуються внаслідок запровадження певних заходів всупереч гарантіям статті 8 ЄКПЛ. ЄСПЛ досліджував це питання, наприклад, у справі *Bernh Larsen Holding AS and Others v. Norway*, коли податковий орган зобов'язав компанію-заявника надати копію всіх даних з комп'ютерного сервера, яким ця компанія ділилася з іншими компаніями (також заявниками). У цій справі ЄСПЛ не встановив порушення ст. 8 ЄКПЛ, зазначивши, що процедура обробки даних супроводжувалася дієвими та адекватними гарантіями: 1) заявника заздалегідь повідомили про можливу податкову перевірку; 2) представники заявників були присутні та могли негайно заперечити проти втручання; 3) резервна копія даних була запечатана та могла бути відкрита лише у присутності заявників; 4) після завершення податкової перевірки всі дані та сліди її змісту підлягали знищенню (§§126-134) [183]. У цьому аспекті прикладом може слугувати також справа *Liberty and Others v. the United Kingdom*, яка стосувалася перехоплення Міністерством оборони комунікацій неурядових організацій, що займаються захистом громадянських свобод

(§§56-57) [184]. Крім того, це питання ЄСПЛ досліджував у справі *Satakunnan Markkinapörssi Oy and Satamedia Oy v. Finland*, що стосувалася заборони компаніям-заявникам здійснювати обробку персональних даних щодо оподаткування, отриманих з публічних джерел (§138) [185].

Примітно, що розвиток технологій призводить і до збільшення видів операцій з персональними даними, які становлять їх обробку у розумінні Конвенції № 108, а відтак у своїх рішеннях ЄСПЛ інтерпретує види обробки даних, якими є, зокрема:

- збирання та зберігання органами влади публічної інформації про особу, наприклад, про її політичну діяльність (Association "21 December 1989" and Others v. Romania, Catt v. the United Kingdom) [168; 186];
- збирання даних за допомогою різних методів таємного спостереження, серед іншого, перехоплення комунікацій (Klass and Others v. Germany, Ekimdzhiev and Others v. Bulgaria), прослуховування телефону (Kopp v. Switzerland), відеонагляд (Köpke v. Germany, Hambardzumyan v. Armenia), GPS трекінг (Uzun v. Germany, Ben Faiza v. France), використання технології розпізнавання обличчя (Glukin v. Russia) [141; 187-193];
- внесення даних про особу до поліцейських реєстрів (Khelili v. Switzerland, Dmitrov-Kazakov v. Bulgaria, Shimovolos v. Russia) [167; 194; 195];
- зберігання даних про особу в національних базах (Gardel v. France) та використання персональних даних з таких баз (M. D. and Others v. Spain) [196; 197];
- поширення даних журналістам та публікація цих даних у пресі (Biriuk v. Lithuania, Hájovský v. Slovakia) [198; 199];
- збирання персональних даних на робочому місці (Antović and Mirković v. Montenegro, López Ribalda and Others v. Spain) [200; 201];
- використання чи відтворення персональних даних у суді (L. L. v. France, Surikov v. Ukraine) [152; 154].

У своїх рішеннях ЄСПЛ також зважає на застосування ключових принципів захисту персональних даних, викладених у ст. 5 Конвенції № 108. Одним з принципів, що відіграє вагому роль у забезпеченні захисту персональних даних, є принцип

законності, тобто наявність передбачених законом підстав для обробки даних, що відповідає встановленій у частині 2 статті 8 ЄКПЛ вимозі «відповідно до закону». Враховуючи усталену практику ЄСПЛ втручання в права особи буде виправданим якщо воно здійснюється «згідно з законом», а сам закон має бути доступним і передбачуваним. Так, у справі *Rotaru v. Romania* ЄСПЛ дійшов висновку, що національне законодавство не було достатньо чітким і передбачуваним, адже не містило чітких положень щодо обмеження повноважень органів служби безпеки, не визначало вид інформації, який можуть збирати і категорії осіб щодо яких можуть бути зібрані дані, а також не встановлювало обмежень щодо строку давності інформації чи тривалості її зберігання (§§57-62) [126]. Водночас у справі *Benedik v. Slovenia* ЄСПЛ наголосив, що національний закон, який дозволяв поліції отримати інформацію про абонента, включаючи динамічну IP-адресу, та спосіб, у який він був застосований національними судами, не були чіткими та не пропонували достатні гарантії від свавільного втручання права статті 8 ЄКПЛ (§132) [142]. У цьому аспекті звернемо увагу також на висновки ЄСПЛ у справі *Mockutė v. Lithuania*, де було наголошено, що втручання в права заявниці не було законним, оскільки ані Уряд, ані національні суди не вказали жодного положення національного законодавства, яке могло б стати юридичною основою для передачі психіатричною лікарнею даних про здоров'я, сексуальне життя та переконання заявниці її матері та журналістам (§§103-104) [202]. Водночас порушення принципу законності було визнано й у справі *Vasil Vasilev v. Bulgaria*, оскільки у цій справі органи влади використали інструкцію, видану для внутрішнього користування органами прокуратури, яка була недоступною для заявника та не була достатньо чіткою (§§93-94) [203]. На додаток до вимоги законності, обробка персональних даних повинна бути справедливою і прозорою. Ці вимоги, серед іншого, стосуються й забезпечення доступу суб'єкта даних до його персональних даних. ЄСПЛ наголошував, що вимога прозорості може бути менш суворою в контексті інформації, яка є важливою для національної безпеки (Leander v. Sweden, §51) [114]. Втім, у справі *Haralambie v. Romania* ЄСПЛ дійшов висновку про порушення прав заявника, оскільки останній понад 5 років не міг отримати доступ до досьє про нього, яке було зібране колишніми спецслужбами за тоталітарних режимів і зберігалося в державних архівах (§97) [161].

У низці справ ЄСПЛ досліджував питання дотримання вимоги, зазначеної у ст. 5 Конвенції № 108, що персональні дані, які підлягають автоматичній обробці, повинні бути зібрані для явних, визначених і законних цілей. Зауважимо, що перелік законних цілей, які можуть виправдати втручання у здійснення прав за ст. 8 ЄКПЛ, перерахований у пункті 2 цієї статті та є досить стислим та включає захист національної та громадської безпеки чи економічного добробуту країни, запобігання заворушенням чи злочинам, захисту здоров'я чи моралі або захисту прав інших осіб. Примітно, що однією із законних цілей є захист прав інших осіб і у цьому аспекті ЄСПЛ неодноразово наголошував, що ключовим є забезпечення балансу конкуруючих прав. Найчастіше питання забезпечення балансу виникає щодо співвідношення права на захист персональних даних та права на свободу вираження поглядів та передання інформації. У цій сфері ЄСПЛ напрацював критерії, яких варто дотримуватися при оприлюдненні публікацій аби не порушувати основні стандарти захисту даних, включаючи внесок у дискусію, що становлять суспільний інтерес; ступінь відомості особи та тема новини; попередня поведінка відповідної особи; зміст, форма та наслідки публікації, а також спосіб і обставини, за яких інформація була отримана (Von Hannover v. Germany (no. 2), §§108-113) [120]. Слід звернути увагу й на нещодавню справу *Biancardi v. Italy* щодо відповідальності заявника-журналіста за відмову деіндексувати теги, пов'язані з опублікованою в Інтернеті статтею, в якій йшлося про конфіденційні дані приватної особи, пов'язані з відкритим кримінальним провадженням. ЄСПЛ зазначив, що ця конкретна справа відрізняється від попередньої судової практики, оскільки стосується не змісту публікації чи способу її опублікування – з анонімізацією чи без неї – а саме не виконання обов'язку деіндексувати її. У цьому випадку ЄСПЛ у контексті права суб'єкта даних вимагати видалення своїх персональних даних, так званого «права бути забутим», запропонував нові критерії оцінки необхідності втручання у свободу вираження поглядів, які включають наступне: 1) час, коли стаття зберігалася в Інтернеті, особливо з огляду на цілі, для яких персональні дані оброблялися спочатку, 2) конфіденційність таких даних, 3) суворість накладених санкцій (§§64-71) [158].

Примітно, що у своїх рішеннях ЄСПЛ також дійшов висновків, що важливо обмежувати використання персональних даних тією метою, для якої вони були зібрані.

Зокрема у справі *Karabeyoğlu v. Turkey* було визнано порушення ст. 8 ЄКПЛ оскільки використання в дисциплінарному розслідуванні даних, отриманих від прослуховування телефону заявника в рамках кримінального розслідування, відбувалося з метою, відмінною від тієї, яка виправдовувала їх збір (§§112-121) [204]. Важливою у цьому аспекті є справа *Peck v. the United Kingdom*, в якій ЄСПЛ зауважив, що спостереження за діями певної особи в громадському місці з метою безпеки та використання записів таких дій в інших цілях, а саме оприлюднення записів про переміщення заявника для громадськості, виходять за межі того, що відповідна особа могла очікувати, а відтак мають наслідком порушення ст. 8 ЄКПЛ (§§59-62) [140]. Подібних висновків ЄСПЛ дійшов у справі *P. G. and J. H. v. the United Kingdom*, в якій запис голосів заявників, який першочергово було зроблено, коли вони відповідали на запитання в поліцейській камері, був використаний для подальшого аналізу зразків їх голосів, а відтак становив обробку персональних даних заявників, що є втручанням у їхнє право на повагу до приватного життя (§§59-60) [162].

У своїх рішеннях ЄСПЛ також наголошував, що склад і зміст персональних даних, що обробляються, повинні бути адекватними, відповідними та ненадмірними стосовно цілей, для яких вони обробляються, що корелює з положеннями статті 5 Конвенції № 108 та відповідає сформульованому ЄСПЛ принципу пропорційності. Зокрема, це питання було досліджено у справі *L. H. v. Latvia*, що стосувалася збирання та обробки медичних даних заявниці, якій незаконно провели кесарів розтин, під час розслідування цього інциденту інспекцією з контролю якості медичних послуг. ЄСПЛ відзначив, що інспекція здійснила збір непропорційно великого обсягу медичних даних заявниці за період тривалістю семи років, що включав рік до та шість років після проведення операції. Водночас збір і обробка медичних даних заявниці відбувалися без її згоди та без належного обґрунтування. Відтак ЄСПЛ дійшов висновку, що інспекція збирала медичні дані заявниці невибірково, без попередньої оцінки того, чи будуть зібрані дані «потенційно вирішальними», «відповідними» чи «важливими» (§§51, 58) [118]. Водночас у справі *P. N. v. Germany* ЄСПЛ не встановив порушення статті 8 ЄКПЛ щодо збору ідентифікаційних даних на вимогу поліції після відкриття нового кримінального провадження проти особи, яка була раніше засуджена. Зокрема, передбачався збір

детальних фотографій обличчя та тіла, включаючи можливі татуювання, разом із відбитками пальців та долонь, а також складення опису особи заявника і включення його в поліцейську базу для подальшої ідентифікації. ЄСПЛ дійшов висновку, що збирання та зберігання вказаних даних заявника мало відносно ненав'язливий характер втручання, ніж, наприклад, збирання зразків клітин чи ДНК профілів, які містять більш чутливу інформацію. Крім того, органи влади чітко встановили тривалість збору ідентифікаційних даних, про які йдеться. Таким чином, зважаючи на обмежений вплив зберігання даних на повсякденне життя заявника, видалення цих даних через п'ять років, а також той факт, що дані зберігалися в базі даних поліції, що передбачала відповідні гарантії захисту та індивідуальний перегляд щодо необхідності подальшого зберігання даних, оскаржуваний захід становив пропорційне втручання в право заявника на повагу до його приватного життя (§§76-91) [205].

ЄСПЛ також систематично розглядає справи, які стосуються дотримання принципу точності та оновлення даних, які охоплюють як випадки зберігання органами влади даних, які виявилися неточними або точність яких оскаржується суб'єктом даних, як от справа *Rotaru v. Romania* [126], так і випадки збирання та збереження органами влади неправдивих або неповних персональних даних як у справі *Khelili v. Switzerland* [167]. У цьому аспекті ЄСПЛ наголошував, що саме на органи влади покладений обов'язок довести точність персональних даних, що зберігаються, а також забезпечити оновлення таких даних за необхідності.

Наголосимо також на важливості дотримання принципу обмеження строків зберігання персональних даних. Тлумачення цього принципу у справах, що стосувалося даних про засуджених осіб, було проаналізовано у справах *Gaugraham v. the United Kingdom* (§96) [206] та *Trajkovski and Chipovski v. North Macedonia* (§56) [207], в яких ЄСПЛ наголосив, що через загальний та невибірковий характер повноважень органів влади щодо збереження профілю ДНК, відбитків пальців і фотографії засуджених без посилання на серйозність злочину чи необхідність такого безперервного зберігання у поєднанні з відсутністю достатніх гарантій, доступних для заявників, не забезпечує досягнення справедливого балансу між конкуруючими державними та приватними інтересами. Втім, ЄСПЛ зауважив у справі *Ayçaguer v. France*, що відсутність

максимального терміну зберігання персональних даних не обов'язково є несумісною зі ст. 8 ЄКПЛ, наприклад, у разі якщо національне законодавство містить гарантії, що такі дані є відповідними та не надмірними щодо цілей, для яких вони зберігаються, і зберігаються у формі, яка дозволяє ідентифікувати суб'єктів даних не довше, ніж це необхідно для цілей зберігання цих даних (§38) [208].

Таким чином, задля забезпечення й гарантування права на захист персональних даних в епоху нових загроз та викликів цифрової ери ЄСПЛ оцінює обставини кожної справи у світлі керівних принципів захисту персональних даних, що втілені перш за все в Конвенції № 108. Новітні технологічні зміни породжують все більш технологічно складні справи, що спонукає ЄСПЛ адаптувати свої попередні критерії до конкретних випадків і ретельно перевіряти свої підходи з огляду на європейські стандарти захисту даних, водночас забезпечуючи пропорційний баланс між конкуруючими основоположними правами, без неправомірного втручання в саму суть цих прав. Варто наголосити, що визнання права на захист персональних даних та його окремих аспектів, як-от права на доступ до персональних даних, права заперечити проти їх обробки чи вимагати виправлення або видалення даних, у конвенційній системі як самостійного права, передбаченого безпосередньо в окремому протоколі до ЄКПЛ, забезпечили б вищий ступінь його захисту та сприяло б мінімізації практичних проблем, пов'язаних із захистом персональних даних.

Висновки до Розділу 2

Дослідження правових засад регулювання захисту персональних даних у РЄ та особливостей їх у судовій практиці ЄСПЛ дають підстави зробити такі висновки.

Визначальну роль в утвердженні захисту персональних даних як основоположного права людини відіграла договірна практика РЄ, зокрема прийняття Конвенції № 108, а також норм рекомендаційного характеру, судова практика ЄСПЛ, які сприяли становленню та розвитку права на захист персональних даних. Положення Конвенції № 108 не були призначені для прямого застосування, контролю ЄСПЛ у рамках конвенційної системи. Однак, ЄСПЛ у низці справ постановив, що захист персональних даних має «фундаментальне значення» для реалізації людиною права на

повагу до приватного життя відповідно до статті 8 ЄКПЛ і вивів з Конвенції № 108 критерії для визначення ступеня порушення цього права, а також необхідні гарантії для його захисту.

У рамках конвенційної системи право на захист персональних даних сформувалося внаслідок застосування ЄСПЛ доктрини еволюційного тлумачення до ст. 8 ЄКПЛ, яка гарантує право на захист приватного життя. Втім, попри високий ступінь взаємозв'язку право на захист приватного життя та право на захист персональних даних не є тотожними. З аналізу судової практики ЄСПЛ випливає, що задля забезпечення і дотримання права на захист персональних даних за притаманних інформаційному суспільству новітніх загроз і викликів цифрової ери, ЄСПЛ оцінює обставини кожної справи у світлі керівних принципів захисту персональних даних, насамперед закріплених у Конвенції № 108.

При вирішенні справ, пов'язаних із захистом персональних даних, ЄСПЛ використовує: 1) доктрину доступності та передбачуваності, що дозволяє оцінити передбачуваність, доступність, точність та ясність законодавства у сфері захисту даних, 2) доктрину позитивних та негативних зобов'язань задля оцінки їх виконання державою у контексті гарантування права на захист персональних даних, а також 3) доктрину свободи розсуду, щоб оцінити свободу дій держави щодо виконання взятих зобов'язань за ЄКПЛ у контексті захисту персональних даних.

Доктрина еволюційного тлумачення та доктрина свободи розсуду дозволяють ЄСПЛ розглядати дедалі складніші та технологічно-новітні справи щодо захисту персональних даних, надаючи розширене тлумачення терміну персональних даних, а також, у конкретних випадках, вирішуючи питання про обсяг прав суб'єкта даних.

Вагоме значення для забезпечення реалізації права на захист персональних даних мають принцип правової визначеності та принцип неілюзорності прав та забезпечення їх практичності та ефективності, які ЄСПЛ застосовує у цій категорії справ. Не менш важливими є принцип пропорційності, який використовується для забезпечення рівноваги інтересів, а також принципи автономного та порівняльного тлумачення понять, які можуть застосовуватися для тлумачення європейських стандартів захисту персональних даних.

Переважна більшість підходів ЄСПЛ щодо захисту персональних даних сформовані та викладені саме в рамках розгляду порушень за ст. 8 ЄКПЛ, яка гарантує право на повагу до приватного життя. Втім, питання захисту персональних даних є більш широкими та можуть стосуватися здійснення й інших конвенційних прав і свобод, зокрема права на справедливий суд, права на свободу думки, совісті та релігії чи права на свободу вираження поглядів. У цьому контексті ЄСПЛ зазвичай використовує принцип пропорційності для забезпечення належного балансу прав та інтересів. Юридична визначеність, доступність і передбачуваність національного законодавства у сфері захисту персональних даних у поєднанні з відносно невеликою свободою дій держави, здатні забезпечити послідовний та ефективний захист персональних даних. Водночас у разі, якщо свобода дій держави є широкою, законодавство повинно передбачати належні гарантії для суб'єкта даних від свавільної поведінки органів влади, наділених широкими повноваженнями щодо збору та обробки даних.

Зважаючи на багатогранність захисту персональних даних, а також далекосяжні наслідки впливу інформаційних технологій на права людини, існує необхідність у гарантуванні права на захист персональних даних як самостійного права, шляхом прийняття окремого протоколу до ЄКПЛ, що забезпечило б належний захист таких аспектів права на захист персональних даних як право на забуття, право на заперечення проти обробки чи права на мобільність даних. Ця необхідність зумовлена тим, що Конвенція № 108 не передбачає створення самостійного контрольного механізму для захисту гарантованого нею права на захист персональних даних. Водночас у рамках конвенційної системи це право розглядається крізь призму статті 8 ЄКПЛ, що не повною мірою забезпечує достатній рівень захисту суб'єкта даних та його основних прав, зокрема права на забуття чи права на мобільність даних, оскільки ці питання можуть залишатися поза увагою ЄСПЛ при розгляді справ за статтею 8 ЄКПЛ.

РОЗДІЛ 3. ЗАХИСТ ПЕРСОНАЛЬНИХ ДАНИХ У СУДІ ЄВРОПЕЙСЬКОГО СОЮЗУ

3.1 Право на захист персональних даних у джерелах первинного та вторинного права Європейського Союзу

Європейський Союз заснований насамперед як наднаціональне, економічне та політичне інтеграційне співтовариство встановлює самобутній правовий порядок. Повага та забезпечення захисту прав людини є одним з провідних напрямків діяльності ЄС відповідно до мети та принципів організації, закріплених в установчих договорах, однак на початкових етапах свого розвитку Європейське економічне співтовариство не приділяло особливої уваги правам людини, концентруючись перш за все на цілях економічної інтеграції. Вочевидь основною причиною того, що на ранніх етапах свого існування ЄС спрямовувався на захист економічних прав є панування на той час ідеології «ринкової людини» [209, с. 187]. Поступово у Європі почали формуватися дві незалежні системи захисту прав людини – в рамках діяльності РЄ та ЄС. Щоправда, захист прав людини в ЄС тривалий час залишався дещо фрагментарним. У цьому аспекті Л. Г. Фалалєєва зауважує, що на практиці європейські співтовариства намагалися уникнути дублювання функцій РЄ, а тому з осторогою ставилися до включення прав людини до категорії, що підлягає захисту в судовому порядку. Однак утвердження прав людини в національному законодавстві та правозастосовній практиці держав-членів ЄС стали тими об’єктивними факторами, що суттєво вплинули на включення основоположних прав правопорядку ЄС, зокрема у преамбулі Єдиного європейського акту 1986 р., а також сприяло подальшому прийняттю Декларації основоположних прав і свобод 1989 р. та Хартії Співтовариства про основоположні соціальні права працівників 1989 р. Водночас прийняття Договору про Європейський Союз 1992 р. (далі – ДЄС) ознаменувало новий етап еволюції системи захисту прав людини в ЄС та закріплення юридично обов’язкового принципу поваги до прав людини і закріплення важливих гарантій захисту основоположних прав як засадничих цінностей діяльності ЄС [90, с. 74-76].

Захист персональних даних як одне з основоположних прав людини сьогодні гарантується ефективним поєднанням різних правових інструментів ЄС, зокрема установчих договорів ЄС і Хартії ЄС та актів вторинного права ЄС. Аналізуючи виникнення та гарантування права на захист персональних даних у правовому порядку ЄС, необхідно звернути увагу на установчі договори ЄС. Вагому роль у розвитку захисту прав людини в ЄС відіграло укладення Лісабонського договору 2007 р., який вніс зміни в установчі договори ЄС. Як наслідок, право на захист персональних даних було закріплено у ст. 16 ДФЄС, яка гарантує право кожного на захист персональних даних. Водночас ст. 16 ДФЄС, як і ст. 39 ДЄС, передбачає право Європейського Парламенту та Ради встановлювати правила обробки персональних даних установами, органами та агентствами ЄС і державами-членами ЄС при здійсненні ними діяльності, що підпадає під сферу права ЄС, а також правила, що стосуються вільного переміщення таких даних. Крім того, ст. 16 ДФЄС наголошує також, що дотримання правил захисту даних має контролюватися незалежним органом [210]. Надання органам ЄС права врегулювання питання захисту персональних даних було юридичним кроком до впровадження підходу всебічного захисту персональних даних в ЄС, що охоплював би не лише питання забезпечення вільного руху даних в ЄС, але й поширювався б на всі інші компетенції ЄС, зокрема у сфері поліцейського та судового співробітництва.

Фундаментальне значення в царині гарантування основоположних прав в ЄС відіграла саме Хартія ЄС, проголошена як політична декларація у 2000 р., з набранням чинності Лісабонським договором у 2009 р. вона отримала таку ж юридичну силу, як і установчі договори ЄС. Стаття 7 Хартії ЄС гарантувала право кожної особи на повагу до приватного життя, але водночас ст. 8 Хартії ЄС проголосила право кожного на захист персональних даних, наголошуючи таким чином на статусі цього права як основоположного на рівні з іншими правами та вказуючи на існування відмінності між приватністю та захистом персональних даних. Разом з тим, у ст. 8 Хартії ЄС було проголошено й ключові вимоги, пов’язані із захистом персональних даних, відповідно до яких обробка даних повинна бути справедливою, переслідувати визначені цілі та здійснюватися на основі згоди особи або на основі іншої законної підстави, встановленої законом. Понад те, у ст. 8 Хартії ЄС було гарантовано також такі ключові права суб’єкта

даних, як право доступу до своїх персональних даних і право на їх виправлення, а також закріплено принцип контролю за дотриманням правил обробки даних з боку незалежного органу. Варто звернути увагу також на положення ст. 52 Хартії ЄС згідно з якими встановлюється принцип пропорційності втручання в гарантовані Хартією ЄС права, який наголошує на повазі до самої суті цих прав, а також передбачає, що обмеження прав людини можуть встановлюватися лише в тому випадку, якщо вони необхідні та справді відповідають цілям загального інтересу, визнаного ЄС, або потребі захисту прав інших осіб. Примітно, що у ст. 52 Хартії ЄС також визначено, що Хартія містить права, які відповідають правам, гарантованим ЄКПЛ, а тому значення та обсяг цих прав є такими ж, як і ті, які встановлені ЄКПЛ, що, однак, не забороняє праву ЄС надавати більш широкий захист [45]. Вочевидь, ст. 8 Хартії ЄС, яка гарантує право на захист персональних даних, не повною мірою корелює зі ст. 8 ЄКПЛ, яка не містить положень, що прямо гарантують це право. Така розбіжність пояснюється перш за все тим, що право на захист персональних даних сформувалося внаслідок застосування ЄСПЛ еволюційної теорії до ст. 8 ЄКПЛ. Втім, оскільки це право визнане у рамках конвенційної системи, тому обсяг гарантованого Хартією ЄС права на захист персональних даних має узгоджуватися з основним положенням ст. 8 ЄКПЛ та принципам, сформованим ЄСПЛ у цій сфері.

Все ж основний масив права ЄС у сфері захисту персональних даних складають регламенти, директиви та рішення ЄС, які є джерелами вторинного права ЄС. Ідея захисту персональних даних зародилася на внутрішньому ринку ЄС, але від початку була пронизана міркуваннями щодо забезпечення прав людини, що і вплинуло на її подальший розвиток. У відповідь на популяризацію автоматизованої обробки даних в рамках ЄС був прийнятий перший спеціалізований акт у цій сфері – Директива 95/46/ЄС, яка мала б сприяти реалізації цілей внутрішнього ринку шляхом прийняття кожною країною-членом ЄС закони про приватність, які є еквівалентними один одному, що сприяло б вільній передачі персональних даних через кордони ЄС [211]. Також зважаючи на необхідність забезпечення економічних інтересів та потреби у транскордонній передачі персональних даних була ухвалена Директива 97/66/ЄС Європейського Парламенту та Ради Про обробку персональних даних і захист прав осіб

у телекомунікаційному секторі 1997 р. Обидва документи деталізували положення Конвенції №108 та обмежували передачу персональних даних як до, так і з Європи до третіх країн, які не забезпечували адекватний рівень захисту персональних даних. Щоправда, міжнародні стандарти у цій сфері гарантували вільний обмін даними між країнами, які дотримуються європейського режиму захисту персональних даних. Також зауважимо, що Директива 97/66/ЄС значною мірою спиралася на здобутки РЄ щодо розробки рекомендації з цього ж питання, яка згодом була втілена у Рекомендації № R (95) 4 КМРЄ державам-членам щодо захисту персональних даних у сфері телекомунікаційних послуг, з особливою увагою до телефонних послуг.

Водночас варто звернути увагу на особливості співвідношення права на приватність та права на захист персональних даних, які з об'єктивних причин мають глибокий взаємозв'язок. Директива 95/46/ЄС, яка поширювалася на низку видів діяльності, пов'язаних з обробкою персональних даних як у державному, так і в приватному секторах, забезпечуючи таким чином широкий спектр захисту, була спрямована на гармонізацію права ЄС і сприяння вільному переміщенню даних в межах ЄС. Як наголошено в ст. 1 Директиви 95/46/ЄС її метою є захист основоположних прав людини та, особливо, їхнє право на невтручання у приватне життя при обробці персональних даних [42]. Відтак Директива 95/46/ЄС визначила персональні дані як один з аспектів права на приватність та розглядала інші основні права в їх цілісності. Все ж виклики цифрової ери, сучасний розвиток комунікаційної сфери, передові технології та інновації змінили уявлення про захист даних та поступово призвели до визнання його основоположним правом у рамках існуючої системи прав людини, що було закріплено у Хартії ЄС, яка вперше на законодавчому рівні закріпила основоположні права людини як основну цінність у правовому порядку ЄС. Одночасно такий підхід був відображений й у рішеннях Суду ЄС, ухвалених після прийняття Хартії ЄС, наприклад, у справі *Tele2 Sverige v. Post-och telestyrelsen and Secretary of State for the Home Department v. Tom Watson and Others* (далі – *Tele2 Sverige*), де було наголошено, що стаття 8 Хартії ЄС стосується основоположного права на захист даних, яке відрізняється від права, закріпленого у статті 7 Хартії ЄС, і яке не має еквіваленту в ЄКПЛ [212].

Важливим актом у сфері захисту персональних даних в ЄС став прийнятий 18 грудня 2000 р. Регламент 45/2001 Європейського Парламенту та Ради Про захист фізичних осіб при обробці персональних даних інститутами і органами Співтовариства і про вільне переміщення таких даних (далі – Регламент 45/2001). Найважливішим досягненням регламенту є запровадження незалежного контролюючого органу для моніторингу застосування його положень – Європейського інспектора із захисту персональних даних (ЄІЗПД), який, зокрема, уповноважений розглядати скарги суб'єкта даних щодо порушення його права на захист персональних даних. Зауважимо, що Регламент 45/2001 деталізує принципи обробки персональних даних, що містяться у Директиві 95/46/ЄС, адаптуючи їх до особливостей обробки даних інститутами і органами Співтовариства. Водночас стаття 6 дозволяє обробку персональних даних для цілей, відмінних від тих, для яких вони були зібрані, якщо зміна цілі прямо дозволена внутрішніми правилами інституту або органу Співтовариства. Крім того, Регламент 45/2001 передбачає можливість передачі персональних даних всередині або між інститутами і органами Співтовариства якщо дані необхідні для виконання передбачених законом завдань, що входять до компетенції одержувача даних (ст. 7). Крім того, у статтях 8 та 9 Регламенту 45/2001 передбачається можливість передачі даних іншим одержувачам, ніж інститутами і органи ЄС. Примітно, що згідно з Регламентом 45/2001 забороняється обробка персональних даних, що розкривають расове чи етнічне походження, політичні погляди, релігійні чи філософські переконання, членство в профспілках, а також даних про здоров'я чи статеве життя, за виключенням випадків, описаних у частині 2 статті 10, зокрема, у разі якщо отримано згоду суб'єкта даних, якщо обробка необхідна для виконання конкретних прав та обов'язків контролера у сфері трудового права відповідно до права ЄС, для захисту життєво важливих інтересів суб'єкта даних або якщо обробка стосується даних, які явно оприлюднюються суб'єктом даних, або необхідні для встановлення, здійснення чи захисту судових позовів [213].

Внаслідок впровадження нових передових цифрових технологій, використання мережі Інтернет для комунікації та обміну даними на глобальному рівні виникла потреба й у забезпеченні захисту приватності та персональних даних також у сфері надання електронних комунікаційних послуг. З огляду на це була розроблена та прийнята

Директива 2002/58/ЄС Європейського Парламенту та Ради Про обробку персональних даних та захисту приватності у секторі електронних комунікацій (Директива про приватність та електронні комунікації). Директива про приватність та електронні комунікації конкретизує та доповнює Директиву 95/46/ЄС задля виконання своєї мети, що полягає у забезпеченні вільного руху персональних даних, включно з даними про трафік та місцезнаходження, та електронного комунікаційного обладнання і послуг у Співтоваристві. Крім того, Директива про приватність та електронні комунікації забезпечує захист законних інтересів абонентів, які є юридичними особами [214]. Таким чином, Директива про приватність та електронні комунікації є *lex specialis* щодо Директиви 95/46/ЄС, яка є *lex generalis*, оскільки з одного боку Директива про приватність та електронні комунікації гарантує право на захист персональних даних абонентів, коли вони користуються електронними комунікаційними послугами, і водночас накладає обмеження на постачальників загальнодоступних електронних комунікаційних послуг щодо відстеження в режимі онлайн (online tracking) та надсилання небажаних повідомлень.

Зауважимо, що у 2009 р. Директива про приватність та електронні комунікації була оновлена Директивою 2009/136/ЄС Європейського Парламенту та Ради про внесення змін до Директиви 2002/22/ЄС про універсальні послуги та права користувачів, що стосуються мереж та послуг електронних комунікацій, Директиви 2002/58/ЄС щодо обробки персональних даних та захист приватності в секторі електронних комунікацій та Регламенту 2006/2004 про співробітництво між національними органами, відповідальними за виконання законів про захист прав споживачів (далі – Директива 2009/136/ЄС). Зважаючи на те, що термінологія використана у Директиві про приватність та електронні комунікації була технологічно нейтральною, значною мірою зміни ухвалені Директивою 2009/136/ЄС стосувалися відстеження в Інтернеті за допомогою файлів cookie та інших методів, які мали бути здійсненні виключно за отримання згоди абонентів чи користувачів послуг на обробку даних про трафік. Крім того, абонентам чи користувачам має бути забезпечена можливість відкликати свою згоду (ст. 6 Директиви 2009/136/ЄС) [215]. Примітно, що Директива про приватність та електронні комунікації є досі чинною навіть після набрання чинності Загальним

регламентом про захист даних, який скасував Директиву 95/46/ЄС. Втім, зважаючи на постійне оновлення та розвиток технологічних методів та засобів збирання даних в електронному комунікаційному секторі у 2017 р. Європейська Комісія прийняла пропозицію щодо прийняття Регламенту про приватність та електронні комунікації (так званий ePrivacy Regulation), робота над яким триває досі.

Примітно, що у 2013 році Європейська Комісія прийняла Регламент 611/2013 про заходи, що застосовуються до повідомлення про витік персональних даних відповідно до Директиви 2002/58/ЄС (далі – Регламент 611/2013). Регламент 611/2013 застосовується до постачальників загальнодоступних електронних комунікаційних послуг та зобов'язує постачальника повідомляти компетентні національні органи про витік даних впродовж 24 годин з моменту виявлення витоку персональних даних, якщо це можливо. На додаток до вищезгаданого зобов'язання постачальник послуг зобов'язаний повідомити абонента або особу, дані якої збираються, у разі якщо витік даних може негативно вплинути на їх персональні дані або приватність. Водночас постачальник послуг звільняється від обов'язку повідомлення про витік даних у разі якщо він продемонстрував компетентному національному органу, що відповідні технологічні засоби захисту були запроваджені та що такі заходи поширювалися на дані, витік яких стався. Такі технологічні заходи захисту повинні робити дані незрозумілими для будь-якої особи, яка не має до них доступу [216].

Важливо також звернути увагу на Директиву 2006/24/ЄС Європейського Парламенту та Ради від 15 березня 2006 року про збереження даних, створених або оброблених у зв'язку з наданням загальнодоступних електронних комунікаційних послуг або мереж зв'язку загального користування (далі – Директива про збереження даних). Як зазначено у преамбулі однією з причин прийняття Директиви про збереження даних були терористичні акти, що сталися в громадському транспорті Лондона 7 липня 2005 року. Відтак основною метою прийняття цієї директиви була уніфікація національного законодавства держав-членів для забезпечення використання даних про трафік і даних про місцезнаходження юридичних та фізичних осіб, а також даних, необхідних для ідентифікації абонента або зареєстрованого користувача, для розслідування, розкриття та судового переслідування кримінальних злочинів (ст. 1).

Відповідно до положень Директиви про збереження даних держави-члени мали забезпечити збереження такі категорії даних: 1) дані, необхідні для відстеження та ідентифікації джерела повідомлення, 2) дані, необхідні для визначення призначення повідомлення, 3) дані, необхідні для визначення дати, часу та тривалості повідомлення, 4) дані, необхідні для визначення типу повідомлень, 5) дані, необхідні для ідентифікації користувачів, їх комунікаційного устаткування та обладнання, 6) дані, необхідні для ідентифікації обладнання мобільного зв'язку. Фактично ці категорії включали дані про номер телефону, ім'я та адресу абонента, IP-адресу, ID користувача, дату і час підключення до послуг Інтернету, кількість вхідних та вихідних дзвінків, ідентифікатор міжнародного мобільного абонента (IMSI) та міжнародний ідентифікатор мобільного обладнання (IMEI) [217]. Хоча Директива про збереження даних наголошувала на дотриманні принципів безпеки персональних даних і забезпечення недоторканності приватного життя, але 8 квітня 2014 р. Суд ЄС розглядаючи справу *Digital Rights Ireland Ltd v. Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others*, так звана справа *Digital Rights Ireland,* визнав її недійсною через порушення основоположних прав, а саме права на приватність та права на захист персональних даних, через загальний (невибірковий) збір даних органами влади [218].

Надалі Радою ЄС було прийняте Рамкове рішення 2008/977/JHA про захист персональних даних, що обробляються в рамках поліцейського та судового співробітництва в кримінальних справах (далі – Рамкове рішення 2008/977/JHA). Примітно, що норми Рамкового рішення 2008/977/JHA застосовуються тільки до даних поліції та судових органів при обміні персональними даними між державами-членами з метою запобігання, розслідування, розкриття або переслідування кримінальних правопорушень або виконання кримінальних покарань, а обробку персональних даних правоохоронними органами на національному рівні було виключено зі сфери його дії. Водночас Рамкове рішення 2008/977/JHA визначає виключні випадки, коли держави можуть передавати приватним особам персональні дані отримані від компетентних органів, зокрема у разі отримання згоди компетентного органу держави від якого дані отримуються, якщо жодні конкретні законні інтереси суб'єкта даних не перешкоджають передачі, а також в окремих випадках, коли передача є важливою для компетентного

органу, який передає дані приватній стороні, наприклад, для виконання законно покладеного на нього завдання, запобігання, розслідування, розкриття або переслідування кримінальних правопорушень або виконання кримінальних покарань або запобігання безпосередній та серйозній загрозі громадській безпеці чи серйозній шкоді правам інших осіб [219].

Визначальним етапом розвитку права ЄС у сфері захисту персональних даних стало прийняття 27 квітня 2016 р. Загального регламенту про захист даних, який замінив Директиву 95/46/ЄС і став одним з керівних законодавчих актів у цій сфері. Прийняття Загального регламенту про захист даних стало поштовхом до оновлення й інших актів вторинного права ЄС у сфері захисту персональних даних, які разом прийнято називати «Пакетом захисту даних». Зокрема, було прийнято Директиву 2016/680 про захист фізичних осіб щодо обробки персональних даних компетентними органами з метою запобігання, розслідування, виявлення або переслідування кримінальних правопорушень або виконання кримінальних покарань та про вільне переміщення таких даних (так звана Директива про захист даних правоохоронними органами). Директива про захист даних правоохоронними органами замінила Рамкове рішення 2008/977/ЈНА, забезпечивши, таким чином, вищий рівень гармонізації національного законодавства. Директива про захист даних правоохоронними органами захищає основоположне право громадян на захист персональних даних, коли дані використовуються правоохоронними органами з метою забезпечення правопорядку. Фактично вона передбачає узгоджені правила захисту та вільного переміщення персональних даних, які обробляються з метою запобігання, розслідування, виявлення чи судового переслідування кримінальних правопорушень або виконання кримінальних покарань, включаючи захист і запобігання загрозам громадської безпеки. Щоб запобігти створенню серйозних ризиків, захист фізичних осіб має бути технологічно нейтральним і не залежати від використовуваних методів. Відтак, Директива про захист даних правоохоронними органами забезпечує належний захист персональних даних таких категорій, як жертв, свідків та підозрюваних та сприяє транскордонному співробітництву в боротьбі зі злочинністю та тероризмом, а також у рамках співробітництва з Інтерполом [209]. Досліджуючи роль Директиви про захист даних правоохоронними органами поділяємо думку науковців Т. Радтке та Т.

Квінтел, що Директива про захист даних правоохоронними органами розглядається як *lex specialis*, застосовний у сфері правоохоронної діяльності [221; 222, с. 104]. Водночас погоджуємося із твердженням науковців М. Р. Лейзер та Б. Х. М. Кастерс, що залежно від контексту Директива про захист даних правоохоронними органами також може розглядатися як правовий режим, що діє паралельно Загальному регламенту про захист даних [223, с. 368-369].

З метою забезпечення чіткого регулювання захисту персональних даних в контексті правоохоронної діяльності із прийняттям Загального регламенту про захист даних було ухвалено й Директиву 2016/681 про використання даних записів імен пасажирів (passenger number records або PNR) для запобігання, виявлення, розслідування та переслідування терористичних та тяжких злочинів (далі – Директива 2016/681). Ця Директива 2016/681 була відповіддю на хвилю масових терактів і спрямована на боротьбу з тероризмом. Дані PNR включають ім'я, дати подорожі, маршрут подорожі, інформацію про квиток, контактні дані, туристичну агенцію, у якої було заброньовано рейс, використаний спосіб оплати, номер місця та інформацію про багаж. Фактично ці дані обробляються та зберігаються перевізниками при бронюванні та реєстрації на рейс, тому використання таких даних для запобігання, виявлення, розслідування та переслідування терористичних та тяжких злочинів не є новим. Втім, Директива 2016/681 визначає низку обов'язків країн ЄС щодо збору даних записів імен пасажирів (PNR), вимагаючи від них: створити конкретні органи, відповідальні за збір, зберігання та обробку даних PNR-так звані підрозділи інформації про пасажирів (passenger information units або PIU), а також прийняти перелік компетентних органів, які мають право запитувати або отримувати дані PNR та створити загальні протоколи та формати даних для передачі даних PNR від авіаперевізників до підрозділів інформації про пасажирів. Дані PNR можуть зберігатися в підрозділах інформації про пасажирів (PIU) впродовж 5 років з моменту, однак після спливу 6 місяців після передачі даних PNR останні мають бути деперсоніфіковані, а використання даних PNR без деперсоніфікації дозволяються лише у виключних випадках. Примітно, що обробка даних PNR, які розкривають расове чи етнічне походження особи, політичні погляди, релігійні чи філософські переконання, дані про здоров'я, сексуальне життя чи сексуальну орієнтацію заборонена та у випадку,

якщо дані PNR, які розкривають таку інформацію, отримані, то вони повинні бути негайно видалені [224].

Примітно, що у 2018 році було прийнято новий Регламент 2018/1725 про захист фізичних осіб щодо обробки персональних даних установами, органами, офісами та агентствами Союзу та про вільний рух таких даних (так званий Регламент про захист даних установами ЄС). Положення Регламенту про захист даних установами ЄС повністю узгоджуються із положеннями Загального регламенту про захист даних, одночасно регламентуючи особливості обробки персональних даних установами ЄС. Зокрема, Регламент 2018/1725 повторює визначення Загального регламенту про захист даних щодо категорії «персональних даних». Разом з тим, у Регламенті 2018/1725 також з'являється така категорія, як «адміністративні персональні дані», наприклад персональні дані про персонал, які, безумовно, становлять значну частину адміністративних персональних даних, що обробляються всіма установами та органами ЄС, незалежно від їх повноважень, та «оперативні персональні дані», тобто дані які обробляються органами, службами чи агентствами Союзу під час здійснення діяльності, яка підпадає під дію глави 4 або глави 5 розділу V частини третьої ДФЄС, а саме у сфері судового співробітництва у кримінальних справах та поліцейського співробітництва. Порівняно з принципами, що містяться в Загальному регламенті про захист даних, Регламент 2018/1725 встановлює правила, за допомогою яких кожна установа чи орган ЄС уповноважена призначати посадову особу із захисту даних. Примітно, що загальні правила Регламенту 2018/1725 щодо обробки оперативних персональних даних повинні застосовуватися без шкоди для конкретних правил, що застосовуються до обробки оперативних персональних даних установами ЄС під час здійснення діяльності, що підпадає під сферу застосування глави 4 та 5 розділу V частини третьої ДФЄС. Такі спеціальні правила слід розглядати як *lex specialis* щодо положень Регламенту 2018/1725 щодо обробки оперативних персональних даних, який закріплює такі випадки за яких можлива передача даних третім країнам чи міжнародним організаціям: 1) передача на основі рішення Європейської Комісії про адекватність рівня захисту, 2) передача за відсутності рішення про адекватність у разі якщо контролер чи оператор забезпечує відповідні гарантії, а також за умови, що права суб'єктів даних підлягають виконанню

та існують ефективні засоби правового захисту для суб'єктів даних, 3) передача або розкриття даних, на основі міжнародної угоди, такої як договір про взаємну правову допомогу, чинний між запитуючою третьою країною та ЄС [225]. Як зауважує Х. Тракол, Регламент 2018/1725 виключає передачу оперативних персональних даних установами та органами ЄС третім державам і міжнародним організаціям і фактично сфера застосування цих положень наразі обмежена передачею даних до таких установ як Агентство ЄС з питань співробітництва у сфері кримінального правосуддя (Євроюст) та Агентство ЄС, яке займається охороною зовнішніх кордонів (Фронтекс) [226, с. 542-543].

Варто зауважити, що 23 жовтня 2019 року було прийнято Директиву Європейського Парламенту і Ради ЄС 2019/1937 про захист осіб, які повідомляють про порушення права ЄС (далі – Директива 2019/1937). Зважаючи на те, що розкриття інформації в інтересах суспільства є запорукою ефективної реалізації демократії як на місцевому, так і регіональному рівні в рамках ЄС було ухвалено Директива 2019/1937. Директива 2019/1937 закріплює низку мінімальних гарантій для захисту прав викривачів порушень права ЄС, серед іншого, у ст. 17 містить однозначне посилання на захист персональних даних в контексті діяльності викривачів, зазначаючи, що обробка персональних даних, яка здійснюється відповідно до цієї Директиви, включаючи обмін або передачу персональних даних компетентними органами, повинна здійснюватися відповідно до Регламенту 2016/679, що стосується захисту персональних даних, Директиви 2016/680, так званої Директиви про захист даних правоохоронними органами. Водночас будь-який обмін або передача інформації установами, органами, службами чи агентствами ЄС здійснюється відповідно до Регламенту 2018/1725. Персональні дані, які явно не мають відношення до обробки конкретного звіту, не збираються або, якщо вони були випадково зібрані, видаляються без невиправданої затримки [227].

Швидкий розвиток та активне використання сучасних технологій, серед іншого, технологій штучного інтелекту (ШІ) стало поштовхом до розробки і представлення Європейською Комісією Акту про штучний інтелект 2021 р. (Artificial Intelligence Act), яким пропонується узгодити правила щодо використання штучного інтелекту з огляду

на потенційні ризики, які вони несуть. Зокрема, цим актом пропонується класифікувати регулювати програми штучного інтелекту за ступенем ризику. Класифікація передбачає: 1) заборонені практики, до прикладу, використання біометричних систем, що працюють у режимі реального часу і віддалено, зокрема, сканування для розпізнавання обличчя; технологій, які передбачають когнітивно-поведінкове маніпулювання людьми або окремими вразливими групами, наприклад, голосові іграшки, які заохочують небезпечну поведінку дітей, а також технологій, які використовуються для класифікації людей на основі їх поведінки, соціально-економічного статусу чи особистих характеристик), 2) системи з високим ступенем ризику, тобто такі, що становлять значну загрозу здоров'ю, безпеці чи основоположним права людини та вимагають постійної оцінки їх відповідності, та 3) інші технології ШІ, як от генеративний ШІ, наприклад, ChatGPT, 4) технології з обмеженим чи мінімальним ризиком, наприклад, системи ШІ для генерування чи маніпулювання зображення, аудіо чи відео контенту. Крім того, пропонуються заходи на підтримку інновацій та створення регуляторних пісочниць зі штучного інтелекту задля надання змоги розробникам та регуляторам співпрацювати у контрольованому просторі. Водночас передбачається створення Європейської ради з питань штучного інтелекту (European Artificial Intelligence Board) та національних компетентних органів задля забезпечення імплементації та єдності застосування Акту про штучний інтелект [228; 229]. Варто зауважити, що 14 червня 2023 року Європейський Парламент схвалив цей законопроєкт і, хоч на сьогодні він ще не прийнятий, але у разі прийняття цей акт є стане першим міжнародним документом для регулювання штучного інтелекту.

Водночас 16 січня 2023 року набула чинності Директива (ЄС) 2022/2555 Європейського Парламенту та Ради від 14 грудня 2022 року про заходи щодо високого загального рівня кібербезпеки в Союзі, внесення змін до Регламенту (ЄС) № 910/2014 і Директиви (ЄС) 2018/1972, а також скасування Директиви (ЄС) 2016/1148 (так звана Директива NIS 2). Директива NIS 2 наголошує на важливості захисту персональних даних, які часто можуть бути під загрозою під час використання мережевих та інформаційних систем. Водночас заходи, пов'язані із запобіганням, виявленням, ідентифікацією, стримуванням, аналізом і реагуванням на інциденти, заходи щодо

підвищення обізнаності щодо конкретних кіберзагроз, обмін інформацією в контексті усунення вразливостей систем, добровільний обмін інформацією про них інциденти, кіберзагрози та вразливості, сповіщення про кібербезпеку та інструменти конфігурації можуть вимагати обробки певних категорій персональних даних, таких як IP-адреси, уніфіковані локатори ресурсів (URL-адреси), доменні імена, електронна пошта адреси та, якщо вони містять персональні дані, позначки часу, обробка яких має відбуватися відповідно до Загального регламенту про захист даних (пункт 121 Преамбули Директиви NIS 2) [230]. Відповідно, в контексті забезпечення кібербезпеки персональні дані обробляються відповідно до права ЄС про захист персональних даних, що втілено у Загальному регламенті про захист даних.

Відтак, правове регулювання ЄС у сфері захисту персональних даних вирізняється наявністю значного масиву законодавчих актів, які детально регламентують питання обробки персональних даних та містять стандарти захисту даних, спрямовані на забезпечення захисту прав осіб при обробці їх даних. Право ЄС у сфері захисту персональних даних складається із низки правових актів різного характеру, включаючи як директиви, які запроваджуються шляхом імплементації у національне законодавство, так і регламенти, які підлягають негайному виконанню всіма державами-членами. Керівну роль у сфері захисту персональних даних відіграє Загальний регламент про захист даних, який виступає в якості *lex generalis*. Водночас інші нормативно-правові акти ЄС, які можуть містити спеціальні правила щодо обробки даних у певних сферах чи обробки певних категорій даних, а відтак розглядаються за конкретних ситуацій як *lex specialis*. Важливу роль у забезпеченні захисту персональних даних і тлумаченні відповідних законодавчих актів ЄС у цій сфері відіграє Суд ЄС.

3.2 Удосконалення правового регулювання Європейського Союзу в сфері захисту персональних даних

Тривалий час Директива 95/46/ЄС залишалась одним з найпрогресивніших документів в системі ЄС, що забезпечував захист персональних даних, адже вільний рух товарів, осіб, послуг та капіталів вимагав забезпечення вільного переміщення даних і забезпечення їх належного захисту. Директива 95/46/ЄС фактично закріпила нові

правила обробки даних та розширила перелік основних прав суб'єктів даних, закріпивши найбільш прогресивні положення щодо захисту даних, що дозволяє віднести її до другого покоління стандартів захисту персональних даних. Зокрема, у ст. 11 Директиви 95/46/ЄС регламентовано порядок отримання даних не від суб'єкта даних та відповідні гарантії для захисту прав останнього, а саме вимога поінформувати суб'єкта даних про особу контролера, цілі обробки, категорії даних, одержувачів даних, існування права на доступ і виправлення даних. Стаття 12 закріплювала право суб'єкта даних вимагати повідомлення третім особам, яким були надані дані, про будь-яке виправлення, стирання чи блокування даних, а ст. 14 гарантуючи право суб'єкта даних на заперечення також наділяла останнього правом заперечити проти обробки даних, які контролер має намір обробити з метою прямого маркетингу. Особливістю Директиви 95/46/ЄС є й те, як зазначив А. В. Пазюк, що вона встановила нові правила, які раніше не були включені ані до Конвенції № 108, ані до Керівних принципів ОЕСР, а саме положення щодо рішень, які приймаються автоматизованими системами під час оцінки особистісних характеристик на основі аналізу інформації, що її стосується. Директива 95/46/ЄС надала особам право ознайомитися з логічною формулою, що її використовує автоматизована система (ст. 12), і право оскаржити рішення, що ґрунтується на основі автоматизованої обробки даних (ст. 15) [41, с. 89].

Крім того, Директива 95/46/ЄС передбачала створення незалежних наглядових органів у державах-членах, а у ст. 29 передбачала створення Робочої групи з питань захисту фізичних осіб при обробці персональних даних (так звана Робоча група Статті 29), яка є консультативним, незалежним органом, який складається з представників національних органів з питань захисту персональних даних держав-членів. Основними завданнями Робочої групи Статті 29 визначено надання висновків щодо рівня захисту даних в ЄС та третіх країнах, сприяння послідовному застосуванню Директиви 95/46/ЄС, надання рекомендацій з питань захисту осіб при обробці персональних даних та опублікування щорічних звітів про ситуацію відносно захисту осіб при обробці персональних даних.

Як зазначено у преамбулі прийняття Директиви 95/46/ЄС мало сприяти гармонізації національного законодавства у сфері захисту персональних даних, у ній був

запропонований більш точний рівень визначень у порівнянні з чинними на той час національними законами про захист персональних даних [88, с. 17-18]. Примітно, що аналізуючи європейське законодавство у сфері захисту персональних даних Європейський комісар з захисту даних П. Хастінгс наголосив, що Директива 95/46/ЄС використовувала Конвенцію № 108 як відправну точку для гармонізації законодавства про захист персональних даних у ЄС і конкретизувала її положення. Перш за все це стосувалося керівних принципів захисту даних, обов'язків контролерів, основних прав суб'єктів даних, а також створення незалежного наглядового органу у сфері захисту даних [231]. Дійсно, гармонізація законодавства європейських держав у сфері захисту даних набула високого рівня завдяки тому, що більшість країн європейського регіону імплементували у національне законодавство положення Конвенції № 108 та Директиви 95/46/ЄС або принаймні один із зазначених документів, які закріплювали доволі подібний підхід до захисту персональних даних. Хоч від початку Директива 95/46/ЄС була втіленням доволі прогресивних норм права ЄС у сфері захисту персональних даних, але нестримний технологічний розвиток та широкомасштабна цифровізація зумовили необхідність оновлення правової регламентації у сфері захисту даних.

Практично одразу після початку 2000-х, Директива 95/46/ ЄС вже не могла ефективно протидіяти новим викликам, які виникали разом з динамічним розвитком технологічної індустрії. Якщо першочергово персональні дані використовувались для потреб бізнесу, то з розвитком технологій виникало все більше процесів обробки даних і невизначеності, зокрема і у сфері соціальних мереж, що неминуче призвело до створення нового підходу до захисту персональних даних [232]. Втім, імплементація директиви як законодавчого акту ЄС надає державам широку свободу розсуду, а тому попри те, що держави-члени ЄС імплементували положення Директиви 95/46/ЄС у власне національне законодавство, на практиці підхід до захисту персональних даних залишився неоднорідним.

Важливим етапом оновлення права ЄС у сфері захисту персональних даних стало прийняття Лісабонського договору 2009 р. Перш за все з набранням чинності Лісабонським договором 2009 р. Хартія ЄС набула юридичної сили первинного права ЄС і стала обов'язковою як для інститутів та органів ЄС при виконанні своїх обов'язків,

так і для держав-членів ЄС. Набуття Хартією ЄС юридично обов'язкової сили сприяло забезпеченню однакового застосування та гарантуванню основоположних прав людини на території держав-членів ЄС, включаючи й право на захист персональних даних, яке було закріплено як самостійне право, окремо від права на повагу до приватного і сімейного життя. Це право передбачається й у ст. 16 ДФЄС у розділі, який присвячений загальним принципам діяльності ЄС. Відтак Лісабонський договір 2009 р. передбачав новий горизонтальний підхід до захисту персональних даних та приватності та забезпечував необхідну юридичну основу для цього (ст. 16 ДФЄС), щоб позбутися наявних відмінностей та розбіжностей, які перешкоджали безперешкодному, послідовному та ефективному захисту усіх осіб.

У 2010 році у своєму Повідомленні про «Комплексний підхід до захисту персональних даних у Європейському Союзі» Європейська Комісія, зауваживши безапеляційний вклад Директиви 95/46/ЄС у розвиток та захист персональних даних в ЄС, дійшла висновку про те, що ЄС потребує більш комплексного і послідовного підходу до захисту основоположного права на захист персональних даних з огляду на швидкий технологічний прогрес та глобалізацію, внаслідок якої виникла необхідність у захисті персональних даних при їх обробці поза межами ЄС. Окрім цього ризики для приватності та захисту персональних даних, пов'язані з діяльністю в Інтернеті, зростали до того ж через масове використання соціальних мереж, а також використання «хмарних обчислень» для зберігання даних, які підвищували ризик втрати контролю над потенційно чутливою інформацією, адже дані зберігаються за допомогою програм, розміщених на обладнанні третіх осіб. Водночас Європейська Комісія наголосила на тому, що способи збору персональних даних стають дедалі складнішими, адже дедалі важче виявити механізми таргетингу, використання процедур, що дозволяють автоматично збирати дані чи надають інформацію про геолокацію. Відтак Європейська Комісія дійшла висновку, що необхідно вирішити такі питання, як: вплив нових технологій, посилення захисту даних в рамках внутрішнього ринку, подолання наслідків глобалізації та удосконалення міжнародної передачі даних, забезпечення міцніших інституційних механізмів для ефективного дотримання правил захисту даних та покращення узгодженості правової бази захисту даних [233].

Зазначені фактори стали поштовхом до початку обговорення щодо необхідності оновлення і посилення захисту приватності та захисту даних у цифровій сфері. Варто також зауважити, що прийняття Загального регламенту про захист даних було об'єктивно зумовлено необхідністю зменшення ризиків порушення права на захист персональних даних, особливо в аспекті здійснення транскордонної передачі персональних даних. Одним з чинників було скасування Судом ЄС Угоди про безпечну гавань між ЄС та США, яка виявилась неспроможною подолати на практиці розбіжності у режимах захисту персональних даних у ЄС та США, впорядкувати засоби для дотримання американськими організаціями Директиви 95/46/ЄС та захистити організації ЄС, що передають персональні дані організаціям США. Хоч для врегулювання цього питання було прийнято Щит конфіденційності між ЄС та США, однак розвиток сучасних технологій, впровадження технологій штучного інтелекту та всеохопна цифровізація вимагала адаптації норм права ЄС із захисту персональних даних до сучасних реалій.

25 січня 2012 року Європейська Комісія запропонувала комплексну реформу права ЄС у сфері захисту даних наголосивши, що 27 держав-членів ЄС імплементували директиву 1995 року по-різному, що призвело до розбіжностей у її застосуванні [234]. Примітно, що у 2012 році розпочався саме паралельний процес оновлення основних міжнародних інструментів захисту персональних даних в ході якого законодавчі органи РЄ та ЄС спрямували зусилля на забезпечення взаємоузгодженості та скоординованості оновлених європейських інструментів захисту даних, що мало наслідком оновлення Конвенції № 108 та прийняття Загального регламенту про захист даних [84, с. 29]. Такий підхід свідчить про існування тісних взаємозв'язків між двома системами захисту та демонструє бажання забезпечити належний рівень та ефективне функціонування захисту персональних даних.

Як наголошує К. С. Мельник, проєкт Загального регламенту про захист даних ґрунтувався на статті 16 ДФЄС, що становив нову юридичну підставу для запровадження правил захисту даних, передбачених Лісабонським договором 2009 року і передбачав оновлення правил щодо захисту фізичних осіб при обробці персональних даних державами-членами ЄС під час здійснення діяльності, яка підпадає під

регулювання права ЄС, а також впровадження правил вільного переміщення персональних даних, включаючи персональні дані, які обробляються державами-членами ЄС чи приватними організаціями [43, с. 59]. Саме стаття 16 ДФЄС, яка розташована у розділі, який присвячений загальним принципам діяльності ЄС, створила незалежну юридичну основу шляхом надання ЄС повноважень законодавчо регулювати питання захисту персональних даних та забезпечити всесторонній підхід до захисту персональних даних, який охоплює всі питання, віднесені до компетенції ЄС [84, с. 31].

Загальний регламент про захист даних, прийнятий 27 квітня 2016 року в ході оновлення права ЄС у сфері захисту даних, набрав чинності 25 травня 2018 року. Загальний регламент про захист даних складається з Преамбули, в якій викладені 173 коментарі (англ. Recitals) щодо особливостей гарантування права на захист персональних даних в інформаційно-цифрову еру, а також 11 глав та 99 статей. Основною метою цього регламенту є захист персональних даних, що гарантується на рівні основоположного права ст. 8 Хартії ЄС та ст. 16 Договору про функціонування ЄС. Враховуючи основні положення Директиви 95/46/ЄС, Загальний регламент про захист даних розвинув та деталізував керівні принципи захисту даних та права суб'єктів даних з огляду на інформаційно-цифрові та технологічні виклики.

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

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

- *матеріальна сфера дії* Загального регламенту про захист даних поширюється на повну чи часткову автоматизовану обробку даних та обробку даних із використанням неавтоматизованих засобів, за виключенням обробки даних інституціями ЄС, що врегульована Регламентом 45/2001. Водночас матеріальна сфера застосування має низку обґрунтованих винятків та не застосовується до обробки персональних даних: 1) в ході діяльності, що виходить за межі дії права ЄС, 2) в ході діяльності, що виходить за межі

глави 2 розділу V Договору про ЄС, що регламентує положення про спільну зовнішню та безпекову політику, 3) обробки даних фізичними особами для задоволення особистих або побутових потреб, 4) під час обробки компетентними органами в ході кримінального переслідування, виконання кримінальних покарань, у тому числі для захисту від загроз громадській безпеці або запобігання таким загрозам (ст. 2 Загального регламенту про захист даних).

- *територіальна дія* Загального регламенту про захист даних застосовується до обробки даних на основі визначення: 1) території діяльності установи контролера або оператора (їх головного осідку), незалежно від фактичного місця обробки, 2) території поза межами ЄС, якщо обробка пов'язана із постачанням товарів чи наданням послуг суб'єктам даних на території ЄС або моніторингом поведінки суб'єктів даних, якщо така поведінка відбувається у межах ЄС (так званий критерій таргетингу), 3) території поза межами ЄС, якщо обробка здійснюється контролером через застосування державою-членом права ЄС, що базується на міжнародному публічному праві, зокрема це стосується діяльності консульств чи круїзних суден під державним прапором країн-членів ЄС (ст. 3) [235];

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

Примітно, що у порівнянні з Директивою 95/46/ЄС у статті 4 Загальний регламент про захист даних закріплює широкий перелік вичерпних та вдосконалених визначень, що використовуються у сфері захисту персональних даних. Варто зауважити, що вісім визначень, які закріплювалися в Директиві 95/46/ЄС, не були виключені чи змінені по суті, а були фактично доповнені вісімнадцятьма новими визначеннями, зокрема визначення профілювання, псевдонімізації, даних про здоров'я, генетичних даних, біометричних даних, витоку персональних даних, представника та інших понять [232].

Що стосується визначення персональних даних, то в цілому воно не надто відрізняється від попереднього визначення, закріпленого Директивою 95/46/ЄС, проте надається розширений перелік ідентифікаторів, що включає, серед іншого, захист даних про місцеперебування, онлайн-ідентифікаторів (IP-адреса, «cookies»). Окремо

виділяються «спеціальні категорії персональних даних», а саме так звані «чутливі дані», до яких відносяться дані, що розкривають расову чи етнічну приналежність, генетичні дані, біометричні дані та інші унікальні ідентифікатори особи. Зауважимо, що у пункті 26 Преамбули Загального регламенту про захист даних визначено, що персональні дані із використанням псевдоніма, який можна віднести до певної фізичної особи шляхом використання додаткової інформації, також вважаються інформацією про особу, яку можна ідентифікувати [47].

Характерною особливістю Загального регламенту про захист даних є те, що він визначає дітей як особливу категорію осіб, що потребують додаткового захисту, оскільки вони можуть бути менш обізнаними про відповідні ризики, наслідки, гарантії, а також власні права щодо обробки персональних даних у контексті надання послуг інформаційного суспільства (пункт 38 Преамбули). Ці аспекти повинні враховуватися при використанні персональних даних дітей для цілей маркетингу чи створення профілів і збирання персональних даних дітей під час користування послугами, які пропонують безпосередньо дитині. З огляду на особливу вразливість дітей, інформація і повідомлення щодо обробки даних дитини мають бути сформульовані чіткою і простою мовою, щоб дитина могла її легко зрозуміти (пункт 58 Преамбули). Відповідно до ст. 8 Загального регламенту про захист даних передбачаються особливості обробки персональних даних дітей, а саме у разі недосягнення ними 16 років, обробка буде законною у разі якщо згоду надано чи погоджено законним представником дитини і лише межах, визначених у такій згоді. Щоправда, держави-члени можуть передбачити у національному законодавстві нижчий вік отримання згоди, проте такий вік не може бути нижчим 13 років. Водночас згода законного представника не вимагається у разі надання профілактичних або консультаційних послуг безпосередньо дитині [47].

Що стосується основних принципів обробки даних, які були встановлені раніше чинною Директивою 95/46/ЄС, то вони закріплені і розвинуті у ст. 5-11 Загального регламенту про захист даних та включають: (a) законність, правомірність та прозорість обробки персональних даних; (b) цільове обмеження; (c) мінімізація даних; (d) точність та оновлення даних; (e) обмеження зберігання; (f) забезпечення цілісності та конфіденційності даних.

Примітно, що Загальний регламент про захист даних деталізував принцип законності, згідно з яким обробка вважатиметься законною якщо вона здійснюється на підставі згоди суб'єкта даних або інший законній підставі, як от виконання договору стороною якого є суб'єкт даних, виконання встановленого законом зобов'язання, що поширюється на контролера, захист життєво важливих інтересів суб'єкта даних або іншої особи, виконання завдання в суспільних інтересах або для здійснення офіційних повноважень контролера, а також у разі якщо обробка є необхідною для захисту інтересів контролера або третьої сторони, окрім випадків, коли над такими інтересами переважають інтереси основоположних прав суб'єкта даних, що вимагають охорони персональних даних, особливо, якщо суб'єктом даних є дитина (ст. 6 Загального регламенту про захист даних) [47].

Оскільки найбільш розповсюдженою підставою для обробки є згода суб'єкта даних, питання що пов'язані з її отриманням і вимогами, які ставляться до такої згоди, є чітко врегульованими. Основна концепція згоди залишається подібною до тієї, що передбачена Директивою 95/46/ЄС, але Загальний регламент про захист даних містить додаткові вказівки в статті 7, а також в пунктах 32, 33, 42 і 43 Преамбули, щодо того, як контролер повинен діяти, щоб відповідати основним елементам вимоги щодо отримання згоди як законної підстави для обробки даних. Перш за все, згода має бути чіткою, добровільною та поінформованою, а інформація про факт і межі надання згоди має бути викладена зрозумілою, доступною мовою із використанням чітких та простих формулювань. Згода не буде вважатися наданою добровільно у випадках, коли є будь-який елемент примусу, тиску або неможливості проявити свободу волі, наприклад, у разі дисбалансу повноважень при отриманні згоди органами державної влади чи роботодавцями. Втім, використання згоди як законної основи для обробки даних у такому разі не виключається повністю, а є лише підставою для більш детального аналізу щодо дійсної добровільності такої згоди. Водночас у пункті 42 Преамбули наголошується, що згода не вважається добровільною у разі якщо суб'єкт даних не здійснює справжнього вибору або не має можливості відмовити у наданні згоди чи її відкликанні, не заподіюючи при цьому шкоди. Крім того, можливість відкликати згоду має бути забезпечена так само у легкодоступній формі, як і при її наданні. Згода може

бути втілена в усній заяві чи письмовій заяві, в тому числі сформульованій з використанням електронних засобів, що може включати, наприклад, заповнення клітинки позначкою при відвідуванні Інтернет-сайті, обрання технічних налаштувань для послуг інформаційного суспільства. Згода може бути втілена й в іншій заяві чи поведінці, що однозначно вказують на погодження суб'єкта даних запропонованої обробки даних. Для того, щоб вважати згоду поінформованою суб'єкт даних повинен бути обізнаний принаймні про особу контролера та цілі обробки даних [47].

Примітно, що згода поширюється на всі види обробки даних, що переслідують одну або однакові цілі, але якщо обробка передбачає досягнення декількох, не пов'язаних цілей, згода потрібна для кожної з них. У цьому аспекті Європейська рада із захисту даних (EDPB) розтлумачила, що у разі якщо передбачається кілька операцій обробки для кількох цілей суб'єкти даних повинні мати право вибирати, яку конкретну ціль обробки вони погоджують, замість того, щоб погоджуватися на групу цілей обробки. Що стосується взаємовідношення між згодою та іншими законними підставами обробки даних, то було наголошено, що повинна бути єдина правова підстава для обробки даних, а контролер не може змінювати згоду на інші законні підстави. Зокрема, не дозволяється ретроспективно використовувати законний інтерес як підставу для обґрунтування обробки, якщо виникли проблеми з дійсністю згоди. Через вимогу щодо розкриття законної підстави, на яку покладається контролер під час збору персональних даних, контролери повинні заздалегідь вирішити, якою є правова основа обробки даних [236, с. 12, 25].

Нововведення Загального регламенту про захист даних також стосувалися деталізації та розширення змісту основних прав суб'єкта даних. Розділ про права суб'єктів даних упорядкований у формі підрозділів, які охоплюють такі групи прав:

1) право на прозорість обробки даних (ст. 12);
2) право на інформацію (ст. 13, 14) та право на доступ до даних (ст. 15);
3) право на виправлення (ст. 16), право на видалення («право на забуття») (ст. 17), право на обмеження обробки (ст. 18), право на мобільність даних (ст. 20);
4) право на заперечення проти автоматизованого індивідуального прийняття рішень (ст. 21).

Детальніше зупинимося на нововведеннях Загального регламенту про захист даних, що стосуються прав суб'єкта даних, зокрема так званого «права на забуття», що закріплене у ст. 17. У рамках ЄС право на забуття тісно пов'язують з рішенням Суду ЄС у справі C-131/12 *Google Spain SL, Google Inc. v Agencia Española de Protección de Datos, Mario Costeja González* (далі – справа *Google Spain*), яка набула значного резонансу. Справа стосувалася вимоги іспанського громадянина Маріо Костехи Гонсалеса до корпорації *Google* видалити електронну версію статті 1998 року з архіву газети La Vanguardia про продаж його будинку на аукціоні в рахунок сплати соціального боргу, який був згодом ним погашений, а також посилання на цю статтю. На думку пана Костехи, ця стаття була такою що компрометує його, адже судова справа давно вирішилася. Згідно з рішенням Суду ЄС оператори пошукової системи зобов'язані видаляти зі списку результатів, виданих у відповідь на пошуковий запит на основі імені особи, посилання на вебсторінки, що містять інформацію про таку особу. Втім, Суд ЄС зауважив, що ця справа не є універсальною, а право на забуття не є абсолютними, а відтак в аналогічних справах рішення виноситимуться на основі аналізу конкретних обставин справи (англ. case-by-case assessment), задля виключення суперечностей між основоположними правами людини [237]. Таким чином, завдяки судовому рішенню у цій справі вперше закріплено «право на забуття», яке згодом набуло свого розвитку із прийняттям Загального регламенту про захист даних, як право громадян ЄС звернутися за певних обставин до оператора будь-якої пошукової системи чи національного органу із захисту даних із запитом про видалення недостовірної або застарілої інформації, що містить їх персональні дані, навіть якщо такі дані першочергово оброблялися законно.

Основним постулатом «права на забуття» є право суб'єкта даних за певних умов вимагати від контролера видалення своїх персональних даних та відмови від їх подальшої обробки. Умови реалізації цього права тісно пов'язані із відсутністю законних підстав обробки даних, як от у разі відсутності потреби в обробці даних для цілей, для яких їх збирали чи обробляли, відкликання згоди суб'єктом даних чи запереченням проти обробки, якщо персональні дані необхідно стерти для дотримання контролером встановленого законом зобов'язання, або якщо обробка даних іншим чином не відповідатиме Загальному регламенту про захист даних, що закріплено у ст.

17. У цьому аспекті можна погодитися з висловлюванням колишньої Єврокомісарки з питань правосуддя, основоположних прав та громадянства В. Редінг, що право на забуття є способом надати людям більший контроль над своїми персональними даними, насамперед над тими даними, що надані самими індивідами, адже з використанням практично безмежних властивостей Інтернету щодо пошуку і збереження даних важливим є забезпечення контролю особи над її ідентичністю онлайн. Звісно право на забуття не є абсолютним і тому не може переважати над свободою вираження поглядів та свободою медіа якщо існують правомірні підстави для збереження даних [238].

Примітно, що задля посилення контролю особи над власними персональними даними Загальний регламент про захист даних закріплює також право на мобільність даних, тобто право на отримання своїх персональних даних, наданих контролеру в структурованому, широко вживаному форматі, що легко зчитується машиною, і право на передачу цих даних іншому контролеру, якщо дані обробляються на основі згоди чи договору і їх обробка є автоматизованою. У п. 67 Преамбули Загального регламенту про захист даних наголошується, що це право необхідно застосовувати, якщо суб'єкт даних надав персональні дані на підставі своєї згоди, або якщо обробка є необхідною для виконання договору. Втім, його не можна застосовувати, якщо обробка ґрунтується на законній підставі, іншої ніж згода чи договір, а також це право не можна реалізовувати проти контролерів, якщо обробка є необхідною для дотримання встановленого законом зобов'язання контролера, для виконання завдання в суспільних інтересах або здійснення офіційних повноважень, покладених на контролера [47].

Правам суб'єктів даних кореспондують низка обов'язків, покладених на контролерів задля забезпечення ефективного захисту їх прав. Перш за все з огляду на сучасний рівень розвитку, витрати на реалізацію, специфіку, обсяг, контекст і цілі обробки, а також ризики різної ймовірності та тяжкості для прав людини, які може спричинити обробка, контролер повинен, у момент визначення засобів обробки та власне в момент обробки, вжити необхідних технічних і організаційних заходів, призначених для ефективної реалізації принципів захисту даних, зокрема, мінімізації даних, і включення необхідних гарантій до обробки для досягнення відповідності вимогам Загального регламенту про захист даних та забезпечення захисту прав суб'єктів

даних (ст. 25 Загального регламенту про захист даних). Такі технічні та організаційні заходи можуть включати, серед іншого, скорочення обробки персональних даних, використання псевдонімів до персональних даних, прозорість щодо функцій та обробки персональних даних чи забезпечення суб'єкта даних можливістю відстежувати обробку даних, а також уможливлення контролера створювати і вдосконалювати характеристики безпеки. У цьому аспекті Загальний регламент про захист даних оперує такими важливими елементами правил захисту персональних даних у праві ЄС як захист даних «за призначенням» і «за замовчуванням» (англ. data protection by design та data protection by default). Захист даних «за призначенням» перш за все стосується використання широкого спектра заходів - від використання передових технічних рішень до базового навчання персоналу, включаючи, серед іншого, псевдонімізацію персональних даних; зберігання персональних даних, доступних у структурованому форматі, який зазвичай зчитується машиною; надання інформації про зберігання персональних даних; наявність систем виявлення зловмисного програмного забезпечення; навчання співробітників основам «кібергігієни»; створення систем управління приватністю та інформаційною безпекою, зобов'язання оператора за договором застосовувати певні методи мінімізації даних тощо. Ці заходи можуть бути впроваджені шляхом поширення стандартів захисту даних, найкращих практик та кодексів поведінки. Що стосується захисту даних «за замовчуванням», то він передбачає обов'язок контролера вжити заходів для гарантування того, що за замовчуванням обробці підлягають лише ті персональні дані, які необхідними для кожної цілі обробки. Сам термін «за замовчуванням» під час обробки персональних даних стосується вибору значень конфігурації або параметрів обробки даних, які встановлюються або призначаються в системі обробки, наприклад, програмне забезпечення, послуга чи пристрій або процедура ручної обробки даних, що впливають на кількість зібраних персональних даних, ступінь їх обробки, період їх зберігання та їх доступність. Відтак першочергово цей обов'язок контролера пов'язаний із впровадженням принципу мінімізації даних. На практиці функція захисту даних може бути вбудована у продукти та послуги, як от соціальні мережі чи мобільні додатки, на початкових етапах розробки, а налаштування приватності «за замовчуванням» будуть забезпечувати мінімізацію кількості зібраних персональних даних, періоду їх зберігання

та їх доступність [239]. Таким чином, на всіх етапах діяльності, пов’язаної з обробкою персональних даних контролер повинен забезпечити дотримання принципів захисту даних та впроваджувати ефективні та відповідні засоби гарантування прав суб’єктів даних. У цьому аспекті чільне місце займає принцип відповідальності контролера щодо дотримання заходів захисту персональних даних.

Ще одним нововведенням Загального регламенту про захист даних було провадження обов’язку контролера без необґрунтованої затримки повідомляти наглядовий орган про виникнення інциденту щодо порушення захисту персональних даних, якщо таке порушення навряд чи призведе до виникнення ризику для прав фізичних осіб. Водночас на оператора покладений обов’язок повідомляти контролера без необґрунтованої затримки після того, як йому стало відомо про порушення захисту персональних даних (ст. 33 Загального регламенту про захист даних). У разі якщо порушення захисту персональних даних ймовірно призведе до виникнення високого ризику для прав фізичних осіб, контролера зобов’язаний без необґрунтованої затримки повідомити суб’єкта даних про таке порушення із використанням простих та чітких формулювань (ст. 34 Загального регламенту про захист даних). Примітно, що якщо тип обробки даних, зокрема, з використанням нових технологій, може призвести до виникнення високого ризику для прав фізичних осіб, контролер повинен провести оцінювання впливу передбачених операцій обробки персональних даних до початку обробки (ст. 35 Загального регламенту про захист даних). Оцінка впливу на захист даних є необхідною у разі систематичного та масштабного аналізу персональних аспектів, що стосуються фізичних осіб та ґрунтується на автоматизованій обробці даних, в тому числі профайлінгу, а також у разі широкомасштабної обробки чутливих персональних даних, персональних даних про судимості та кримінальні злочини або у разі систематичного та широкомасштабного моніторингу масиву даних, що знаходиться у відкритому доступі. З оцінкою ризиків впливу на захист даних нерозривно пов’язаний обов’язок контролера та оператора призначити співробітника з питань захисту даних, що встановлений ст. 37 Загального регламенту про захист даних, адже призначення такого співробітника є обов’язковим у разі якщо: 1) обробку здійснює публічний орган чи установа, за винятком судів, 2) основні види діяльності контролера чи оператора пов’язані з

операціями обробки, які внаслідок їх специфіки, обсягів та/або цілей, вимагають регулярного, систематичного і широкомасштабного моніторингу суб'єктів даних, 3) основні види діяльності контролера чи оператора пов'язані з широкомасштабною обробкою спеціальних категорій даних, а саме чутливих даних, даних про судимості чи кримінальні злочини [47].

Однією з новел Загального регламенту про захист даних також є встановлення штрафних санкцій за порушення правил обробки даних та матеріальну чи нематеріальну шкоду, заподіяну з вини контролера або оператора даних (ст. 77-84 Загального регламенту про захист даних) [47]. У цьому аспекті варто наголосити, що контролери та оператори даних несуть відповідальність не лише за порушення правил обробки персональних даних, але і фактично за будь-яку невідповідність стандартам, впровадженим Загальним регламентом про захист даних.

Водночас Загальний регламент про захист даних передбачає створення системи наглядових органів у сфері захисту персональних даних. При цьому важливу роль відіграють компетентні органи із захисту даних, що створюються в державах-членах ЄС. Такі органи повинні бути забезпечені високим рівнем незалежності від зовнішнього контролю та впливу, а їх члени повинні бути призначені шляхом прозорих процедур, мають володіти необхідними кваліфікаціями, досвідом та навичками та призначаються на посаду протягом чотирьох років. Водночас на підставі ст. 68 Загального регламенту про захист даних було створено незалежну європейську інституцію – Європейську раду із захисту даних, яка є наступником Робочої групи статті 29 та замінила Європейського інспектора із захисту персональних даних, який діяв відповідно до Директиви 95/46/ЄС. Саме на Європейську раду із захисту даних покладається обов'язок забезпечити послідовне застосування положень Загального регламенту про захист даних, а також сприяти ефективному співробітництву між національними наглядовими органами в країнах ЄС. Задля цього Європейська рада із захисту даних публікує висновки, рекомендації та керівництва стосовно тих чи інших аспектів захисту персональних даних відповідно до положень Загального регламенту про захист даних. Водночас Регламентом ЄС № 45/2001, який було оновлено відповідно до Загального регламенту про захист даних, також передбачено діяльність Європейського інспектора із захисту

даних, на якого покладена функція забезпечення дотримання вимог Загального регламенту про захист даних всіма органами ЄС, а також уповноважено представляти ЄС під час розгляду справ, пов'язаних із захистом персональних даних Судом ЄС і Загальним судом.

Зауважимо, що положення глави V Загального регламенту про захист даних також закріплюють оновлені стандарти щодо міжнародної передачі даних. Одним з найбільш поширених способів передачі персональних даних з ЄС до третьої країни чи міжнародної організації є отримання рішення від Європейської комісії про адекватність, передбачене ст. 45 Загального регламенту про захист даних. Країни, які отримали рішення про адекватність, підлягають систематичному моніторингу з боку Європейської ради із захисту персональних даних. Водночас кожне з рішень про адекватність підлягає періодичному перегляду кожні 4 роки після їх видачі, а рішення видані на підставі Директиви 95/46/ЄС підлягають моніторингу на постійній основі (ст. 45 Загального регламенту про захист даних). Іншим способом передачі даних до третіх країн чи міжнародних організацій є передача з урахуванням належних гарантій та прав суб'єктів даних, що підлягають реалізації, та дієвих засобів правового захисту для суб'єктів даних. Належні гарантії можуть бути надані без запиту на отримання від наглядового органу будь-якого спеціального дозволу. Такі гарантії можуть включати, зокрема, стандартні договірні положення (англ. standart contractual clauses), що підлягають застосуванню між публічними органами чи організаціями, зобов'язальні корпоративні правила (англ. binding corporate rules), стандартні положення щодо захисту даних, ухвалені Європейською комісією чи наглядовим органом, кодекси поведінки, а також затверджені механізми сертифікації [47; 232].

Таким чином, прийняття Загального регламенту про захист даних було наслідком закономірного розвитку права на захист персональних даних в період широкомасштабного впровадження інформаційно-цифрових технологій та глобалізації. Загальний регламент про захист даних виводить персональні дані в комплексний і захисний регуляторний режим, що не є повністю відмінним від правового режиму, передбаченого Директивою 95/46/ЄС, а навпаки містить оновлені та проактивні правові норми, що здатні гарантувати належний рівень захисту персональних даних в епоху

викликів цифрової ери. Примітно, що основоположною цінністю, орієнтиром у сфері захисту персональних даних, є гарантування прав суб'єкта даних, що фактично визначає зміст та спрямованість діяльності контролера та оператора даних. Загальний регламент про захист даних закріплює чіткі принципи захисту даних та детально описує зобов'язання та вимоги щодо обробки, які покладаються на сторони, залучені до процесу обробки даних, на всіх етапах обробки задля гарантування захисту персональних даних.

3.3 Особливості захисту персональних даних у Суді Європейського Союзу

Провідну роль у забезпеченні ефективної реалізації положень права ЄС у сфері захисту персональних даних відіграє Суд ЄС, який не тільки здійснює тлумачення норм права ЄС, але й сприяє формуванню однакової правозастосовчої практики на всій території ЄС. Практика Суду ЄС має принципове значення для забезпечення правопорядку ЄС, а тому рішення Суду ЄС розглядаються як окреме джерело права ЄС.

Варто зауважити, що судова система ЄС виступає як самостійний наднаціональний інститут неполітичного характеру, призначенням якого є захист та забезпечення однакового розуміння та застосування установчих договорів ЄС та правових актів, виданих на їх основі. Саме судовим органам ЄС належить виключна роль у формуванні і розвитку права ЄС, затвердженні його ролі і значення як провідного інтеграційного фактора. У рішеннях судових органів ЄС сформульовані та розшифровані зміст і основні кваліфікаційні ознаки права ЄС, а також концептуальні засади та умови еволюції європейської інтеграції, уточнені порядок діяльності та компетенція інститутів та органів ЄС [240]. Таким чином, Суд ЄС тлумачить право ЄС та врегульовує спори між національними урядами та інститутами ЄС, розглядаючи провадження про порушення права ЄС, анулювання правових актів ЄС, забезпечення вжиття заходів ЄС та провадження щодо відшкодування шкоди. Погоджуємося й з аргументованою позицією професора Т. В. Комарової, яка наголошує на унікальній ролі Суду ЄС в контексті гарантування основоположних прав людини [241, с. 385-386].

В аспекті забезпечення права на захист персональних даних Суд ЄС уповноважений вирішувати справи стосовно виконання державами-членами ЄС своїх зобов'язань за правом ЄС у сфері захисту персональних даних або так звані справи про

правопорушення, що можуть виявлятися в різних формах, зокрема у формі невиконання чи незастосування права ЄС або нездійснення імплементації рішень ЄС. Іншим аспектом його діяльності є винесення преюдиційних (або попередніх) рішень щодо тлумачення установчих договорів ЄС та права ЄС у сфері захисту персональних даних на звернення національних судів. Звернення із преюдиційним запитом до Суду ЄС дозволяє національним судам держав-членів ЄС у процесі вирішення спорів, переданих до них, передавати питання до Суду ЄС щодо тлумачення права ЄС. Зауважимо, що Суд ЄС у такому разі не вирішує спір, а саме національний суд держави-члена ЄС повинен вирішити справу з урахуванням преюдиційного рішення Суду ЄС, яке так само є обов'язковим для інших національних судів держав-членів ЄС, перед якими порушується подібне питання. Таким чином, попередні рішення сприяють наближенню національного законодавства держав-членів до права ЄС та забезпечують його однакове застосування, а також можуть призводити до прийняття нових законодавчих актів ЄС у певній сфері. До прикладу, рішення Суду ЄС у справах *Shrems* та *Shrems II* мали далекосяжні наслідки для системи захисту персональних даних у ЄС та призвели до оновлення права ЄС у сфері захисту персональних даних. У цьому аспекті О. Павелек та Д. Заїчкова зауважують, що кількість рішень, прийнятих Судом ЄС, природно корелює з обсягом прийнятого права ЄС. Примітно, що у більшості рішень Суду ЄС у сфері захисту персональних даних стороною виступають приватні особи (наприклад, *Sergejs Buivids v. Datu valsts inspekcija, Heinz Huber v. Bundesrepublik Deutschland*), у меншій частині рішень стороною є юридичні особи (наприклад, *Fashion ID GmbH & Co. KG v. Verbraucherzentrale NRW eV, Josef Probst v. mr.nexnet GmbH*), але учасниками справ також виступає ЄС чи окремі його органи, як-от Європейський Парламент чи Європейська Комісія (наприклад, *European Commission v. Federal Republic of Germany, European Parliament v. Council of the European Union, European Commission v. the Bavarian Lager Co. Ltd.*) [242, с. 174].

Примітно, що ще у 1969 році Суд ЄС у справі *Erich Stauder v. City of Ulm – Sozialamt* (C-29/69), яка стосувалася питання ідентифікації бенефіціара за ім'ям, вперше визнав право на захист приватної інформації як одне з основоположних прав, закріплене в загальних принципах права ЄС (§§6-7) [243]. Від тоді Суд ЄС все частіше розглядає

справи та приймає рішення щодо тлумачення права на приватність і права на захист даних у праві ЄС, що зумовлено технологічним розвитком, всеохопною цифровізацією та підвищенням значущості права на захист персональних даних у сучасному інформаційному суспільстві.

Аналізуючи особливості захисту персональних даних у правопорядку ЄС, в якому повага до основоположних прав людини є частиною загальних принципів права ЄС, виникає потреба визначити вочевидь глибокий зв'язок та сутність основоположних права на приватне життя і права на захист персональних даних. З судової практики Суду ЄС вбачається, що вищезазначені права не були систематично розмежовані та, навпаки, періодично розглядалися як цілісний, складний феномен [244, с. 4]. Це питання насамперед пов'язано з тим, що Директива 95/46/ЄС розглядала персональні дані як один з аспектів права на приватність і оцінювала інші основоположні права в їх сукупності. Лише після прийняття Хартії ЄС право на захист персональних даних було сприйнято як самостійне основоположне право, спеціально гарантоване ст. 8, на рівні із правом на приватне життя, яке гарантується в ст. 7 Хартії ЄС. Одночасно це було відображено в рішеннях Суду ЄС, ухвалених після прийняття Хартії ЄС, зокрема у справі *Tele2 Sverige*, шляхом визнання того, що ст. 8 Хартії ЄС стосується основоположого права на захист персональних даних, яке відрізняється від права, закріпленого в ст. 7 Хартії ЄС, і якому немає еквівалента в ЄКПЛ (§§92-96) [212].

Відтак, з огляду на становлення та розвиток права на захист даних у правопорядку ЄС практику Суду ЄС щодо захисту персональних даних можна поділити на дві категорії – ухвалену до прийняття Хартії ЄС та після прийняття останньої. Період до прийняття Хартії ЄС характеризувався тим, що питання захисту персональних даних розглядалися в рамках права на приватність. Цей підхід повністю узгоджувався з практикою ЄСПЛ щодо тлумачення ст. 8 ЄКПЛ, яка гарантує право на захист приватного життя та в контексті якої розглядалися питання, пов'язані з обробкою персональних даних. У цьому аспекті професори П. Крейг та Г. де Бурка підкреслюють, що до набрання чинності Хартією ЄС основним міжнародним інструментом захисту прав людини, який використовувався Судом ЄС як «особливе джерело натхнення» в контексті загальних принципів права ЄС, була ЄКПЛ. Зважаючи на те, що Суд ЄС

розглядав ЄКПЛ радше як «джерело натхнення», а не як офіційно зобов'язальний або повністю інкорпорований білль про права, Суд ЄС зберіг свободу «виходити за межі» ЄКПЛ у визнанні прав людини частиною права ЄС. Це ідея пізніше була втілена у ст. 52 (3) Хартії ЄС, яка визначає, що значення і обсяг гарантованих Хартією ЄС прав, відповідає правам, гарантованим ЄКПЛ, але «це положення не перешкоджає праву ЄС забезпечувати більший захист» [245, с. 419-421].

З набранням чинності Лісабонським договором 2007 р., який вніс зміни до установчих договорів ЄС та змінив юридичний статус Хартії ЄС, прирівнявши її до установчих договорів ЄС, захист персональних даних набув якісно нового рівня захисту, адже був гарантований на рівні нового основоположого права, яке розглядалося окремо від права на захист приватного життя (ст. 8 Хартії ЄС, ст. 16 ДФЄС) та яке випливає із права ЄС та права РЄ. Як зазначають дослідники О. Павелек та Д. Заїчкова, Лісабонський договір 2007 р. створив потенціал для більш всеохопної законодавчої участі у сфері захисту персональних даних через ст. 16 ДФЄС. Таким чином, у практиці Суду ЄС захист персональних даних почало розглядатися як самостійне основоположне право людини [242, с. 169]. Варто зауважити, що з набранням чинності Хартією ЄС Суд ЄС розглядав питання захисту даних в контексті права на приватність та права на захист персональних даних, гарантованих ст. 7 та 8 Хартії ЄС, тобто розглядаючи право на захист персональних даних як невідлільно пов'язане з приватністю, що відповідало підходу, закріпленому в практиці ЄСПЛ. Ці два права отримують окрему судову оцінку лише у контексті тлумачення того, що становить втручання, та того, що може негативно вплинути безпосередньо на їх сутність. Суд ЄС у своїй практиці зазначив, що оскільки Лісабонський договір набув чинності, дійсність зобов'язань має бути оцінена у світлі Хартії ЄС. Крім того, було зауважено, що право на захист персональних даних тісно пов'язане з правом на повагу до приватного життя, але не є абсолютним правом і має бути оцінено в у світлі ст. 52 Хартії ЄС, яка встановлює умови, коли обмеження можуть бути накладені на здійснення прав (§§45-46) [246].

Варто також звернути увагу, що в цілому, ієрархія норм права ЄС вимагає, щоб нижче правове джерело (вторинне право) читалося у світлі вищого правового джерела (первинного права) [245, с. 136-139]. У цьому аспекті П. Войацоглу та П. Вальке

зазначають, що Суд ЄС демонструє певну гнучкість щодо використання підходів до співвідношення між первинним і вторинним правом у контексті захисту персональних даних, адже сама ст. 8 Хартії ЄС, яка належить до первинного права, містить положення щодо принципів обробки даних, а також перелік прав суб'єкта даних. Втім, вплив вторинного права ЄС на принципи захисту персональних даних та права суб'єкта даних, передбачені частиною 2 статті 8 Хартії ЄС, є важливим для визначення широти їх охоплення [247, с. 19-20]. Відповідно, в аспекті гарантування права захист на персональних даних, закріпленого ст. 8 Хартії ЄС, Суд ЄС розглядає втручання в це право крізь призму положень вторинного права ЄС, а саме Директиви 95/46/ЄС, в більш ранніх справах Суду ЄС, та нещодавно прийнятого Загального регламенту про захист даних, приділяючи особливу увагу принципам і правам, встановлені у них. Саме практика Суду ЄС сприяє затвердженню основоположних європейських стандартів захисту персональних даних, що поступово оновлюються з огляду на виклики та загрози сучасності.

Оскільки персональні дані є доволі широкою категорією, відтак перед Судом ЄС доволі часто постає питання віднесення до неї тих чи інших даних про особу і, відповідно, питання застосування права ЄС у сфері захисту персональних даних. Зауважимо, що як і Директива 95/46/ЄС, Загальний регламент про захист даних передбачає, що для прямої чи опосередкованої ідентифікації фізичної особи можливо використовувати певні ідентифікатори такі, як ім'я/прізвище, ідентифікаційний номер, дані про місцезнаходження, онлайн-ідентифікатор, або за один чи декілька факторів, що є визначальними для фізичної, фізіологічної, генетичної, розумової, економічної, культурної чи соціальної ідентичності такої фізичної особи [47]. Відповідно, для ідентифікації особи необхідна наявність елементів, які описують цю особу у такий спосіб, що її можливо вирізнити з-поміж інших осіб та впізнати як індивіда. Найпоширенішим ідентифікатором виступає ім'я/прізвище особи, але телефонний номер, номер соціального страхування, номер документа, що посвідчує особу чи номерний знак автомобіля також є тією інформацією, яка може призвести до ідентифікації особи. Для ідентифікації особи можуть бути використані й комп'ютеризовані файли, файли cookies та засоби спостереження за вебтрафіком,

оскільки використовуючи ці дані, можна виокремити осіб з-поміж інших через ідентифікацію їхньої поведінки та звичок [84, с. 99].

Важливим питанням, що доволі часто стає предметом розгляду Суду ЄС є визначення обсягу та категорії інформації, що становить персональні дані особи. Зокрема, у рішенні по справі *Criminal proceedings against Bodil Lindqvist* (далі – справа *Bodil Lindqvist*) пані Ліндквіст створила особисту Інтернет-сторінку, де розміщувала певну інформацію про себе та своїх колег. Водночас вона не повідомила своїх колег про існування цієї Інтернет-сторінки і не отримала їхньої згоди, хоч на їх вимогу згодом видалила ці дані. Суд ЄС постановив, що посилання на інформацію про різних осіб на Інтернет-сторінці та їх ідентифікація за іменем, внаслідок описання посад, які займали її колеги, їхніх захоплень, а також сімейних обставин, певних медичних даних та телефонних номерів становить обробку персональних даних за допомогою використання автоматизованих засобів (§§41, 46) [248].

У справі *Michael Schwarz v. Stadt Bochum* Суд ЄС досліджував питання захисту права на повагу до приватного життя та права на захист персональних даних при використанні біометричних ідентифікаторів, а саме відбитків пальців, при видачі паспорта органами влади. Суд ЄС підкреслив, що відбитки пальців є персональними даними, оскільки вони об'єктивно містять унікальну інформацію про фізичну особу, яка дозволяє точно її ідентифікувати, при цьому відібрання та збереження відбитків пальців ставить обробку персональних даних (§§27-30) [249].

У цьому аспекті варто звернути увагу на висновки у справі *Scarlet Extended SA v. Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM*), яка стосувалася відмови провайдера інтернет-послуг «Scarlet» встановити систему фільтрів електронних комунікацій для попередження обміну файлами в порушення авторського права на вимогу менеджерської компанії SABAM, яка представляє авторів, композиторів та видавців. Суд ЄС у цій справі дійшов висновку, що встановлення оспорюваної системи фільтрів передбачало б моніторинг всіх електронних комунікацій здійснюваних через мережу провайдера інтернет-послуг, систематичний аналіз всього контенту, а також збір та ідентифікацію IP-адреси користувачів, які є «*захищеними персональними даними, оскільки вони дозволяють точно ідентифікувати цих користувачів*» (§§47, 51) [250].

У справі *Patrick Breyer v. Bundesrepublik Deutschland* Суд ЄС розглянув питання віднесення до персональних даних динамічних IP-адрес, які призначаються для кожного підключення до Інтернету та замінюються при наступних підключеннях. У цій справі Суд ЄС дійшов висновку, що динамічна IP-адреса за певних випадків, з використанням додаткових даних, уможливлює непряму ідентифікацію суб'єктів даних постачальником онлайн-медіа послуг (§§38-49) [251]. Примітно, що у справі *Digital Rights Ireland*, яка стосувалася збереження даних постачальниками загальнодоступних електронних комунікаційних послуг або мереж загального зв'язку задля цілей попередження, розслідування, розкриття та переслідування тяжких злочинів, Суд ЄС визнав важливість метаданих в контексті захисту персональних даних з огляду на те, що «*ці дані, взяті в цілому, можуть дозволити зробити дуже точні висновки щодо приватного життя осіб, чиї дані були збережені, наприклад, звички повсякденного життя, постійне чи тимчасове місце проживання, щоденні чи інші переміщення, діяльність, що здійснюється, соціальні зв'язки цих осіб і соціальне середовище, в якому вони часто бувають*» (§27) [218].

Водночас у справі *Peter Nowak v. Data Protection Commissioner*, Суд ЄС вирішив, що письмові відповіді на тестуванні, подані кандидатом на фаховому іспиті, є персональними даними, що дозволяють ідентифікувати особу, використовуючи ідентифікаційний номер, вказаний на екзаменаційному листі. Суд ЄС дійшов таких висновків насамперед тому, що зміст цих відповідей відображає ступінь знань та компетентності кандидата в певній галузі, а в деяких випадках і рівень його інтелекту, його думки та судження. Водночас метою збору цих відповідей є оцінка професійних здібностей кандидата та його придатності до відповідної професії. Окрім того, використання цієї інформації, може порушувати права та інтереси кандидата, оскільки може визначати або впливати, зокрема, на шанс отримати бажану посаду. Водночас Суд ЄС підкреслив, що зауваження екзаменатора стосовно відповідей, поданих кандидатом на іспиті, також є персональними даними. Примітно, що у своєму аналізі Суд ЄС посилався на Загальний регламент про захист даних, хоча останній ще не набув чинності на той момент (§§37-62) [252].

В одному з нещодавніх рішень у справі *OT v. Vyriausioji tarnybinės etikos komisija* Суд ЄС розглянув питання захисту персональних даних при непрямій ідентифікації суб'єкта даних за допомогою даних, оприлюднених в Інтернеті. У цій справі питання стосувалося публічного оприлюднення в Інтернеті декларації про приватні інтереси, яка включає інформацію про другого з подружжя, співмешканця або партнера декларанта та яка подається з метою забезпечення прозорості та запобігання корупції та конфлікту інтересів. Суд ЄС дійшов висновку, що публічне оприлюднення в Інтернеті конкретних даних щодо імені другого з подружжя, партнера або співмешканця декларанта, або осіб, які є близькими родичами декларанта або відомі йому, може розкрити інформацію про певні чутливі аспекти приватного життя суб'єктів даних, включаючи, наприклад, їх сексуальну орієнтацію. Відтак, непряме виявлення сексуальної орієнтації було б можливим за допомогою інтелектуальної операції, що включає методи зіставлення або дедукції. Таким чином, Суд ЄС дійшов висновку, що персональні дані, які можуть опосередковано розкривати сексуальну орієнтацію фізичної особи, становлять обробку спеціальних категорій персональних даних у розумінні статті 9 Загального регламенту про захист даних (§§100-103) [253].

Таким чином, з огляду на практику Суду ЄС, до категорії «персональні дані» відносяться дані, які прямо ідентифікують особу, серед іншого, зображення особи (*František Ryneš v. Úřadu pro ochranu osobních údajů*, Case C-212/13), біометричні дані в документах, що посвідчують особу (*Michael Schwarz v. Stadt Bochum,* C-291/12, *W.P.Willems v. Burgemeester van Nuth and Others,* Joined Cases C-446/12 to C-449/12), номер документа, що посвідчує особу, та адреса (*Valsts policijas Rīgas reģiona pārvaldes Kārtības policijas pārvalde v. Rīgas pašvaldības SIA "Rīgas satiksme"*, Case C-13/16), дані, пов'язані із дозволом на проживання, які містяться в адміністративних документах (*YS v. Minister voor Immigratie, Integratie en Asiel and Minister voor Immigratie, Integratie en Asiel v. M and S,* Joined Cases C-141/12 and C-372/12), дані, що зберігаються в реєстрах (*Camera di Commercio, Industria, Artigianato e Agricoltura di Lecce v. Salvatore Manni*, C-398/15), дані про попередню фінансову історію та заборгованості (справа *Google Spain and Google*, C-131/12), а також дані, які дозволяють опосередковано ідентифікувати особу, зокрема, динамічні IP-адреси (*Patrick Breyer v. Bundesrepublik Deutschland*, C-

582/14), письмові відповіді кандидата та примітки екзаменатора (*Peter Nowak v. Data Protection Commissioner,* Case C-434/16), дані щодо другого з подружжя, партнера чи співмешканця, публічно оприлюднені в декларації (*OT v. Vyriausioji tarnybinės etikos komisija,* Case, C-184/20) та інформація про штрафні бали, нараховані водіям транспортних засобів за порушення правил дорожнього руху (*B v. Latvijas Republikas Saeima,* Case C-439/19) [254]. Вочевидь цей перелік не є виключним і питання віднесення тієї чи іншої категорії інформації до персональних даних особи вирішується Судом ЄС в кожній індивідуальній справі зважаючи на актуалізацію та розвиток європейських стандартів захисту персональних даних.

У контексті вирішення питання дотримання стандартів захисту персональних даних Суд ЄС керується принципами обробки даних, які були гарантовані Директивою 95/46/ЄС та нині закріплені у Загальному регламенті про захист даних. У цьому контексті у нещодавньому рішенні *Digi Távközlési és Szolgáltató Kft. v. Nemzeti Adatvédelmi és Információszabadság Hatóság* Суд ЄС наголосив, що Загальний регламент про захист даних встановлює принципи, що регулюють обробку персональних даних, і права суб'єкта даних, які мають дотримуватися при будь-якій обробці персональних даних. Відповідно, будь-яка обробка персональних даних повинна відповідати принципам, що стосуються обробки даних, викладеним у ст. 5 цього Регламенту, і задовольняти одну з умов щодо законності обробки, перелічених у ст. 6 цього Регламенту (§§49, 56) [255].

Зауважимо, що виходячи з аналізу практики Суду ЄС, сфери, пов'язані із захистом персональних даних є різноманітними та включать, серед іншого, наступні питання: 1) обмеження права на захист персональних даних та баланс конкуруючих прав основоположних прав людини чи інших законних інтересів (*Volker und Markus Schecke GbR and Hartmut Eifert v. Land Hessen,* Joined cases C-92/09 and C-93/09, *Tietosuojavaltuutettu v. Satakunnan Markkinapörssi Oy and Satamedia Oy,* Case C-73/07, *European Commission v. the Bavarian Lager Co. Ltd,* C-615/13P, *ClientEarth, PAN Europe v. EFSA*, Case C-615/13 P); 2) обробки персональних даних у журналістських цілях, зокрема відеофіксація проведення процесуальних заходів працівниками міліції у відділку поліції і подальшій публікації цього відео на вебсайті YouTube (*Sergejs Buivids v. Datu valsts*

inspekcija, Case C-345/17); 3) обробки даних у ході суто особистої чи побутової діяльності, зокрема використання відзнятого на камеру матеріалу (*František Ryneš v. Úřadu pro ochranu osobních údajů*, Case C-212/13); 4) обробки даних в контексті поліцейської діяльності чи діяльності адміністративних органів (*Valsts policijas Rīgas reģiona pārvaldes Kārtības policijas pārvalde v. Rīgas pašvaldības SIA 'Rīgas satiksme'*, Case C-13/16, *Peter Puškár v. Finančnému riaditeľstvu Slovenskej republiky, Kriminálnemu úradu nančnej správy*, Case C-73/16); 5) розкриття даних у контексті боротьби зі злочинністю (*Tele2 Sverige AB v. Post-och telestyrelsen and Secretary of State for the Home Department v. Watson*, Joined cases C-203/15 and C-698/15); 6) захист персональних даних працівників та обліку їх робочого часу (*Pharmacontinente – Saúde e Higiene SA, Domingos Sequeira de Almeida, Luis Mesquita Soares Moutinho, Rui Teixeira Soares de Almeida, André de Carvalho e Sousa contre Autoridade para as Condições do Trabalho (ACT)*, C-683/13, *Worten – Equipamentos para o Lar, SA v. Autoridade para as Condições de Trabalho (ACT)*, Case C-342/12); 7) відображення персональних даних у результатах пошуку в Інтернеті чи публікації персональних даних в мережі Інтернет (справа *Google Spain*, C-131/12, *GC, AF, BH, ED v. Commission nationale de l'informatique et des libertés*, C- 136/17, *Criminal proceedings against Bodil Lindqvist*, Case C-101/01); 8) збір та обробка персональних даних в ході релігійної діяльності (*Tietosuojavaltuutettu v. Jehovan todistajat – uskonnollinen yhdyskunta*, C-25/17), 9) обробка персональних даних в контексті ведення реєстрів (*Heinz Huber v. Bundesrepublik Deutschland*, Case C-524/06) [254].

Примітно, що питання захисту персональних даних виникають також у контексті доступу до публічних документів інститутів ЄС. Так, у справі *European Commission v. the Bavarian Lager Co. Ltd.* компанія Bavarian Lager звернулась до Європейської Комісії з проханням надати певні документи, зокрема, копію протоколу засідання представників Європейської Комісії, органів державної влади Сполученого Королівства і Конфедерації загального ринку пивоварів. Європейська Комісія надала деякі документи, що стосувалися засідання, але зашифрувала у протоколі імена п'яти учасників: двоє з яких чітко заявили, що заперечують проти розкриття їхніх імен, а з трьома іншими Комісія не змогла встановити зв'язок. Суд ЄС дійшов висновку, що оскільки компанія Bavarian Lager не надала явного і законного обґрунтування або іншого переконливого аргументу

для того, щоб продемонструвати необхідність у персональних даних, що були зашифровані, Європейська Комісія належним чином виконала свій обов'язок щодо дотримання відкритості публічної інформації, коли надала запитуваний документ із зашифрованими іменами (§78) [256].

Іншою справою, що стосується доступу до персональних даних є справа *Volker und Markus Schecke GbR (C-92/09) and Hartmut Eifert (C-93/09) v. Land Hessen*. На розгляд Суду ЄС було поставлено питання щодо пропорційності оприлюднення інформації про імена отримувачів субсидій від двох сільськогосподарських фондів ЄС і розмір отриманих коштів, які, на думку Суду ЄС, підпадають під категорію персональних даних. Хоча оприлюднення цих даних і було виправдано передбачено законом і відповідало меті зміцнення прозорості використання державних коштів в ЄС, попри це Суд ЄС дійшов висновку, що оприлюднення імен отримувачів сільськогосподарської субсидії і точних сум субсидій, не відповідає вимогам пункту 1 статті 52 Хартії ЄС щодо пропорційності та виправданості такого втручання. Примітно, що розглядаючи цю справу у §§52-53 Суд ЄС наголосив, що право на повагу до приватного життя в контексті обробки персональних даних відповідно до ст. 7 та 8 Хартії ЄС стосується будь-якої інформації про ідентифіковану фізичну особу або особу, яку може бути ідентифіковано, і відтак дійшов висновку, що *«юридичні особи можуть вимагати захисту за статтями 7 та 8 Хартії щодо такої ідентифікації тільки тією мірою, в якій офіційна назва юридичної особи ідентифікує одну або більше фізичних осіб […]*». Крім того, Суд ЄС зазначив, що у цьому контексті немає значення, що персональні дані стосуються діяльності професійного характеру, адже ЄСПЛ здійснюючи тлумачення статті 8 ЄКПЛ підсумував, що поняття «приватне життя» не може тлумачитися вузько, і що немає жодних принципових причин, що виправдовували б виключення діяльності професійного характеру з поняття «приватного життя» [246].

У контексті розгляду правових позицій Суду ЄС на увагу заслуговують висновки щодо отримання згоди як законної підстави для обробки персональних даних. Зокрема, у справі *Michael Schwarz v. Stadt Bochum* Суд ЄС зауважив, що згода суб'єкта даних буде під загрозою, якщо останній не матиме реального вибору заперечити проти обробки своїх даних (§§31-32) [249]. Аналізуючи питання законності обробки персональних

даних на підставі згоди у справі *Bundesverband der Verbraucherzentralen und Verbraucherverbände – Verbraucherzentrale Bundesverband eV v. Planet49 GmbH* Суд ЄС визначив, що згода не вважатиметься дійсною у разі мовчання, галочок, поставлених за замовчуванням, або внаслідок бездіяльності. Втім, згода на онлайн обробку даних, включаючи файли cookies, не може бути законною, якщо вона встановлена за допомогою попередньо встановлених галочок. Водночас Суд ЄС наголосив, що будь-яка згода, отримана для cookies, не може бути достатньо інформованою відповідно до чинного права ЄС, якщо користувач не може зрозуміти, як функціонуватимуть файли cookies на певному вебсайті (§§55-57, 76-81) [257]. Примітно, що у справі *Orange România SA v. Autoritatea Națională de Supraveghere a Prelucrării Datelor cu Caracter Personal (ANSPDCP)* в контексті надання згоди, шляхом погодження з застереженням у договорі, що стосувалося обробки даних, було підкреслено, що щоб гарантувати, що суб'єкт даних має справжню свободу вибору, договірні умови не повинні вводити його в оману щодо можливості укладення договору, навіть якщо він або вона відмовляється дати згоду на обробку даних. Без інформації такого роду згода суб'єкта даних на обробку персональних даних не може вважатися такою, що була надана добровільно або, більш того, як така, що була надана усвідомлено (§41) [258]. Зауважимо, що хоч згода суб'єкта даних не є виключною правомірною підставою обробки персональних даних, але саме на основі згоди найчастіше відбувається обробка персональних даних.

Таким чином, захист основоположних прав людини, включаючи право на захист персональних даних, поступово став складовою права ЄС. Становлення права на захист персональних даних у правопорядку ЄС охоплює два значні періоди – до ухвалення Хартії ЄС, коли право на захист персональних даних розглядалося в контексті захисту права на приватність, та після, тобто з набранням чинності Хартією ЄС, коли згадані права були розмежовані і закріплені окремо. Зважаючи на швидкий технологічний розвиток, процеси глобалізації, економічної та соціальної інтеграції, з набранням чинності Лісабонським договором у 2009 році, у правопорядку ЄС право на захист персональних даних, закріплене у ст. 8 Хартії ЄС, затвердилося як самостійне основоположне право людини. Визначну роль у становленні та розвитку права на захист персональних даних у правопорядку ЄС відіграє Суд ЄС, який здійснює тлумачення

права ЄС у сфері захисту персональних даних, сприяє розширенню сфери захисту, наданої особам правом ЄС у сфері захисту персональних даних, забезпечує ефективний захист прав, гарантованих Хартією ЄС, сприяє реалізації на практиці принципу поваги до прав людини та зміцненню правопорядку ЄС. У цьому аспекті в діяльності Суду ЄС вирізняються преюдиційні рішення, у яких Суд ЄС втілює свої повноваження щодо тлумачення права ЄС і які є обов'язковими для всіх національних судів держав-членів ЄС, коли вони застосовують ці конкретні положення в окремих справах. Практичне застосування Хартії ЄС на практиці здійснює Суд ЄС, який має виключні повноваження щодо тлумачення обсягу права на захист персональних даних, а також ключових аспектів, пов'язаних з його ефективною реалізацією у світлі права ЄС у цій сфері.

3.4 Практика Суду Європейського Союзу щодо захисту персональних даних

Виникнення і розвиток права на захист персональних даних у правовому полі ЄС, перш за все, було зумовлено необхідністю забезпечення економічних інтересів і інтеграції внутрішнього ринку ЄС. Розглядаючи справи та ухвалюючи преюдиційні рішення щодо тлумачення правових норм, що гарантують право на приватність та право на захист персональних даних Суд ЄС не тільки сприяє однаковому застосуванню права ЄС у цій сфері, а й забезпечує баланс національних інтересів, інтересів ЄС та інтересів особи у зв'язку з обробкою персональних даних і закріплює норми щодо вільного руху таких даних між державами-членами ЄС.

У своїх перших рішеннях щодо тлумачення положень Директиви 95/46/ЄС, наприклад справи *Bodil Lindqvist* (§§39-41) та *Tietosuojavaltuutettu v. Satakunnan Markkinapörssi Oy and Satamedia Oy* (§§41-43) Суд ЄС наголосив, що вона має дуже широку сферу застосування, яка не залежить у кожному випадку від прямого зв'язку з функціонуванням внутрішнього ринку, в якому забезпечується вільний рух товарів, осіб, послуг і капіталу, і в принципі може охоплювати інші сфери політики ЄС [248; 261]. Дійсно, матеріальна сфера застосування Директиви 95/46/ЄС, так само як і чинного Загального регламенту про захист даних поширювалася на обробку даних повністю чи частково із застосуванням автоматизованих засобів та неавтоматизованих засобів, які є частиною картотеки чи призначенні для внесення в останню [42; 47]. Право ЄС у сфері

захисту даних, втім, передбачає два винятки: по-перше, обробка здійснюється в ході діяльності поза сферою дії права ЄС, наприклад, у ході діяльності щодо національної безпеки чи Спільної зовнішньої та безпекової політики ЄС, і в будь-якому випадку, коли це стосується громадської безпеки, оборони, державної безпеки чи правоохоронних органів, в тому числі діяльності щодо запобігання, розслідування, виявлення або переслідування за вчинення кримінальних злочинів або для виконання кримінальних покарань, і по-друге, обробка здійснюється фізичною особою під час суто особистої чи побутової діяльності. Виняток для обробки даних, що стосуються громадської безпеки та правоохоронних органів, було розтлумачено Судом ЄС у відомій справі *European Parliament v. Council of the European Union and Commission of the European Communities,* що стосувалася питання передачі даних пасажирів авіакомпаній з ЄС до США в безпекових цілях, що було викликано терористичними атаками 11 вересня 2001 року. Суд ЄС, зокрема, наголосив, що той факт, що персональні дані збиралися приватними перевізниками першочергово задля комерційних цілей, тобто в рамках сфери дії права ЄС, не змінює того, що передача таких даних здійснюється для цілей громадської безпеки і діяльності держав у сфері кримінального права, а відтак вона виключена зі сфери застосування Директиви 95/46/ЄС (§§56-59, 67-69) [260].

Що стосується обробки персональних даних фізичною особою в ході суто особистої чи побутової діяльності, то Суд ЄС підкреслив, що це виключення стосується лише діяльності, яка здійснюється в ході приватного чи сімейного життя осіб, що вочевидь не застосовується до ситуацій, коли персональні дані стають доступними для невизначеного або необмеженого кола людей, наприклад, внаслідок публікації в мережі Інтернет, як це було у справі *Bodil Lindqvist* чи справі *Satakunnan Markkinapörssi Oy and Satamedia Oy* [248; 261]. Примітно, що у справі *František Ryneš v. Úřad pro ochranu osobních údajů* Суд ЄС дійшов висновку, що не може розглядатися як «суто особиста або побутова» діяльність, яка поширюється, хоч навіть і частково, на публічний простір і, відповідно, спрямована за межі приватного середовища особи, яка обробляє дані таким чином (§33) [262].

У контексті гарантування права на захист персональних даних важливу роль відіграють принципи, концепції, підходи та інтерпретаційні техніки, що застосовуються

Судом ЄС. У цьому аспекті, слід враховувати, що відповідно до усталеної практики Суду ЄС тлумачення положення права ЄС вимагає врахування не лише його формулювання, але і контексту, цілей і мети, яка переслідується актом, частиною якого є це положення. Крім того, якщо положення права ЄС відкрите для кількох тлумачень, перевагу слід надавати тому тлумаченню, яке гарантує, що положення зберігає свою ефективність [263].

Одним з найважливіших принципів, що застосовується Судом ЄС є *принцип пропорційності*, який є загальним принципом діяльності ЄС, що визначає обмеження повноважень ЄС *vis-a-vis* держав-членів. Примітно, що *принцип пропорційності* часто згадується у тексті Загального регламенту про захист даних і, зокрема, ст. 23 вимагає від держав-членів запроваджувати обмеження щодо захисту персональних даних у пропорційний спосіб. Професори П. Крейг та Г. де Бурка стверджують, що як загальний принцип права ЄС принцип пропорційності передбачає такі три складові: 1) чи є запроваджуваний захід придатним для досягнення законної мети, 2) чи є захід необхідним для досягнення цієї мети, 3) чи накладає захід тягар на особу, який є надмірним щодо мети, яку прагнуть досягти (пропорційність *stricto sensu*) [245, с. 583]. Як зазначає науковець Л. Далла Корто заходи, що застосовуються, у разі, якщо вони є відповідними, необхідними і *stricto sensu* пропорційними у світлі цілей, на досягнення яких вони спрямовані, можна вважати *lato sensu* пропорційним [264, с. 262]. У цьому контексті професор Е. Герлін-Карнелл зауважує, що перевірка балансу між запроваджуваними обмеженнями та цілями, які вони переслідують, тобто пропорційність у вузькому сенсі (*stricto sensu*), безсумнівно, є найважливішим аспектом принципу пропорційності в контексті захисту персональних даних в ЄС [265, с. 74].

Принцип пропорційності виступає головною передумовою обмеження права на захист персональних даних, адже це право не є абсолютним та має розглядатися з огляду на його функцію у суспільстві і бути збалансованим щодо інших основоположних прав [266, с. 6]. З урахуванням частини 1 статті 52 Хартії ЄС, обмеження щодо основоположних прав, гарантованих Хартією ЄС, має бути: 1) передбачено законом, 2) поважати саму сутність права, яке обмежується, 3) здійснюватися з дотриманням принципу пропорційності, 4) має бути необхідним та справді відповідати цілям

загального інтересу, визнаного ЄС, або бути необхідними для захисту прав інших осіб [45]. Зважаючи на те, що право на захист персональних даних визнано самостійним основоположним правом у системі права ЄС, будь-яка обробка персональних даних сама собою становитиме втручання, не залежно від того чи мають відношення персональні дані до приватного життя особи, чи є вони чутливими, або чи відчули суб'єкти персональних даних будь-які незручності. Задля того, щоб бути правомірним, таке втручання має відповідати всім умовам, передбаченим частиною 1 статті 52 Хартії ЄС [84, с. 47].

Екстраполюючи вказаний принцип у сферу захисту персональних даних, варто наголосити на тому, що принцип пропорційності, згадуваний у ст. 8 та 52 Хартії ЄС не є тотожними. *Принцип пропорційності*, що згадується у ст. 8 Хартії ЄС стосується того, як повинні оброблятися персональні дані, тобто він розглядається як конститутивна риса основоположного права на захист персональних даних, у той час, як пропорційність, що закріплена у ст. 52 Хартії ЄС, є вимогою стосовно можливих обмежень права на захист персональних даних у контексті визначення правомірності такого обмеження. З огляду на практику Суду ЄС *принцип пропорційності* за частиною 1 статті 52 Хартії ЄС є суворою вимогою, якої потрібно дотримуватися, адже будь-які обмеження права на захист персональних даних мають застосовуватися лише настільки, наскільки це вкрай необхідно [74; 212; 218; 246; 261].

Згідно з усталеною практикою Суду ЄС, зокрема у рішенні *Volker und Markus Schecke GbR (C-92/09) and Hartmut Eifert (C-93/09) v. Land Hessen*, головна вимога *принципу пропорційності* полягає в тому, що акти інституцій ЄС мають відповідати законним цілям, які переслідує відповідне законодавство, і не виходити за рамки того, що є доцільним і необхідним для досягнення цих цілей (§§72-74) [246]. Отже, *принцип пропорційності* у широкому розумінні охоплює вимоги необхідності та відповідності запроваджуваного заходу, тобто повинен існувати логічний зв'язок між таким заходом та переслідуваної законної мети. Примітно, що для оцінки пропорційності Суд ЄС спочатку встановлює чи був запроваджуваний захід необхідним, тобто здійснює засновану на фактах оцінку ефективності заходу для досягнення поставленої мети та оцінки того, чи порівняно з іншими заходами досягнення тієї ж мети оскаржуваний захід

передбачає менший ступінь втручання [266, с. 9-10]. Наприклад, у справі *Digital Rights Ireland* Суд ЄС не здійснював оцінку пропорційності після того, як встановив, що обмеження права на приватність та права на захист персональних даних, гарантованих ст. 7 і 8 Хартії ЄС, не були суворо необхідними. У цій справі Суд ЄС також постановив, що: *«якщо йдеться про втручання в основоположні права, обсяг дискреційних повноважень законодавчого органу ЄС може виявитися обмеженим залежно від низки факторів, включаючи, серед іншого, відповідну сферу, характер гарантованого Хартією ЄС права, про яке йдеться, характер і серйозність втручання та мету втручання»* (§47). Понад те, Суд ЄС наголосив, що відповідне право ЄС повинно встановлювати чіткі та точні правила, що регулюють сферу застосування відповідного заходу та встановлюють мінімальні гарантії, щоб особи, чиї персональні дані були збережені, мали достатні гарантії для ефективного захисту своїх персональних даних від ризику зловживання та проти будь-якого незаконного доступу і використання цих даних (§54) [218]. У цій справі Суд ЄС проаналізував вимоги Директиви про збереження даних і встановив, що оскільки дані про трафік та місце розташування, агреговані та взяті в цілому, можуть бути проаналізовані і можуть представити детальну картину приватного життя фізичних осіб, то має місце серйозне втручання у права на приватність та захист даних. Застосувавши вказані міркування, Суд ЄС підкреслив, що прийнявши Директиву про збереження даних, законодавчий орган ЄС перевищив обмеження, встановлені відповідно до принципу пропорційності у світлі ст. 7, 8 і 52 (1) Хартії ЄС та, як наслідок, визнав цю директиву нечинною.

Ці висновки Суду ЄС були розвинуті у справі *Tele2 Sveirge*, що стосувалася питання збереження даних про абонентів постачальниками електронних комунікацій. У цій справі було підсумовано вимогу стосовно того, що захід, який обмежує основоположні права, може вважатися пропорційним лише у разі якщо він є суворо необхідним та пропорційним поставленій меті. Відповідно, недоліки, спричинені такими заходами, не повинні бути непропорційними поставленим цілям. З цих причин Суд ЄС постановив, що шведське законодавство, яке дозволяє загальне, тобто таке, що не передбачає виключень, систематичне, постійне та невибіркове збереження всього трафіку та даних про місцезнаходження всіх абонентів і зареєстрованих користувачів,

що стосуються всіх засобів електронного зв'язку, навіть переслідуючи мету боротьби зі злочинністю, перевищує межі того, що є суворо необхідним і не може вважатися виправданим у демократичному суспільстві (§§92-96, 129) [212]. Примітно, що як у справі *Digital Rights Ireland* (§100), так і у справі *Tele2 Sverige* (§37) Суд ЄС наголосив, що втручання у право на приватність та право на захист даних було особливо серйозним з огляду на той факт, що дані зберігаються без інформування абонента або зареєстрованого користувача, може викликати у відповідних осіб відчуття, що їх особисте життя є предметом постійного спостереження [212; 218].

Водночас важливим компонентом зважування інтересів або балансування в кожному конкретному випадку є критерій, що стосується серйозності порушення прав суб'єкта даних. Щоб оцінити серйозність втручання, необхідно враховувати, серед іншого, характер персональних даних, про які йде мова, зокрема будь-яку чутливість цих даних, а також характер і конкретні методи обробки відповідних даних, зокрема щодо кількості осіб, які мають доступ до цих даних, і методів доступу до них (TK v. Asociaţia de Proprietari bloc M5A ScaraA, §57) [267].

Зауважимо, що не менш вагому роль *принцип пропорційності* відіграє в контексті взаємозв'язку між конкуруючими основоположними правами (fundamental rights in conflict), що є особливо актуальним у світлі нестримного технологічного розвитку в епоху цифрових технологій та всеосяжного інтернету, яка вимагає як дотримання права на захист персональних даних і права на приватність, так і їх збалансування з іншими правами, зокрема зі правом на свободу вираження поглядів, правом на отримання і розповсюдження інформації чи правом на доступ до публічних документів. Примітно, що ні в основоположних договорах ЄС, ні в самій Хартії ЄС прямо не йдеться про ієрархію основоположних прав, однак, як слушно зазначає дослідник М. Бркан, втручання у сутність права на приватність і права захист даних має визначатися в кожному конкретному випадку [268, с. 867]. Таким чином, відмінність між особливо серйозними втручаннями в основоположні права необхідно розглядати у світлі принципу пропорційності та втручання в сутність цих основоположних прав, як того вимагає частина 1 статті 52 Хартії ЄС.

У справах *Sky Österreich GmbH v. Österreichischer Rundfunk* (§60) та *Productores de Música de España (Promusicae) v. Telefónica de España SAU*, так звана справа *Promusicae* (§§65-66) Суд ЄС підкреслював, що *«якщо йдеться про кілька прав і основоположних свобод, які захищаються правопорядком Європейського Союзу, оцінка можливого непропорційного характеру положення права Європейського Союзу повинна проводитися з метою узгодження вимог захисту цих різних прав і свобод та справедливого балансу між ними»* [269; 270]. Це питання розглядалося, серед іншого, й у справі *Bavarian Lager*, де Суд ЄС вирішував питання взаємозв'язку між правом на доступ до публічних документів і правом на захист персональних даних. З цього приводу Суд ЄС дійшов висновку, що захист персональних даних переважає у ситуації, коли доступ до документів може ставити під загрозу захист приватного життя та недоторканності особи. Відтак Суд ЄС підкреслив, що право на доступ до публічних документів повинно тлумачитися обмежувально і розглядатися та оцінюватися у світлі права ЄС щодо захисту персональних даних (§§25-26) [256].

Примітно, що у справі *Promusicae* Суд ЄС розглянув питання розкриття персональних даних з метою порушення цивільного провадження щодо забезпечення ефективного захисту авторського права. Ця справа стосувалася вирішення питання про баланс права на власність, яке включає право інтелектуальної власності, права на ефективний засіб захисту, права на захист персональних даних і права на приватність. Суд ЄС підкреслив, що конфлікт основоположних прав має бути вирішений з огляду на необхідність узгодити вимоги щодо захисту тих різноманітних основоположних прав, які захищає правовий порядок ЄС, і знайти справедливий баланс між ними (§§61, 65-69) [270]. Слід приділити належну увагу міркуванням у справі *Bavarian Lager*, адже Суд ЄС визнав, що в контексті доступу до документів, що містять персональні дані, право на захист даних переважає над принципом прозорості діяльності та процесу прийняття рішень публічними органами (§§49-50) [256]. Крім того, у справі *Peter Puškár v. Finančné riaditeľstvo Slovenskej republiky and Kriminálny úrad finančnej správy* Суд ЄС звернув особливу увагу на той факт, що захист основоположного права на повагу до приватного життя на рівні ЄС вимагає, щоб відступи від захисту персональних даних та його обмеження здійснювалися в межах того, що суворо необхідним (§§112) [271].

Серйозним викликом є також забезпечення балансу між правом на свободу вираження поглядів і правом на захист персональних даних. Це питання було розглянуто у справі *Bodil Lindqvist*, де Суд ЄС постановив, що розміщення персональних даних осіб на інтернет-сторінці, зробила їх доступними для невизначеної кількості людей, всупереч виняткам, передбаченим статтею 3 (2) Директиви 95/46/ЄС, які стосується діяльності, яка виходить за межі права ЄС, та особистої чи побутової діяльності. Ці міркування привели до висновку, що у цій справі обробка даних не відповідала вимогам Директиви 95/46/ЄС, а право на захист персональних даних переважало над правом на свободу вираження поглядів (§§47, 81-82) [248]. Водночас у справі *Sergejs Buivids v. Datu valsts inspekcija*, яка стосувалася адміністративного провадження щодо заявника, який зробив відеозапис у латвійській поліцейській дільниці, нібито через неправомірну поведінку поліції, і згодом опублікував його в мережі, Суд ЄС дійшов висновку, що відеозапис не підпадає під обробку персональних даних виключно для *«особистого та побутового використання»*, адже після публікації на YouTube його може переглядати необмежена аудиторія. Втім, врахувавши конкретні обставини цієї справи, Суд ЄС вирішив, що може бути застосовано виключення щодо діяльності журналістів. Суд ЄС також посилався на практику ЄСПЛ, звертаючи увагу на відповідні критерії, а саме: 1) внесок у дебати, що становлять суспільний інтерес, 2) ступінь відомості постраждалої особи, 3) тематику новинного повідомлення, 4) зміст, форму та наслідки публікації, а також 5) спосіб і обставини, за яких була отримана інформація (§§48, 65-69) [272].

Зауважимо, що у справах щодо захисту персональних даних Суд ЄС також використовував *доктрину свободи розсуду*. У цьому аспекті варто наголосити, що *доктрина свободи розсуду* є більш притаманною ЄСПЛ та передбачає, що застосування ЄКПЛ не обов'язково є однаковим у всіх державах-членах, тоді як застосування Хартії ЄС менше стосується національних особливостей і виступає за безумовне дотримання єдиних стандартів захисту, встановлених у ній. Суд ЄС у справі *Stefano Melloni v. Ministerio Fiscal* вказав, що Стаття 53 Хартії ЄС підтверджує, що, якщо правовий акт ЄС вимагає національних імплементаційних заходів, національні органи влади та суди залишаються вільними застосовувати національні стандарти захисту основних прав за умови, що рівень захисту, передбачений Хартією ЄС, а також примат, єдність і

ефективність права ЄС таким чином не порушуються (§60) [273]. Суд ЄС також наголошував у справі *Bodil Lindqvist*, що положення директив є відносно загальними, оскільки вони повинні застосовуватися до великої кількості різних ситуацій, які можуть виникнути в будь-якій державі-члені ЄС. Тому вони логічно включають правила, які залишають державам-членам необхідну свободу дій для визначення засобів імплементації відповідних норм, які можуть бути адаптовані до різних можливих ситуацій (§84) [248]. Крім того, у справі *Heinz Huber v. Bundesrepublik Deutschland* було також зауважено, що гармонізація національних законів не обмежується мінімальною гармонізацією, але становить гармонізацію, яка загалом є повною (§51) [274].

Відтак у контексті захисту персональних даних *доктрина свободи розсуду* переважно застосовувалася у контексті тлумачення положень Директиви 95/46/ЄС та оцінки свободи дій держав щодо імплементації її норм у національне законодавство. Примітно, що у пункті 10 преамбули Директиви 95/46/ЄС наголошено, що наближення національних законів про обробку персональних даних не повинно призводити до будь-якого зменшення захисту, який вони забезпечують, а має, навпаки, прагнути забезпечити високий рівень захисту у ЄС [275, с. 225].

У справі *Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF), Federación de Comercio Electrónico y Marketing Directo (FECEMD) v Administración del Estado* (далі – справа *ASNEF ma FECEMD*), що стосувалася критеріїв законної обробки персональних даних, Суд ЄС дійшов висновку, що Іспанія неправильно імплементувала в національне законодавство ст. 7 (f) Директиви 95/46/ЄС, вимагаючи, щоб – за відсутності згоди суб'єкта даних – будь-які дані, що оброблялися, з'явилися в загальнодоступних джерелах. Суд ЄС постановив, що ст. 7 (f) Директиви 95/46/ЄС має пряму дію, а відтак обмежує свободу розсуду, яку мають держави-члени щодо її імплементації. Зокрема, вони не повинні переступати тонку межу між уточненням чи роз'ясненням, з одного боку, та встановленням додаткових вимог, які б змінили сферу застосування ст. 7 (f) Директиви 95/46/ЄС, з іншого боку. Таким чином, свобода розсуду, яку мають держави-члени згідно зі ст. 5 Директиви 95/46/ЄС, може використовуватися лише відповідно до мети, яка переслідується Директивою 95/46/ЄС та полягає у

підтриманні балансу між вільним рухом персональних даних і захистом приватного життя (§35) [276].

Зауважимо, що з урахуванням ст. 288 ДФЄС норми Загального регламенту про захист даних є обов'язковими у всіх своїх складових і підлягають прямому застосуванню в усіх державах-членах ЄС, тобто застосовуються безпосередньо і не вимагають їх імплементації у національне законодавство. Відповідно, свобода дій держави у цьому аспекті буде обмеженою нормами самого регламенту, який вимагатиме внесення поправок у національні закони задля узгодження з його положеннями. Втім, Загальний регламент про захист даних не забороняє державам встановлювати більш широкі норми, наприклад, стосовно правил обробки чутливих даних, в тому числі більш точно визначити умови, за яких обробка персональних даних є законною чи передбачити спеціальні правила щодо обробки персональних даних померлих осіб, тому в цьому контексті свобода розсуду може бути застосовна. Іншим аспектом свободи розсуду держав є те, що національні органи влади та суди залишаються вільними застосовувати національні стандарти захисту персональних даних [275, с. 226].

Водночас з урахуванням положень ст. 267 ДФЄС обов'язком національних судів у співробітництві з Судом ЄС є забезпечення однакового тлумачення положень Загального регламенту про захист даних у ЄС. У такому разі Суд ЄС ймовірніше за все надаватиме перевагу *принципу верховенства*, що полягає у верховенстві права ЄС над національним правом. Як зауважує професор А. Лазовські, ця загальноприйнята фундаментальна доктрина права ЄС має практичне значення та походить з судової практики, зокрема рішень *Costa v. ENEL* та *Van Gend en Loos*. Понад те, з урахуванням рішення у справі *Simmenthal* всі національні суди, коли стикаються із національним законодавством, яке безпосередньо порушує чинне право ЄС, мають обов'язок залишити поза увагою національні правила і вирішити справу на основі права ЄС [277, с. 35, 39]. Водночас важливе практичне значення у поєднанні з *принципом верховенства права ЄС*, традиційно, мають й такі принципи, розроблені Судом ЄС як: 1) *принцип прямої дії*, що дозволяє особам безпосередньо посилатися на основі норми права ЄС і домагатися їх реалізації через національні суди [278, с. 18-19], що в контексті захисту персональних даних означає, що чіткі, точні та однозначні зобов'язання породжують

визначені індивідуальні права, на які може посилатися особа в національних судах, як Суд ЄС наголосив в об'єднаній справі *ASNEF та FECEMD* (§§51-55) [279], 2) *принцип непрямої дії*, згідно з яким національні суди зобов'язані тлумачити національне законодавство відповідно до права ЄС, що включає всі джерела права ЄС, у тому числі акти м'якого права, наприклад, рекомендації Європейської ради із захисту даних (EDPB), висновки, рамкові акти чи кодекси поведінки [279, с. 101], 3) *принцип відповідальності держави*, що виникає у разі, якщо ні пряма, ні непряма дія права ЄС не призводить до бажаних результатів, а має наслідком достатньо серйозне порушення прав, гарантованих правом ЄС, що сталося із вини широкого кола національних органів, а, за певних обставин, також національних судів [279, с. 103].

Зауважимо, що у контексті захисту персональних даних із зазначеними вище принципами тісно пов'язаний й *принцип еквівалентного захисту*. Варто зазначити, що Директива 95/46/ЄС мала на меті, як випливає, серед іншого, з пункту 8 її преамбули, забезпечити рівноцінний (еквівалентний) рівень захисту прав людини щодо обробки персональних даних в усіх державах-членах. Дійсно, Суд ЄС наголошував, що гармонізація національних законів має дорівнювати гармонізації, яка загалом є повною [248]. У справі *ASNEF та FECEMD* було наголошено, що з метою забезпечення еквівалентного рівня захисту в усіх державах-членах випливає, що стаття 7 Директиви 95/46/ЄС встановлює вичерпний та обмежувальний перелік випадків, у яких обробка персональних даних може вважатися законною. З цього випливає, що держави-члени не можуть додавати нові принципи, що стосуються законності обробки персональних даних, до статті 7 Директиви 95/46/ЄС або встановлювати додаткові вимоги, які мають наслідком зміну сфери застосування одного з шести принципів, передбачених у цій статті (§§30, 32) [276]. Зокрема, у справі *Heinz Huber* розглядаючи питання обробки даних відповідно до ст. 7 (e) Директиви 95/46/ЄС, тобто у разі коли обробка необхідна в цілях законних інтересів контролера чи третіх осіб, Суд ЄС зауважив, що з огляду на мету забезпечення еквівалентного рівня захисту в усіх державах-членах, концепція необхідності, викладена в ст. 7(e) Директиви 95/46/ЄС, мета якої полягає в тому, щоб точно розмежувати одну із ситуацій, у яких обробка персональних даних є законною, не може мати значення, яке різниться між державами-членами. Звідси випливає, що

йдеться про концепцію, яка має власне незалежне значення в праві ЄС і яку слід тлумачити таким чином, щоб повністю відображати мету Директиви 95/46/ЄС, яка закріплена у її ст. 1 (§52) [274].

Примітно, що у пункті 10 Преамбули до Загального регламенту про захист даних також наголошується, що рівень захисту прав людини щодо обробки таких даних має бути еквівалентним у всіх державах-членах задля забезпечення послідовного і високого рівня захисту, а також усунення перешкод для руху персональних даних у межах ЄС. Крім того, у пункті 101 його Преамбули наголошується на важливості забезпечення вільного потоку персональних даних до країн та з країн поза межами ЄС, що є необхідними для розширення міжнародної торгівлі та міжнародного співробітництва, однак варто забезпечити рівень захисту персональних даних фізичних осіб, який не буде нижчим за рівень, який забезпечується цим регламентом [47].

Відповідно, *принцип еквівалентного захисту* пов'язаний також із забезпеченням належного рівня захисту у разі передачі персональних даних у третю країну поза межами ЄС чи міжнародну організацію на основі рішення Європейської Комісії про адекватний рівень захисту, яке є обов'язковим для держав-членів і таким чином гарантуватиме правову визначеність і однорідність у межах ЄС. У такому разі третя країна повинна запропонувати гарантії, що забезпечують адекватний рівень захисту, по суті еквівалентний тому, що забезпечується в межах ЄС. Серед іншого, третя країна повинна надати гарантії, що забезпечують належний рівень захисту та передбачають дієвий нагляд за захистом персональних даних, механізми співробітництва з органами із захисту даних держав-членів ЄС, а також надати суб'єктам даних ефективні права, які можна реалізувати, та дієві адміністративні і судові засоби правового захисту. На цьому аспекті було наголошено у знакових рішеннях Суду ЄС у справах *Schrems* (§§72, 96, 97) та *Schrems II* (§§92-96), внаслідок ухвалення яких були визнані недійсними угоди, якими було впроваджено правові режими Safe Harbour та EU-U.S. Privacy Shield, що передбачали режим передачі персональних даних з ЄС до США. Хоч Суд ЄС і наголошував, що третя країна, до якої передаються персональні дані, не повинна забезпечувати рівень захисту даних ідентичний тому, що гарантується в ЄС, але вона має забезпечити захист по суті еквівалентний рівню захисту в ЄС. Проаналізувавши

згадані правові режими передачі даних між ЄС та США Суд ЄС дійшов висновку, що рівень захисту в США не відповідав цьому критерію, адже не передбачав достатніх гарантій, які б обмежували доступ розвідувальних органів США до персональних даних, які передаються і надавали б належні гарантії суб'єктам даних [74*;* 76].

Примітно, що *принцип еквівалентного захисту* також стосується взаємовідносин між Судом ЄС та ЄСПЛ в контексті захисту основоположних прав. Вважається, що в контексті взаємодії правових систем ЄС та ЄКПЛ *принцип еквівалентного захисту* був сформований ЄСПЛ у справі *Bosphorus Hava Yolları Turizm ve Ticaret Anonim Şirketi v. Ireland*. Він передбачає, що існує презумпція, згідно з якою ЄС забезпечує рівень захисту основоположних прав, який є еквівалентний, що означає «порівнянний», а не «ідентичний», тому, що встановлений в ЄКПЛ (так звана Босфорська презумпція). Однак ЄСПЛ також зауважив, що *«якщо з огляду на обставини конкретної справи стає очевидним, що захист прав, передбачених Конвенцією, був явно недостатнім, презумпцію можна спростувати і можна встановити порушення Конвенції»* (§§155-156) [280]. Вочевидь, інтерпретаційні інструменти та методи, що використовуються ЄСПЛ та Судом ЄС є подібними, адже спрямовуються на досягнення однієї мети – гарантування основоположних прав людини, включаючи право на приватність та право на захист персональних даних. Однак ЄСПЛ не має юрисдикції скасовувати національні закони чи адміністративну практику, які порушують ЄКПЛ, але може висловити поради щодо їх скасування чи внесення змін. Суд ЄС, навпаки, посилається на принцип верховенства ЄС, принцип прямої дії та принцип відповідальності держави, таким чином зобов'язуючи державу змінити чи анулювати національне законодавство, яке буде визнано таким, що порушує право ЄС. Ці два суди хоч і не пов'язані між собою, але вони мають по суті ідентичні підходи щодо приватності та захисту даних. Таким чином, з метою забезпечення правової визначеності вони часто перехресно посилаються на практику один одного, сприяючи створенню «єдиного стандарту прав людини». Відтак, розглядаючи справи щодо порушення права на захист персональних даних Суд ЄС тлумачить Хартію ЄС і відповідне право ЄС з урахуванням практики ЄСПЛ, однак Суд ЄС не зв'язаний цією практикою, адже згідно зі ст. 52 (3) Хартії ЄС значення та обсяг гарантованих нею прав є такими ж, як і у відповідній статті ЄКПЛ, однак це не

перешкоджає праву ЄС гарантувати більш широкий захист. У цьому аспекті варто зауважити, що право на захист персональних даних безпосередньо не закріплене в ЄКПЛ чи Протоколах до неї, а походить з практики ЄСПЛ, в той час, як Хартія ЄС гарантує його на рівні з правом на приватність. Відповідно, Суд ЄС враховує відповідну практику ЄСПЛ, а також викладені в ст. 8 ЄКПЛ механізми обмеження, які застосовуються до права на приватність та права на захист персональних даних, водночас запобігаючи негативному впливу на автономію права ЄС та Суду ЄС. Водночас ЄСПЛ розглядаючи справи щодо захисту персональних даних тлумачить основні стандарти захисту даних, закріплені у Конвенції № 108, а також праві ЄС та практиці Суду ЄС. Відтак, співпраця Суду ЄС та ЄСПЛ спрямована на забезпечення і гарантування еквівалентного рівня захисту основоположного права на захист персональних даних. У цьому аспекті варто звернути увагу на перспективи приєднання ЄС до ЄКПЛ, що, як зазначає дослідниця Л. Г. Фалалєєва, сприяло б запобіганню юрисдикційним конфліктам і правовим колізіям, дало б змогу уникнути розбіжностей у тлумаченні норм у сфері прав людини Судом ЄС та ЄСПЛ, а також уможливило б поступове формування загальноєвропейської системи захисту прав людини на основі функціонуючих у ЄС та РЄ систем захисту прав людини [90, с. 173-175].

Водночас в контексті захисту персональних даних важливим принципом також є *принцип ефективності*, який, як зазначив Суд ЄС у справі *East Sussex County Council v. Information Commissioner and Others,* означає, що детальні процесуальні правила, які регулюють дії щодо захисту прав, наданих правом ЄС, не повинні робити на практиці неможливим або надмірно ускладненим здійснення цих прав (§§52-55) [281]. Понад те, у справах *Google Spain* (§38) та нещодавній справі *TU, RE v. Google LLC* (§51), що стосувалися обробки даних пошуковою системою Google, Суд ЄС наголосив, що оскільки діяльність пошукової системи може суттєво вплинути на основоположні право на приватне життя і право захист персональних даних, оператор пошукової системи повинен забезпечувати, в рамках своїх обов'язків, повноважень і можливостей, щоб така діяльність відповідала вимогам Директиви 95/46/ЄС і Загальному регламенту про захист даних для того, щоб гарантії, встановлені останніми,

могли мати повну силу і щоб ефективний і повний захист суб'єктів даних міг бути фактично досягнутий [237; 282].

Принцип ефективності також безпосередньо пов'язаний з правом отримати ефективний засіб захисту у разі порушення права на захист персональних даних, як це гарантовано ст. 47 Хартії ЄС. Примітно, що у справі *BE v. Nemzeti Adatvédelmi és Információszabadság Hatóság* Суд ЄС постановив, що різні засоби правового захисту, передбачені Загальним регламентом про захист даних, а саме: право подати скаргу до наглядового органу (ст. 77); право на ефективний судовий захист проти наглядового органу (ст. 78) та право на ефективний судовий захист проти контролера або процесора (ст. 79), можуть використовуватися незалежно одне від одного та одночасно. Суд ЄС звернув увагу, що не існує ієрархії між цивільними та адміністративними засобами правового захисту, а також немає правила пріоритету. Однак паралельні процедури можуть призвести до суперечливих результатів з боку різних залучених органів. Саме тому держави-члени ЄС повинні вирішувати ці конфлікти за допомогою детальних національних процедурних правил, забезпечуючи при цьому право особи на ефективний засіб правового захисту та ефективний захист її прав відповідно до регламенту (§§53-57) [283].

Зауважимо, що у світлі стрімкого технологічного розвитку і глобалізації виникають більш складні та прогресивні справи, зокрема, щодо забезпечення персональних даних у контексті використання штучного інтелекту, масового перехоплення даних чи використання інноваційних технологій. З огляду на нові виклики, що постали перед захистом персональних даних, Суд ЄС все частіше використовує й *принцип недискримінації*, особливо в контексті обробки чутливих даних, особливості обробки яких визначені у ст. 9 Загального регламенту про захист даних. Питання недискримінації розглядалося у справі *Heinz Huber*, що стосувалася системи обробки персональних даних громадян ЄС, які не є громадянами відповідної держави-члена, в контексті боротьби зі злочинністю і захистом публічного порядку. Суд ЄС дійшов висновку, що впровадження такої системи, коли обробка обмежена даними громадян ЄС, які не є громадянами відповідної держави-члена, та не стосується громадян такої держави-члена є дискримінацією за ознакою національності (§§75-80)

[274]. На цей принцип Суд ЄС звернув увагу у справі *La Quadrature du Net and Others v. Premier ministre and Others*, яка стосувалася обов'язку постачальників електронних комунікаційних послуг здійснювати загальну та невибіркову передачу даних трафіку та даних про місцезнаходження користувачів службам безпеки та розвідувальним службам. Зокрема, Суд ЄС підкреслив, що за певних обставин такі заходи можуть здійснюватися з метою захисту національної безпеки, боротьби з серйозними злочинами і запобігання серйозним загрозам громадській безпеці, але рішення про дозвіл на збір таких даних має ґрунтуватися на об'єктивних і недискримінаційних критеріях, передбачених національним законодавством (§168) [284].

З розвитком інноваційних технологій та використанням алгоритмічних інструментів, нейронних мереж, технологій профайлінгу та систем штучного інтелекту викликом для захисту персональних даних постало питання так званої алгоритмічної дискримінації. Пов'язані із використанням систем штучного інтелекту ризики дискримінації можуть бути як наслідком недоліків у загальній конструкції систем штучного інтелекту, зокрема, щодо спостереження за людьми (англ. human observation), так і наслідком використання помилково-упереджених даних через викривленість початкових даних, наприклад, коли система навчається з використанням лише або переважно даних, наданих чоловіками, що призводить до неоптимальних результатів щодо жінок. Водночас аналізуючи великі обсяги даних і виявляючи зв'язки між ними, штучний інтелект також може використовуватися для повторного відстеження та деанонімізації даних про осіб, створюючи нові ризики для захисту персональних даних навіть щодо наборів даних, які самі по собі не містять персональних даних [285]. Таким чином, можна виділити такі основні проблеми, пов'язані із використанням штучного інтелекту, що можуть призвести до алгоритмічної дискримінації, як: 1) збільшення потенціалу постійного спостереження за людьми, 2) накопичення великих обсягів персональних даних користувачів, 3) потенціал деанонімізації великих наборів даних, 4) непрозорий процес прийняття рішень, 5) створення дискримінаційних результатів.

Зауважимо, що право ЄС має доволі розвинуті інструменти щодо захисту від дискримінації, що застосовується й в контексті захисту даних незалежно від залучення штучного інтелекту чи інших алгоритмічних інструментів, але ризики, які вони

створюють, мають бути оцінені в кожній ситуації з метою коригування та удосконалення конкретних правових інструментів. Так, Загальний регламент про захист даних, серед іншого, підлягає застосуванню до частково або повністю автоматичних систем штучного інтелекту, які обробляють персональні дані, що є частиною або мають бути частиною системи зберігання даних. Одним із запобіжників в контексті запобігання алгоритмічній дискримінації виступає стаття 22 Загального регламенту про захист даних згідно з якою суб'єкт даних повинен мати право не підлягати рішенню, що ґрунтується виняткова на автоматизованій обробці, в тому числі профайлінгу [47]. Іншим запобіжником виступає вимога отримання поінформованої згоди на обробку персональних даних, що включає, серед іншого, вимогу довести до суб'єкта даних у зрозумілій формі яким чином та з якою метою відбувається обробка даних. У цьому аспекті погоджуємося з дослідницею Ф. Уферт, що використання повністю чи частково автоматизованих систем штучного інтелекту обмежено за Загальним регламентом про захист даних завдяки принципу відповідальності контролера даних, як наголосив Суд ЄС у справах *Google Spain*, яка стосувалася обов'язку оператора пошукової системи, як контролера даних, за певних умов видалити персональні дані користувача з результатів пошуковика, та *GC and Others v. CNIL*, яка стосувалася відповідальності оператора пошукової системи під час отримання запиту на видалення посилань збалансувати право на захист персональних даних з іншими правами, на які може вплинути видалення відповідних посилань, наприклад, права на свободу інформації. Також примітно, що хоч Загальний регламент про захист даних і застосовується до обробки персональних даних повністю автоматизованими засобами, але він також забороняє використання повністю автономних систем штучного інтелекту для обробки персональних даних, що створює юридичні наслідки для осіб [286, с. 1092-1093].

Варто зауважити, що 21 квітня 2021 року в ЄС була прийнята Пропозиція 2021/0106 (COD) щодо ухвалення Регламенту Європейського Парламенту та Ради Про встановлення гармонізованих правил щодо штучного інтелекту (Акт про штучний інтелект) та внесення змін до деяких законодавчих актів ЄС. Вказаним актом передбачається доповнення Загального регламенту захисту даних і Директиви 2016/680 про правоохоронну діяльність набором узгоджених правил, що застосовуються до

проєктування, розробки та використання певних систем штучного інтелекту з високим ризиком і обмеження окремих випадків використання систем дистанційної біометричної ідентифікації. Крім того, чинне право ЄС про недискримінацію доповнюється конкретними вимогами, спрямованими на мінімізацію ризику алгоритмічної дискримінації, регламентуючи перелік заборонених практик використання штучного інтелекту, які використовують вразливість певної групи осіб, наприклад, через їх вік або фізичні чи розумові вади, а також регулює особливості використання високоризикованих систем штучного інтелекту та зобов'язань щодо прозорості, зокрема, у разі використання технології «діпфейк» (англ. deepfake AI) [228].

Відтак з розвитком технологій поступово оновлюються й відповідні правові механізми ЄС задля того, щоб протистояти відповідним викликам та ризикам, а також забезпечити рівність та запобігти дискримінації, зокрема й алгоритмічній дискримінації. Відповідно, з використанням інформаційних технологій, технологій штучного інтелекту, алгоритмічних інструментів *принцип недискримінації* набуде подальшого розвитку у практиці Суду ЄС у контексті захисту персональних даних.

Проаналізувавши підходи, застосовані у практиці Суду ЄС, можна зробити однозначний висновок, що Суд ЄС у своїх рішеннях оцінює право на захист даних у зв'язку з його безпрецедентною роллю в суспільстві та оцінює пропорційність втручання у право на захист персональних даних у кожній конкретній справі. Варто зауважити, що Суд ЄС оцінює кожну справу із позиції дотримання зобов'язань та принципів захисту персональних даних, визначених в Загальному регламенті про захист даних, а у справах, розглянутих раніше – визначених у Директиві 95/46/ЄС, у поєднанні із застосуванням низки концептуальних підходів та принципів, які сприяють всебічному аналізу конкретної справи та забезпечують єдність у тлумаченні права ЄС у сфері захисту персональних даних. У справах, пов'язаних з питанням захисту персональних даних, одним з найважливіших виступає принцип пропорційності, який є головною передумовою обмеження права на захист персональних даних та використовується для оцінки рівня втручання в право особи на приватність та захист персональних даних, з одного боку, та інші основоположні права, приватні чи публічні інтереси, з іншого боку. Щоправда, на відміну від традиційного трискладового тесту, що застосовується ЄСПЛ,

оцінюючи правомірність втручання в право на захист персональних даних окрім законності, необхідності та пропорційності Суд ЄС також повинен встановити чи була забезпечено саму суть права на захист персональних даних та чи відповідають обмеження цілям загального інтересу, що визнаний ЄС, або є необхідними для захисту прав інших осіб.

Вагому роль у гарантуванні права на захист персональних даних відіграють також *доктрина свободи розсуду* та *принцип верховенства права ЄС*, які сприяють уніфікації правових норм щодо захисту персональних даних на території ЄС та єдності у їх правозастосуванні. Важливим в цьому контексті виступає й *принцип ефективності*, а також *принцип еквівалентного захисту*. Водночас з розвитком технологій в контексті захисту персональних даних актуальності набуває *принцип недискримінації*. Особливу роль у захисті персональних даних відіграє також *принцип пропорційності*, який дозволяє досягти справедливого балансу між конкуруючими інтересами, правами і свободами. Зауважимо, що усі принципи, коцепції, підходи та інтерпретаційні техніки, що застосовуються Судом ЄС є взаємопов'язаними та взаємодоповнюючими. Послідовність підходів Суду ЄС сприяє належному рівню захисту права на захист персональних даних у світлі більш складних та прогресивних справ, які, серед іншого, включають питання забезпечення персональних даних у контексті використання штучного інтелекту, масового перехоплення даних чи використання інноваційних технологій.

Висновки до Розділу 3

Вивчення джерел первинного та вторинного права ЄС, правового регулювання ЄС у сфері захисту персональних даних та особливостей захисту персональних даних у діяльності Суду ЄС дає змогу сформувати такі висновки.

У правопорядку ЄС право на захист персональних даних є основоположним правом на рівні з правом на приватне життя. Захист персональних даних як одне з основоположних прав людини гарантується ефективним поєднанням різних правових інструментів ЄС, зокрема його установчих договорів і Хартії ЄС, а також актів вторинного права ЄС.

Правове регулювання ЄС у сфері захисту персональних даних вирізняється наявністю значного масиву законодавчих актів, які детально регламентують питання обробки персональних даних та містять стандарти захисту даних, спрямовані на забезпечення захисту прав людини при обробці їх даних. Чільне місце серед актів вторинного права ЄС займає Загальний регламент про захист даних, який скасував раніше чинну Директиву 95/46/ЄС. Прийняття Загального регламенту про захист даних стало закономірним етапом розвитку права на захист персональних даних у період широкомасштабного впровадження інформаційно-цифрових технологій та глобалізаційних процесів. Загальний регламент про захист даних виводить персональні дані у комплексний і захисний регуляторний режим, що не є повністю відмінним від правового режиму, передбаченого Директивою 95/46/ЄС, а містить модернізовані і проактивні правові норми, здатні забезпечити належний рівень захисту персональних даних у світлі викликів цифрової ери.

Провідну роль у забезпеченні ефективної реалізації положень права ЄС у сфері захисту персональних даних відіграє Суд ЄС, який не тільки здійснює тлумачення норм права ЄС, але й сприяє його однаковому застосуванню на всій території ЄС. Діяльність Суду ЄС у сфері захисту персональних даних реалізується у формі надання попередніх рішень за зверненням національних судів з приводу законності обробки даних, дотримання принципів обробки даних, строків зберігання чи доступу до даних, забезпечення належного рівня безпеки даних, а також вирішення по суті справ щодо невиконання чи порушення права ЄС у цій сфері, а також оцінки контексту, цілей і мети, яка переслідується певним актом.

У переважній більшості справ Суд ЄС розглядав право на захист персональних даних разом з правом на приватне життя, але з часом прослідковується тенденція до набуття самобутності правом на захист персональних даних. Проаналізувавши підходи, застосовані у практиці Суду ЄС, зроблено висновок, що право на захист персональних даних, оцінюється у зв’язку з його безпрецедентною роллю в суспільстві та через оцінку пропорційності втручання у це право у кожній конкретній справі.

Суд ЄС оцінює кожну справу із позиції дотримання зобов’язань та принципів захисту персональних даних, визначених у Загальному регламенті про захист даних, а у

справах, розглянутих раніше – визначених у Директиві 95/46/ЄС, у поєднанні із застосуванням низки концептуальних підходів та принципів, які сприяють всебічному аналізу конкретної справи та забезпечують єдність у тлумаченні права ЄС у сфері захисту персональних даних.

Принципи, концепції, підходи та інтерпретаційні техніки, що застосовуються Судом ЄС є взаємопов'язаними та взаємодоповнюючими. Зокрема, концепція свободи розсуду та принцип верховенства права ЄС у поєднанні з принципами прямої та непрямої дії права ЄС, принципом відповідальності держави сприяють уніфікації правових норм щодо захисту персональних даних на території ЄС та забезпечують єдність у їх правозастосуванні. Важливим в цьому контексті виступає принцип еквівалентного захисту та принцип ефективності. Водночас з розвитком технологій в контексті захисту персональних даних актуальності набуває принцип недискримінації.

Послідовність підходів Суду ЄС сприяє належному рівню захисту права на захист персональних даних у світлі більш складних та прогресивних справ, які, серед іншого, включають питання забезпечення персональних даних у контексті використання штучного інтелекту, масового перехоплення даних чи використання інноваційних технологій.

РОЗДІЛ 4. СТАН ВПРОВАДЖЕННЯ ЄВРОПЕЙСЬКИХ СТАНДАРТІВ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ У ЗАКОНОДАВСТВО УКРАЇНИ

4.1 Законодавчі гарантії захисту персональних даних і практика їх забезпечення в Україні

Засадничі принципи та основні стандарти захисту персональних даних формуються на міжнародно-правовому та національно-правовому рівнях. На сьогодні найбільш прогресивні норми, що регулюють питання захисту персональних даних втілені у європейських стандартах захисту даних. Згадані міжнародно-правові норми набувають деталізації у національних законодавчих актах.

На законодавчому рівні Україна всеохопно підтримує та впроваджує в національну правову систему міжнародні стандарти та практики захисту персональних даних. Україна ратифікувала Конвенцію № 108 та Додатковий протокол до неї 06 липня 2010 року. Втілення міжнародних стандартів захисту даних у національному законодавстві було закріплено у ЗУ «Про захист персональних даних» від 01 червня 2010 року [287], який за своїм змістом схожий із положеннями Конвенції № 108 та Директиви 95/46/ЄС, що належать до другого покоління стандартів захисту персональних даних. Зауважимо, що попри те, що прийняття цього Закону було позитивним кроком у процесі приведення у відповідність вітчизняного законодавства до європейських стандартів у сфері захисту персональних даних, але експерти М. Жорж та Г. Саттон зауважили певні невідповідності, серед іншого, неповну імплементацію принципів, закріплених в ст. 5 Конвенції № 108 у ст. 6 Закону; вужче коло обсягу прав суб'єкта персональних даних у порівнянні з переліком відповідних прав, що містяться в Конвенції № 108 та Директиві 95/46/ЄС; відсутність незалежності наглядового органу при виконанні своїх функцій [288]. Наголосимо, що на момент ухвалення згаданий закон в цілому відповідав основним європейським стандартам захисту, містив основні терміни та визначення, але з розвитком інформаційних технологій, широкомасштабним використанням інтернету і цифровізації багатьох сфер життя виникла необхідність у його суттєвому оновленні. Згаданий закон на законодавчому рівні закріплює визначення «персональних даних», яке кореспондує визначенням закріпленим у Конвенції № 108 та

Директиви 95/46/ЄС, а саме як відомості чи сукупність відомостей про фізичну особу, яка ідентифікована або може бути конкретно ідентифікована. Все ж деякі положення національного закону не відображають сучасний стан регулювання захисту персональних даних у світі, зокрема, у порівнянні з сучасними європейськими стандартами захисту даних у законі закріплене обмежене визначення терміну «персональні дані», не міститься визначення чутливих персональних даних (зокрема, таких як «генетичні дані», «біологічні дані» та «дані стосовно стану здоров'я»), не закріплено терміни «профайлінг», «псевдонімізація», «обмежена обробка», «наглядовий орган», а також не деталізовано права суб'єкта даних [47; 49; 288]. Таким чином, захист персональних даних в Україні, як сфера правового регулювання, наразі перебуває на етапі свого становлення та потребує удосконалення та увідповіднення до новітніх європейських стандартів захисту персональних даних третього покоління - Конвенції № 108+ та Загального регламенту про захист даних.

Варто зауважити, що впродовж останніх десятиліть міжнародне і національне законодавство ввело в обіг низку спеціальних понять у сфері захисту персональних даних, зокрема «персональні дані», «чутливі персональні дані», «обробка даних», «суб'єкт даних», «контролер (володілець) даних», «розпорядник (оператор) даних» тощо. У своїй сукупності ці терміни утворюють відповідний понятійний апарат, який є логічно об'єднаними, взаємообумовленим та взаємодоповнюючим у цій сфері.

Попри узгодження термінологічного інструментарію у сфері захисту персональних даних у міжнародно-правових актах, у вітчизняній науці, як і на практиці, спостерігається взаємозамінне, а інколи й паралельне використання, термінів «персональні дані», «інформація про особу», «персоніфікована інформація», «персональна інформація», «конфіденційна інформація» та «інформація про особисте життя фізичної особи», що характеризується відсутністю чітких критеріїв їх розмежування. Насамперед така невизначеність пов'язана із тим, що у національному законодавстві окремі питання захисту персональних даних врегульовані, серед іншого:

1) ЗУ «Про інформацію» від 02 жовтня 1992 року, який надає визначення «інформації про фізичну особу (персональних даних)» як відомостей чи сукупності відомостей про фізичну особу, яка ідентифікована або може бути конкретно

ідентифікована, тобто фактично повторює визначення надане у ст.1 ЗУ «Про захист персональних даних», при цьому ототожнюючи поняття «персональні дані» та «інформація про фізичну особу» [289];

2) ЗУ «Про доступ до публічної інформації» від 13 січня 2011 року, який у ст. 10 використовує термін «інформація про особу» [290];

3) ЗУ «Про доступ до судових рішень» від 22 грудня 2005 року, який у ст. 7 згадує термін «відомості, що дають можливість ідентифікувати фізичну особу» [291];

4) ЗУ «Про збір та облік єдиного внеску на загальнообов'язкове державне соціальне страхування» від 08 липня 2010 року, який у ст. 20 вживає термін «персоніфіковані відомості» в контексті ведення Реєстру застрахованих осіб [292].

Водночас Конституція України у ст. 32 згадує поняття «конфіденційна інформація про особу», а Цивільний кодекс України оперує поняттям «інформація про особисте життя фізичної особи», згаданим у ст. 302, яка регламентує особливості здійснення права на інформацію. Відтак, наявність різних категорій у національному законодавстві у різних галузях права на практиці доволі часто призводить до взаємозамінного використання низки термінів і категорій у сфері захисту персональних даних.

У цьому аспекті погоджуємося із дослідницею Н. В Камінською, яка стверджує, що у науці міжнародного права та у вітчизняній юридичній науці триває пошук моделі правового механізму регулювання відносин з використання персоніфікованої інформації, захисту персональних даних, яка узгоджувалася б з міжнародно-правовими стандартами, гарантувала б ефективний захист прав людини. Однак відсутність точно визначеного термінологічного інструментарію у сфері захисту персональних даних ускладнює процес практичної реалізації чинних міжнародних та національних нормативно-правових актів [293, с. 107].

Зауважимо, що неточності у застосуванні міжнародних стандартів захисту персональних даних на національному рівні зумовлені дещо застарілими нормами, а також певними законодавчими прогалинами. До прикладу, згідно зі ст. 7 ЗУ «Про поховання та похоронну справу» держава гарантує конфіденційність інформації про померлого, а надання такої інформації здійснюється в порядку, передбаченому ЗУ «Про інформацію», який, однак, не містить окремого порядку. Водночас як наголошує

колектив авторів В. Венгер, А. Кошман, О. Шевчук, існує також проблема застосування відповідних норм національного законодавства у сфері захисту даних, оскільки незважаючи на закріплення принципів обробки даних у законі, вони практично відсутні у національній судовій практиці. Відтак, елементи захисту персональних даних фактично віднайшли своє логічне продовження, розвиток і деталізацію у принципах захисту даних і тлумачаться у світлі останніх [294, с. 7].

Іншим проблемним аспектом є відсутність єдності щодо визначення основних термінів у цій сфері, що призводить й до того, що у національній доктрині формуються різні підходи щодо питання співвідношення термінів «персональні дані», «інформація про особу», «персональна інформація», «персоніфікована інформація», а також «інформації про приватне і сімейне життя», які гарантують право на захист персональних даних та право на приватність.

Так, у вітчизняній правовій доктрині виділяють два основні підходи щодо співвідношення термінів «персональні дані», який визначений у ЗУ «Про захист персональних даних», та «інформація про фізичну особу» чи «інформація про особу», які вживаються у Конституції України, ЗУ «Про інформацію» та ЗУ «Про доступ до публічної інформації». Згідно з першим підходом (Н. В. Камінська, Р. С. Концевой, В. Ф. Погорілко, І. І. Романюк) ці терміни розглядаються як тотожні поняття, що перш за все пояснюється буквальним тлумаченням положень національного законодавства, а саме ЗУ «Про інформацію», де закріплено визначення терміну «інформація про фізичну особу (персональні дані)» і фактично ототожнено ці дві категорії [294, с. 112-113; 295, с. 27]. Зокрема, В. Ф. Погорілко визначає інформацію про особу, як сукупність документованих або прилюдно оголошених відомостей про особу та зазначає, що основною інформацією про особу (персональними даними) є національність, громадянство, сімейний стан, релігійність, стан здоров’я, а також адреса, дата і місце народження [296, с. 718]. Водночас І. І. Романюк стверджує, що термін «інформація про особу» є українським відповідником англійського терміну «personal data», який вживається у міжнародно-правових актах, а власне термін «персональні дані» є більш наближеним до оригіналу способом його перекладу [297, с. 84, 89; 298, с. 38].

Згідно з іншим підходом, «персональні дані» розглядаються як особлива складова більш загального поняття «інформація про особу». Так, О. О. Серебряник зауважує, що поняття «інформація про особу» охоплює не лише персональні дані, а й комунікаційні дані (метадані), інформацію про приватне життя, розкриває расове чи етнічне походження, політичні чи філософські погляди, віросповідання, дані про членство у професійній спілці, місцезнаходження людини, а також дані, що стосуються здоров'я, інтимного життя, творчості, іміджу [299, с. 96-97]. Водночас дослідниця А. Кардаш зауважує, що термін персональні дані може вживатися в контексті позначення інформації про особу, яка не є анонімною. Як стверджує дослідниця відмінності між «інформацією про особу» і «персональними даними» є переважно семантичними, а надання переваги вживанню одного з цих двох термінів викликане історичними причинами, відсутністю усталеної єдиної термінології та різноманітністю юридичної лексики в різних кранах [70, с. 49].

Хоча обидва підходи мають раціональне підґрунтя, загалом вважаємо виправданим визнання «інформації про особу» як найбільш загального терміну, що включає широкий обсяг даних та відомостей, які стосуються фізичної особи. Термін «персональні дані» використовується для позначення окремої категорії даних, для яких характерною ознакою є саме можливість прямої чи опосередкованої ідентифікації особи, а тому, якщо певні дані не дають змогу ідентифікувати особу, вони не відносяться до персональних даних, зокрема, це стосується відкритих даних, анонімної інформації, деперсоналізованих даних або недостовірної інформації.

Водночас науковиця Ю. Д. Бєлова зауважує, що основним критерієм розмежування понять у цій сфері виступає обробка даних. Так, науковиця зазначає, що поняття «персональні дані» варто відмежовувати від суміжних понять, таких як «інформація про особу», «відомості про особисте життя фізичної особи», «ознаки, що індивідуалізують фізичну особу», оскільки згадані поняття можуть мати спільний обсяг і одночасно належить до декількох категорій, але відповідні відомості набувають правового режиму персональних даних саме внаслідок їх обробки [85, с. 40, 87-88].

Варто зауважити, що теорії та практиці існують також дискусії щодо відсутності критеріїв розмежування «персональних даних» та «конфіденційної інформації», тобто

інформації, доступ до якої обмежено фізичною чи юридичною особою. Щодо цього варто згадати положення ч. 2 ст. 5 ЗУ «Про захист персональних даних», якою визначено, що персональні дані можуть бути віднесені до конфіденційної інформації законом або відповідною особою, але не є конфіденційною інформацією персональні дані, що стосуються здійснення особою, уповноваженою на виконання функцій держави або місцевого самоврядування, посадових або службових повноважень. Як зазначає А.В. Кардаш, фактично будь-яку інформацію про особу, яка придатна для ідентифікації, можна апріорі визначити конфіденційною інформацією про особу і водночас фізична особа може додатково обмежити доступ до певної інформації про себе, а відтак зробити цю інформацію конфіденційною [70, с. 34-35]. Вважаємо, що ототожнення «конфіденційної інформації» та «персональних даних» на практиці часто відбувається з огляду на те, що обидві категорії можуть бути поширені тільки за наявності згоди на використання таких даних. Такий підхід невиправдано звужує обсяг «персональних даних», адже знеособлені дані і деякі категорії персональних даних, як от біографічні відомості про публічних осіб, дані, що стосуються посадовців чи інформація про отримувача бюджетних коштів, можуть перебувати у відкритому доступі, а відтак не є конфіденційною інформацією. Водночас персональні дані можуть містити конфіденційну інформацію, яку особа не бажає поширювати, наприклад, відомості про кримінальне засудження чи медичні дані. У цьому аспекті поділяємо думку А. В. Туніка та Х. В. Буртник, які зазначають, що поняття «персональні дані» та «конфіденційна інформація про особу» співвідносяться між собою як загальне та часткове, тобто саме конфіденційна інформація про особу є завжди інформацією з обмеженим доступом і її поширення без згоди цієї особи можливе лише у чітко визначених випадках [300, с. 7; 301].

Одночасно з термінами «персональні дані», «інформація про особу» та «конфіденційна інформація про особу» на законодавчому рівні закріплено термін «інформація про особисте (приватне) життя (фізичної) особи», що створює зайву термінологічну плутанину [70, с. 36; 85, с. 40]. Взаємозамінне використання та ототожнення термінів «конфіденційна інформація», «персональні дані» та «інформація про приватне життя особи» зумовлено позицією Конституційного Суду України (далі –

КСУ) у рішенні № 2-рп/2012 від 20.01.2012 р., де КСУ, надаючи офіційне тлумачення ч. 1, 2 ст. 32 Конституції України, зазначив: «*інформація про особисте та сімейне життя особи (персональні дані про неї)* - ***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 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 тільки за їх згодою, крім випадків, визначених законом, і лише в інтересах національної безпеки, економічного добробуту та прав людини*» [302].

Відтак у згаданому рішенні було надано широкий перелік інформації, що становить персональні дані, але фактично було звужено розуміння терміну «персональні дані» внаслідок його ототожнення з «інформацією про особисте та сімейне життя» та «конфіденційною інформацією про особу». Втім, як зазначено вище, «конфіденційна інформація про особу» та «персональні дані» не є ідентичними. Вважаємо, що термін «персональні дані» є ширшим й за термін «інформація про приватне життя особи» та включає останній, оскільки обробка інформації про приватне життя сама по собі може не вважатися порушенням права на приватне життя, однак обробка цієї інформації може призвести до ідентифікації особи, а відтак потрапляє до сфери захисту персональних даних і може становити втручання у право на захист персональних даних залежно від конкретних обставин справи. Варто зауважити, що такий підхід узгоджується з позицією ЄСПЛ, висловленою у рішенні *Amann v. Switzerland*, де ЄСПЛ розтлумачив, що персональні дані можуть включати інформацію про приватне життя, а термін «приватне життя» в цьому контексті не повинен тлумачитися обмежувально [115].

Водночас у доктрині також існують різні підходи й до співвідношення термінів «персональні дані» та «персоніфікована інформація». За Р. О. Стефанчуком персоніфікована інформація (від лат. *persona* – особа і *...ficatio*, від *facio* – роблю) – це інформація, з якої однозначно можна встановити, що вона стосується конкретної особи або ж включає її до кола осіб, яких ця інформація стосується [303, с. 507]. Водночас колектив науковців у складі В. М. Брижка, А. І. Радянської та М. Я. Швець наголошують, що персоніфікована інформація стала одним із головних об'єктів втручання у право на захист приватності на етапі переходу до інформаційного суспільства. Така інформація отримала назву «персональні дані», тобто дані про людину та її життя, які обробляються за допомогою автоматизованих засобів чи збирають у спеціальних формах, придатних для такої обробки. Однією з причин виокремлення поняття «персональні дані» із загальної маси різноманітної інформації є те, що вони належать до найбільш важливих, делікатних та вразливих атрибутів недоторканості приватного життя людини та потребують захисту за допомогою юридичних та організаційних засобів [69, с. 7]. З наведеного вбачається, що «персоніфікована інформація» та «персональні дані» розглядаються як ідентичні поняття. Тобто відповідно до першого підходу персональні дані та персоніфікована інформація використовуються як взаємозамінні поняття.

Існує також й інший підхід щодо співвідношення цих двох видів інформації. Як наголошує дослідник А. В. Пазюк, терміни «персоніфікована інформація» та «персональні дані» є різними з огляду на свої характерні риси. Так, під персоніфікованою інформацією розуміється різновид інформації, яка відображає як індивідуальність окремої особи крізь призму фізичної, фізіологічної, психічної, економічної, культурної чи соціальної тотожності, так і загальнолюдські біологічні й соціальні властивості людини. У такому разі, визначальною ознакою є її індивідуалізований характер, а саме здатність персоніфікованої інформації ідентифікувати конкретну людину, використовуючи ті чи інші відомості, а тому саме інформація, яка дозволяє безпосередньо ідентифікувати людину, і належить до персоніфікованої інформації. На думку науковця, задля позначення відомостей про особу, які були піддані обробці, зафіксовані на конкретному носії, систематизовані та придатні для автоматизованої обробки виправданим є вживання терміну «персональні

дані» [41, с. 13-14]. Варто зауважити, що обробка даних не обмежується використанням виключно автоматизованих засобів, а включає будь-які операції з персональними даними, зокрема і шляхом не автоматизованої обробки, а тому вважаємо, що критерії обробки даних і їх придатності для автоматизованої обробки не може бути виключною підставою для розмежування персональних даних та інших суміжних категорій і має розглядатися у взаємозв'язку з іншими критеріями, зокрема, можливістю ідентифікації особи.

Варто зазначити, що у науці також використовується термін «персональна інформація», тобто інформації, яка має індивідуалізований характер, тобто може ідентифікувати особу за допомогою певних критеріїв, та включає інформацію про індивідуальність окремої особи, відображає її загальнолюдські, біологічні й соціальні властивості. За Т. І. Обуховською процес персоніфікації відомостей, тобто їх віднесення до конкретної особи, відбувається під час ідентифікації, а тому інформація, яка ідентифікує, дозволяє безпосередньо чи за допомогою інших чинників встановити особу, є персональною інформацією [304, с. 19]. Науковець О. П. Радкевич стверджує, що персональна інформація не обмежена певними межами, матеріальними чи часовими і може містити ім'я, адресу, телефонний номер, професію та рід діяльності, інформацію про те, що купувала особа в магазинах, номер і назву школи, в якій навчалася тощо. Щоправда, при розміщенні інформації персонального характеру у мережу Інтернет вона видозмінюється, але тільки у понятійному аспекті, й перетворюється на персональні дані [305, с. 40, 42]. Вважаємо, що нині використання терміну «персональна інформація» не є виправданим, оскільки цей термін повністю збігається із сучасним визначенням «персональних даних» згідно з яким особа може бути ідентифікована за одним чи декількома факторами, що є визначальними для фізичної, фізіологічної, генетичної, розумової, економічної, культурної чи соціальної сутності такої фізичної особи, як визначено у Загальному регламенті про захист даних [47].

Вищезгадані різноманітні підходи щодо впровадження, а також паралельного застосування у вітчизняній доктрині та практиці термінів «персональні дані», «особиста інформація», «приватна інформація про особу», «персональна інформація», «конфіденційна особиста інформація», а також «особиста інформація», «інформація

персонального характеру», «приватна інформація про особу» як стверджує А. В. Тунік зазвичай є наслідком авторського перекладу міжнародно-правових актів у сфері захисту персональних даних, оскільки етимологічний аналіз цих термінів свідчить про їх змістовну ідентичність терміну «персональні дані» [300, с. 7]. Водночас висловлюється позиція, що використання різноманітних термінів часто зумовлене також національними традиціями правових систем [70, с. 49].

У цьому аспекті науковець В. М. Брижко зазначає, що: «*Визнання та обов'язковість у виконанні приписів європейських правових стандартів щодо основоположних прав захисту фізичних осіб у зв'язку з обробкою персональних даних, передбачає підвищення точності ключових юридичних дефініцій та однозначності у тлумаченні понять шляхом застосування семантичної оцінки ознак предмета захисту та безпеки приватності персональних даних*». Існує необхідність не лише оновлення юридичних норм для увідповіднення новим міжнародно-правовим документам, але й концептуального оновлення відповідного законодавства [306, с. 64]. Відтак, перегляд національного законодавства України потребує оновлення ключових дефініцій, а також загальних принципів та підходів у цій сфері, оскільки вони є взаємопов'язаними та лише комплексна трансформація цих стандартів може підвищити рівень захисту персональних даних з огляду на зміни у суспільстві, технологічний прогрес і виникнення нових міжнародно-правових норм.

Підсумовуючи, зазначимо, що з урахуванням європейських стандартів захисту персональних даних, з метою забезпечення уніфікації термінологічного апарату у цій сфері вважаємо, що цілком виправданим є використання саме терміну «персональні дані» для позначення інформації, що підлягає обробці та містить відомості про ідентифіковану особу чи особу, яку можна ідентифікувати. Водночас вирішальне значення для процесу ідентифікації мають не окремі дані про особу, а саме їх сукупність.

У контексті використання відповідного термінологічного інструментарію, варто звернути увагу і на те, що на відміну від основних міжнародно-правових документів РЄ та ЄС, в українському законодавстві, а також на практиці, замість термінів «контролер» та «оператор» персональних даних використовують терміни «володілець» та «розпорядник» персональних даних, які закріплені в національному законодавстві. Самі

визначення цих термінів, наведені у ст. 2 ЗУ «Про захист персональних даних», є дещо застарілими. Так, володільцем персональних даних визначено фізичну або юридичну особу, яка визначає мету обробки персональних даних, встановлює склад цих даних та процедури їх обробки, якщо інше не визначено законом [287]. Таке тлумачення є дещо звуженим, адже фактично не передбачає випадки коли цілі та засоби обробки даних можуть визначатися двома чи більше володільцями (співволодільцями). Крім того, встановлення того, хто є «володільцем» частіше не визначено самим володільцем, а передбачено законом чи наведено в положеннях підзаконних нормативно-правових актах, положеннях, установчих чи інших документах, наприклад, Порядку ведення інформаційної системи «Моніторинг соціально значущих хвороб», затвердженому Наказом Міністерства охорони здоров'я України від 25.07.2022 № 1317 чи Порядку обробки персональних даних у базі персональних даних - Державному реєстрі фізичних осіб-платників податків, затвердженому Наказом Міністерства фінансів України від 24.02.2015 № 210. Водночас в національному законі фактично ототожнено одержувача даних і третіх осіб, хоча з урахуванням європейських стандартів у цій сфері поняття одержувача даних є ширшим і включає фізичну чи юридичну особу, якій розкриті дані, незалежно від того чи є вона третьою стороною. Понад те, науковці М. В. Бем та І. М. Городиський зауважують, що закон не містить визначення поняття «захист персональних даних», що призводить до суперечливого тлумачення ст. 2 цього закону, у якій йдеться про те, що обробка даних включає використання як одну з дій, але не включає захист даних, та ст. 10 цього закону, згідно з якою використання передбачає будь-які дії щодо захисту даних. Втім, згідно зі стандартами РЄ та ЄС захист персональних даних не є елементом обробки, адже не передбачає вчинення дій з персональними даними [307, с. 22-23]. З урахуванням наведеного вважаємо, що з метою забезпечення узгодженості термінологічного апарату у цій сфері виправданим є оновлення відповідних положень вітчизняного законодавства та вживання термінів контролер та оператор даних, треті особи, наведених у Конвенції № 108+ та Загальному регламенті про захист даних, які найбільш повно характеризують сутність прав та обов'язків кожного з цих суб'єктів.

Також варто зауважити, що хоч питання надання згоди на обробку персональних даних врегульовано у національному законі, але ця вимога не є деталізованою та не відповідає сучасним європейським стандартам захисту персональних даних, адже фактично оминає вимоги щодо надання вільної, конкретизованої та однозначної згоди і не деталізує їх, обмежуючись загальним посиланням на добровільність надання згоди та поінформованість особи. Водночас національне законодавство не врегульовує питання надання згоди стосовно обробки персональних даних дітей. Примітно, що Велика Палата Верховного Суду у зразковій справі № 806/3265/17, яка стосувалася відмови територіального відділу Державної міграційної служби у видачі паспорта громадянина України у формі паперової книжечки, також звернула увагу, що законодавство не врегульовує питання щодо наслідків відмови особи від обробки її персональних даних, тобто фактично відсутня будь-яка альтернатива такого вибору, що обумовлює низьку якість закону та порушення конституційних прав такої особи. Водночас Велика Палата Верховного Суду наголосила, що реалізація функцій держави повинна здійснюватися без примушування людини на надання згоди на обробку персональних даних [308].

Таким чином, національне законодавство у сфері захисту персональних даних, яке складається з низки нормативно-правових актів, включаючи ЗУ «Про захист персональних даних», ЗУ «Про інформацію» та ЗУ «Про доступ до публічної інформації», є не повною мірою взаємоузгодженим. Як у доктрині, так і у практиці відсутня єдність у використанні відповідного термінологічного апарату, а також стосовно співвідношення персональних даних та інших суміжних категорій, як от конфіденційна інформація про особу чи інформація про особу. Хоч в цілому законодавство України про захист персональних даних відповідає сучасним стандартам захисту у цій сфері, але певні аспекти захисту персональних даних в Україні все ще потребують вдосконалення та їх увідповіднення до найбільш прогресивних європейських стандартів захисту персональних даних, закріплених у Загальному регламенті про захист даних та Конвенції № 108+.

4.2 Виконання Україною міжнародно-правових зобов’язань у сфері захисту персональних даних

Прогресивний розвиток міжнародно-правового регулювання забезпечення права на приватне життя та права на захист персональних даних в України інтенсивно розгортався на регіональному рівні, в рамках діяльності РЄ стосовно розробки і прийняття договірних інструментів забезпечення захисту основоположних прав людини. У вітчизняній науці і практиці правові та організаційні питання захисту персональних даних набули своєї актуальності у другій половині 90-их років XX ст., після набуття Україною членства у РЄ. Як повноправний член РЄ у 2010 році Україна ратифікувала Конвенцію № 108 та Додатковий протокол до неї, чим виразила згоду на обов'язковість основних положень, що стосувалися захисту осіб у зв'язку з обробкою персональних даних. В результаті імплементації Конвенції № 108 у 2010 році в Україні було прийнято ЗУ «Про захист персональних даних». Втім, швидкі темпи інформатизації суспільства та постійне вдосконалення інформаційно-комунікаційних технологій розкрили перед людьми нові перспективи в галузі обробки, зберігання, накопичення та використання персональних даних, що дає поштовх до вдосконалення чинних актів у цій сфері як на міжнародно-правовому рівні, так і на національному. Крім того, погоджуємося із науковцем І. М. Городиським, що ухвалення ЗУ «Про захист персональних даних» стало вагомим кроком в частині виконання Україною міжнародно-правових зобов'язань у сфері захисту персональних даних, втім прийняття цього закону є лише окремим аспектом цього шляху, адже інколи прийняті на національному рівні норми не відповідають міжнародним стандартам у цій сфері [309, с. 105].

Варто наголосити, що Додатковий протокол до Конвенції № 108 2001 року передбачає створення незалежного наглядового органу, тобто інституційного механізму публічного контролю у сфері захисту персональних даних, який, як зазначають М. В. Бем та І. М. Городиський, є важливим механізмом реалізації відповідних стандартів і дієвості гарантій, встановлених законодавством у сфері захисту персональних даних [307, с. 113]. Так само вимога створення незалежного наглядового органу встановлена у ст. 51 та 52 Загального регламенту про захист даних [47].

Згідно зі ст. 22 ЗУ «Про захист персональних даних», контроль за дотриманням законодавства про захист персональних даних здійснюють Уповноважений ВРУ з прав людини (далі – Уповноважений) та суди [287]. Зауважимо, що до 2014 року органом

державної влади, відповідальним за захист персональних даних, була Державна служба України з питань захисту персональних даних, яка була ліквідована у зв'язку з обмеженим ступенем незалежності, адже її діяльність спрямовувалася і координувалася Кабінетом Міністрів України через Міністра юстиції України. Як наслідок, повноваження у сфері контролю за дотриманням законодавства у цій сфері перейшли до Уповноваженого. Однак, нині у доктрині та практиці існують дискусії стосовно того чи є Уповноважений належним наглядовим органом у сфері захисту персональних даних у розумінні вимог, встановлених Додатковим протоколом до Конвенції № 108.

Як зауважують науковці В. Г. Пилипчук та В. М. Брижко, покладення на Уповноваженого повноважень щодо нагляду і контролю за законодавством у сфері захисту персональних даних, а також фактичне здійснення функцій органу виконавчої влади, зокрема право здійснювати перевірки, затверджувати нормативно-правові акти у сфері захисту персональних даних, не відповідає ст. 6 Конституції України в частині поділу влади на законодавчу, виконавчу та судову і розподіл відповідних функцій між органами державної влади. Водночас з урахуванням європейських стандартів В. Г. Пилипчук та В. М. Брижко пропонують впровадження нової моделі захисту персональних даних, яка включатиме, серед іншого, створення інституту Уповноваженого з питань захисту персональних даних, підзвітного ВРУ, основними функціями якого можуть бути забезпечення нагляду і контролю та удосконалення нормативно-правової бази з питань захисту персональних даних, а також взаємодія з уповноваженими органами ЄС та держав-членів ЄС з питань захисту даних, а виконавчі функції з питань захисту персональних даних пропонується передати окремому підрозділу у складі Міністерства юстиції України або відновленій Державній службі (агенції) з питань захисту персональних даних [310, с. 40, 46]. В цілому погоджуємося із зазначеною вище пропозицією, адже інститут Уповноваженого є універсальним інструментом моніторингу і сприяння усуненню порушень прав людини, а врахування специфіки захисту персональних даних вимагає створення незалежного органу, наділеного ширшими повноваженнями не лише виявляти порушення законодавства у цій сфері, але й повноваженням розслідувати скарги і накладати санкцій за виявлені порушення.

Іншим проблемним аспектом постає питання доцільності покладення контрольної функції у сфері захисту персональних даних на Уповноваженого. З метою реалізації згаданих функцій в офісі Уповноваженого запроваджено посаду Представника Уповноваженого з питань захисту персональних даних, а в структурі Секретаріату Уповноваженого утворено самостійний структурний підрозділ – Департамент з питань захисту персональних даних. Зауважується, що дієвість такого механізму контролю на практиці виявляється не достатньо ефективною, адже офіс Уповноваженого, окрім повноважень у сфері захисту персональних даних, має низку інших повноважень, зокрема здійснює функцію контролю за дотриманням вимог ЗУ «Про доступ до публічної інформації» та ЗУ «Про звернення громадян» [301, с. 5]. Таким чином, питання ефективності механізму контролю у сфері захисту персональних даних, який відповідно до національного закону здійснює Уповноважений, вочевидь співвідноситься і залежить від інституційної спроможності та ресурсів офісу Уповноваженого.

Крім того, на увагу заслуговують питання реалізації повноважень щодо притягнення до відповідальності за порушення у сфері захисту персональних даних. У цьому аспекті зауважимо, що Загальний регламент про захист даних передбачає наявність двох органів інституційного контролю у сфері захисту персональних даних – Уповноваженого із захисту персональних даних, який фактично відповідає за моніторинг застосування відповідного законодавства, а також Інспектора з захисту персональних даних, який, серед іншого, уповноважений на розгляд скарг та накладення санкцій за порушення законодавства у сфері захисту даних. Фактично, основна форма діяльності щодо контролю реалізується вітчизняним Уповноваженим, його Представником та відповідним департаментом у складі Секретаріату, у вигляді проведення перевірок, за результатами яких встановлюється наявність або відсутність порушень законодавства у сфері захисту даних. Втім, у разі встановлення за результатами проведених перевірок порушення законодавства у сфері захисту персональних даних Уповноважений, його Представник та відповідний департамент, не мають права накладати стягнення, а може лише складати протоколи про адміністративні правопорушення, які згодом передаються для розгляду до суду. Крім того,

Уповноважений може складати приписи щодо усунення виявлених порушень, але такі приписи мають рекомендаційний характер, а для притягнення до відповідальності за їх невиконання має бути складений протокол про вчинення адміністративного правопорушення, який передається на розгляд до суду. Примітно, що вітчизняне законодавство за порушення у сфері захисту персональних даних та невиконання законних вимог Уповноваженого, ст.188-39 та ст. 188-40 Кодексу України про адміністративні правопорушення відповідно, передбачає вкрай низькі штрафні санкції – від ста до двох тисяч неоподатковуваних мінімумів доходів громадян, тобто від 1700 до максимум 34 000 гривень. До прикладу, за незначні порушення Загального регламенту про захист даних відповідальність може сягати максимум 10 000 000 євро або 2% від річного обігу компанії за попередній фінансовий рік, а за значні порушення - до 20 000 000 євро або до 4% від річного обігу, залежно від того, яка сума буде більшою. Відповідно, ефективність, оперативність та дієвість вітчизняного інституційного механізму контролю у сфері захисту персональних даних виявляється доволі низькою і обмеженою, що підтверджується, серед іншого, офіційною статистикою, опублікованою Уповноваженим за 2022 рік. Так, у 2022 році Уповноваженим було отримано 844 звернення щодо порушення законодавства у сфері захисту персональних даних, але було відкрито лише 66 проваджень, за якими вжито заходи реагування з метою поновлення прав суб'єктів персональних даних [312]. З огляду на зазначене, вважаємо, що необхідним є посилення спроможності інституту Уповноваженого щодо ефективного вирішення питань порушень у сфері захисту персональних даних шляхом позасудових засобів або шляхом наділення такою функцією окремого органу у цій сфері.

На увагу заслуговують й пропозиції щодо структури й повноважень контролюючого органу, висловлені дослідниками В. Венгером та О. Заярним, які пропонують наступні три моделі інституціоналізації державного контролю у сфері персональних даних та публічної інформації, а саме: 1) створення окремого державного органу, що не входить і не підпорядкований жодній з гілок влади, як от Національна комісія з інформаційних технологій та свобод у Франції чи Офіс захисту персональних даних у Польщі, 2) створення окремого органу владу в системі органів виконавчої влади, як от Державна інспекція захисту персональних даних, яка відповідальна перед Урядом

та Міністром юстиції у Литві, 3) створення системи органів здійснення інституційного контролю [313, с. 14-26]. Зауважимо, що незалежно від обраної моделі важливо забезпечити достатню незалежність та самостійність відповідного органу контролю за додержанням законодавства про захист даних, врегулювавши у вітчизняному законодавстві питання утворення та діяльності такого органу, гарантії незалежності, включаючи умови фінансування, забезпечення об'єктивності, неупередженості та безсторонності, шляхом чіткого визначення компетенції, повноважень та правил взаємодії з іншими державними органами і органами держав-членів РЄ та ЄС.

Ідея створення окремого незалежного органу була втілена у проєкті ЗУ«Про Національну комісію з питань захисту персональних даних та доступу до публічної інформації» № 6177 від 18.10.2021 (далі – законопроєкт № 6177) [314]. Вказаний законопроєкт безумовно є правильним кроком, навіть попри те, що висловлюються сумніви щодо доцільності поєднання в одному органі повноважень з формування та реалізації державної політики та контрольної функції, поєднання функцій із захисту персональних даних та контролю у сфері доступу до публічної інформації, наділення повноваженнями щодо погодження проєктів нормативно-правових актів [315]. Втім, на сьогодні цей законопроєкт все ще перебуває на розгляді, відповідно, питання ефективності інституційного механізму контролю у сфері захисту персональних даних залишається актуальним.

Окремо варто зауважити на тому, що національне законодавство у сфері захисту персональних даних послідовно розвивається у відповідь на обставини сучасних реалій. Так, з огляду на виклики, які постали в Україні після повномасштабного вторгнення у 2022 році було прийнято ЗУ «Про державну реєстрацію геномної інформації людини». Під геномною інформацією людини у згаданому законі розуміються відомості про генетичні ознаки людини, тобто фактично це генетичні дані (зразки ДНК). Відтак поняття геномної інформації визначене в законі доволі широко, адже включає фактично будь-які відомості про генетичні ознаки людини. У розумінні законодавства про захист персональних даних геномна інформація належить до чутливих персональних даних, тобто відомостей, які підлягають особливому порядку обробки та відповідним гарантіям захисту. Варто звернути увагу, що ст. 6 Конвенції № 108 закріплює вимогу, що

персональні дані не можуть піддаватися автоматизованій обробці, якщо внутрішнє законодавство не забезпечує відповідних гарантій. Тому, перш за все, ухвалення цього закону є важливим для виконання вимог міжнародних зобов'язань [316].

Головним чином геномна інформація використовується в кримінальному провадженні для розкриття злочинів, розшуку безвісти зниклих, ідентифікації загиблих, а також ідентифікації осіб, які не здатні через стан здоров'я, вік або інші обставини повідомити інформацію про себе. Враховуючи масові порушення прав людини з якими Україна стикнулася з початком повномасштабного вторгнення, прийняття згаданого закону може позитивно відзначитися на ефективному розслідування воєнних злочинів та пошуку зниклих безвісти. Примітно, що законом також передбачено можливість обміну геномною інформацією з іншими країнами та міжнародними організаціями під час кримінального провадження, що може принести позитивні результати в контексті розслідування воєнних злочинів, вчинених на території України [317].

Варто зауважити, що деякі положення цього закону носять певні ризики стосовно забезпечення прав суб'єкта даних. Так, попри те, що геномна інформація є чутливими персональними даними, право на її використання належить широкому колу суб'єктів. Водночас законом передбачені доволі тривалі строки зберігання геномної інформації (впродовж 50 років), що несе істотні ризики, зокрема у разі потенційної загрози витоку такої інформації. З урахуванням законодавства у сфері захисту персональних даних саме володілець (контролер) даних повинен вживати всіх організаційних та технічних заходів для забезпечення безпеки даних, що обробляються. Втім, у прийнятому законі відсутні чіткі гарантії та запобіжники щодо попередження ризику втрати геномної інформації чи її витоку, а також не закріплений обов'язок володільця (контролера) повідомити особу про такі порушення безпеки персональних даних. Фактично питання запобігання ризику розкриття інформації для інших цілей чи її розголошення, у тому числі шляхом несанкціонованого доступу, в законі чітко врегульовано лише щодо обміну геномною інформацією з іншими країнами чи міжнародними організаціями під час кримінального провадження. Крім того, не конкретизовані й питання можливості вилучення геномної інформації у зв'язку зі смертю особи, яка її надала, що необхідно для того, щоб мінімізувати ризики доступу до чутливих персональних даних родичів такої особи. Так

само відсутні положення щодо права на видалення і відкликання згоди на обробку геномної інформації особою, яка їх надала, адже у ст. 8 цього закону визначено перелік категорій осіб, які під час дії воєнного стану обов'язково надають біологічні матеріали для державної реєстрації, зокрема, до таких осіб відносять військовослужбовців, поліцейських, осіб рядового та начальницького складу служби цивільного захисту, а також членів добровольчих формувань територіальних громад. До того ж за порушення законодавства у сфері державної реєстрації геномної інформації, яка належить до чутливих даних, фактично передбачена загальна адміністративна та кримінальна відповідальність за порушення законодавства у сфері персональних даних. Інший аспект ризиків, пов'язаних з обробкою таких даних, виявляється у тому, що у законі не прописаний чітко механізм контролю за дотриманням законності при обробці геномної інформації, хоча і міститься загальне положення, що контроль за додержанням прав людини здійснює Уповноважений [305]. Відтак, попри те, що прийняття вказаного закону є позитивним кроком в контексті виконання Україною своїх міжнародних зобов'язань у відповідь на ризики, що виникають у зв'язку з введенням воєнного стану, в аспекті обробки геномної інформації вкотре постає основна проблема захисту персональних даних в Україні, а саме відсутність незалежного регуляторного органу у сфері захисту даних, наділеного повноваженнями здійснювати системні перевірки, надавати консультації та накладати санкції за порушення законодавства у сфері захисту персональних даних [316].

Зауважимо, що стан виконання Україною своїх міжнародних зобов'язань є безперервним процесом, який варто оцінювати в контексті змін вітчизняного законодавства та його оновлення з огляду на сучасні реалії, зокрема процеси європейської та євроатлантичної інтеграції, які були закріплені у 2019 році в Основному Законі та розвинули процес оновлення вітчизняного законодавства. В контексті євроатлантичної інтеграції та зміцнення інформаційної безпеки, поділяємо думку, що сучасна діяльність Організації Північноатлантичного договору (НАТО) стосується не лише питань безпеки й оборони, а й відстоювання принципів демократії, верховенства права та захисту прав людини, що водночас є предметом діяльності низки інших міжнародних організацій, членом яких є Україна. Примітно, що деякі положення Річних

національних програм НАТО також передбачають вжиття заходів з імплементації міжнародно-правових актів чи з виконання рекомендацій, розроблених не тільки під егідою НАТО, а й в рамках діяльності інших міжнародних організацій [318, с. 294]. Серед іншого, Річна національна програма під егідою Комісії Україна - НАТО на 2021 рік передбачала як одне з пріоритетних завдань забезпечення імплементації положення Загального регламенту про захист даних у національне законодавство [319]. К. О Савчук та І. М. Проценко зауважують, що виконання Річних національних програм під егідою Комісії Україна – НАТО допомагають не лише наблизити законодавство України до стандартів НАТО, але і сприяють розвитку держави, побудованої на засадах демократії та верховенства права [320, с. 258].

Водночас особливо гостро питання гарантування інформаційної безпеки постало в умовах воєнного стану, зокрема, беручи до уваги стрімкий розвиток інформаційно-цифрових технологій, використання технологій штучного інтелекту, масового перехоплення даних та інших інноваційних технологій, які створюють низку викликів у інформаційній сфері. О. С. Переверзєва підкреслює, що використання інформаційно-комунікаційних технологій, включаючи засоби інтерактивної комунікації, також сприяє розвитку інформаційного суспільства, проголошеного як одна з цілей ЄС [321, с. 521]. У цьому аспекті А. В. Войцеховський стверджує, що основним завданням європейських та інших країн в сучасних умовах є вжиття заходів, що дозволять принципово зменшити, а подекуди – унеможливити повністю, негативні наслідки від кіберзагроз, джерелом яких можуть виступати іноземні військові та розвідувальні служби, організовані злочинні угруповання, терористичні та екстремістські групи. Значну роль у процесі вироблення єдиних підходів щодо забезпечення кібербезпеки як складової національної безпеки країн відіграє НАТО [322, с. 42].

З огляду на зазначене, одним з пріоритетних напрямків розвитку вітчизняного законодавства є підвищення рівня захисту персональних даних в контексті забезпечення інформаційної безпеки. Окремим аспектом розбудови ефективного механізму захисту даних є впровадження Стратегії інформаційної безпеки, яка була введена в дію рішенням Ради національної безпеки і оборони України від 15 жовтня 2021 року, згідно з якою захист персональних даних визнається пріоритетом державної діяльності в галузі

гарантування інформаційної безпеки. Вважаємо, що вказані цілі можуть бути досягнуті шляхом імплементації європейських стандартів захисту персональних даних, які втілені в оновленій Конвенції № 108+ та Загальному регламенті про захист даних [323, с. 24].

Окремо варто зауважити, що зважаючи на вагому роль технологій штучного інтелекту у різноманітних галузях повсякденного життя, включаючи медицину, освіту, правоохоронну систему, оборону тощо, набуває актуальності встановлення відповідного правового регулювання у цій сфері. Зауважимо, що сфера правового регулювання використання штучного інтелекту перебуває на етапі свого становлення на міжнародному та загальноєвропейському рівнях. Пріоритетним аспектом європейського підходу є встановлення етичних стандартів впровадження штучного інтелекту, орієнтованого на людину, що наразі формується у діяльності РЄ, яка займається розробкою рамкової конвенції з питань штучного інтелекту, та ЄС, який розробляє Регламент ЄС про штучний інтелект. У вітчизняній правовій системі, попри відсутність чіткого правового регулювання у цій сфері, також вживаються заходи щодо розробки правових норм та розвитку використання технологій штучного інтелекту. Зокрема, Розпорядженням Кабінету Міністрів України від 02 грудня 2020 р. № 1556-р було схвалено Концепцію розвитку штучного інтелекту в Україні [324]. Крім того, Україна є членом Комітету РЄ з питань штучного інтелекту, а також у жовтні 2019 року приєдналася до Рекомендацій ОЕСР з питань штучного інтелекту OECD/LEGAL/0449. Таким чином, можна стверджувати, що Україна активно бере участь у впровадженні на національному рівні найкращих міжнародних практик і напрацювань щодо використання передових технологій і розглядає такі сфери як пріоритетні аспекти розвитку загальнодержавної політики.

Водночас одним з основоположних чинників забезпечення і гарантування основоположних прав людини, серед іншого, й права на захист персональних даних, а також приведення національного законодавства, зокрема й у галузі прав людини, та практики його застосування у відповідність до європейських стандартів є виконання рішень ЄСПЛ. Примітно, що у преамбулі ЄКПЛ також наголошено, що її метою є забезпечення і розвиток основоположних прав людини, а також забезпечення колективного гарантування прав європейськими державами [26]. Зауважимо, що цей

нормативний ідеал втілено у ст. 17 ЗУ «Про виконання рішень та застосування практики Європейського суду з прав людини», відповідно до якої національні суди при розгляді справ застосовують ЄКПЛ та практику ЄСПЛ як джерело права [325]. Обов'язковість виконання рішень ЄСПЛ безпосередньо державами-учасницями передбачено статтею 46 ЄКПЛ, але стосується ця вимога виключно рішень, в якій держава-учасник є стороною. Як зазначив ЄСПЛ у справі *Scozzari and Giunta v. Italy* під обов'язком Високих Договірних Сторін виконувати остаточні рішення ЄСПЛ у будь-якій справі, в якій вони є сторонами, розуміється, що рішення, відповідно до якого ЄСПЛ визнав порушення, покладає на державу-відповідача обов'язок не лише здійснити на користь заявника виплати, присуджені як справедлива сатисфакція, але також і здійснити під контролем КМРЄ загальні і, якщо це доречно, індивідуальні заходи, здійснення яких є необхідним у рамках внутрішньої правової системи, аби покласти край виявленому порушенню та виправити негативні наслідки такого порушення (§249) [326].

Як зауважують професори В. І. Муравйов та Н. Б. Мушак виконання рішень ЄСПЛ мають важливе значення для України, що зумовлено, серед іншого, обов'язком виконання міжнародно-правових зобов'язань та здатністю дотримуватись своїх зобов'язань у відносинах з міжнародними партнерами та РЄ [327, с. 21]. Водночас професор Н. М. Оніщенко, розглядаючи феномен контролю за забезпеченням прав людини, підкреслює, що у демократичних правових системах контроль *«охоплює функціональну здатність забезпечення прав, свобод і законних інтересів особистості, а отже: легітимність влади, що дієво захищає честь, гідність і права людини»* [328, с. 25]. Відповідно, окрім обов'язку виконувати рішення ЄСПЛ у всіх справах, стороною яких є Україна, національні органи також зобов'язані враховувати і застосувати всі висновки та критерії, викладені в судовій практиці ЄСПЛ, що сприятиме утвердженню та забезпеченню основоположних прав людини.

Попри те, що кількість рішень ЄСПЛ щодо України, які зачіпають питання захисту персональних даних, є нечисленною, все ж ухвалені рішення призвели до якісних змін у вітчизняній практиці та ефективного забезпечення прав людини. Варто наголосити на прецедентному значенні рішення у справі *Garnaga v. Ukraine*, що стосувалася необґрунтованої відмови органів влади та судів у задоволенні клопотання

заявниці про зміну її по батькові з рідного імені батька на ім'я вітчима, оскільки вона більш тісно пов'язувала себе із вітчимом і неповнорідним братом. Хоч відзначив, що національне законодавство, яке регулювало зміну імені та прізвища, було доволі гнучким і заявниця змогла змінити своє прізвище на прізвище вітчима, але воно не містило достатніх підстав для обмеження права на зміну по батькові. Відтак, відмовивши у праві заявниці змінити по батькові, національні органи не виконали своїх зобов'язань, що призвело до порушення ст. 8 ЄКПЛ (§36) [116]. На виконання цього рішення 03 листопада 2020 р. ВРУ прийняла зміни до Цивільного та Сімейного кодексів України, які закріплюють право вибирати та змінювати по батькові і забезпечують справедливий баланс між конкуруючими інтересами особи та суспільства в цілому. Відтак, вжиті у цій справі заходи на виконання рішення ЄСПЛ не тільки повністю усунули наслідки порушень ЄКПЛ для заявника, але й запобігатимуть новим подібним порушенням. Поділяємо думку О. Мазур і Л. Грицаєнко, що виконання рішення ЄСПЛ не передбачає *stricto sensu* певних законодавчих змін, але виявляючи недолік у правовій системі ЄСПЛ може вказати на цю проблему, що сприятиме подальшому оновленню вітчизняного законодавства відповідно до європейських стандартів захисту прав людини [329, с. 37].

Низка рішень ЄСПЛ проти України стосувалися проблеми захисту персональних даних про стан здоров'я та медичної інформації. Зокрема, у справі *Panteleyenko v. Ukraine* ЄСПЛ встановив порушення ст. 8 ЄКПЛ через розголошення конфіденційної медичної інформації стосовно психічного здоров'я і психіатричного лікування заявника у рамках розгляду справи про наклеп та відсутність внутрішнього засобу правового захисту для оскарження та отримання компенсації за розкриття такої інформації [153]. Примітно, що справі *Panteleyenko v. Ukraine* порушення сталося не внаслідок відсутності певних законодавчих норм, а через неправильне застосування судом національного законодавства стосовно збирання, зберігання, використання та поширення інформації про стан психічного здоров'я особи, яке, до того ж не було вирішальним для судового процесу. Подібною є також справа *Zaichenko v. Ukraine № 2*, яка стосується питання законності дій органів внутрішніх справ щодо збирання відомостей про стан здоров'я заявника, що не було необхідними для розгляду на національному рівні справи про

адміністративні правопорушення. У цій справі ЄСПЛ також констатував порушення прав заявника через відсутність спеціальних положень національного законодавства, що регламентували б порядок проведення примусового обстеження (і, зокрема, збору інформації про психічний стан здоров'я) в рамках розгляду справи про скоєння адміністративного правопорушення. На виконання цього рішення було розроблено законопроєкт про внесення змін до деяких законодавчих актів України щодо проведення судово-психіатричної експертизи в адміністративному провадженні внесено урядом до ВРУ (№ 7472 від 29.12.2017). Щоправда, згодом цей законопроєкт було відкликано. Оскільки справа все ще перебуває на контролі КМРЄ, Міністерством юстиції України опрацьовується питання щодо доопрацювання зазначеного законопроєкту для подальшого внесення його на розгляд ВРУ [330].

Варто також взяти до уваги нещодавнє рішення *M. K. v. Ukraine*, у якому було встановлено порушення права заявниці на повагу до її приватного життя через те, що вона не була належним чином поінформована про результат тестування на ВІЛ, яке було проведене під час її регулярного огляду у військовому госпіталі. Як наслідок, інформація про ВІЛ позитивний статус військовослужбовиці була розголошена її матері та за місцем її служби [144]. Хоч ця справа стосувалася законодавства, яке було змінено невдовзі після обставин, що мали місце у справі, але це рішення вкотре наголошує на важливості захисту чутливих даних, а також необхідність отримання чіткої згоди на обробку таких даних. Примітно, що у цій справі ЄСПЛ посилався на свої попередні висновки у справі *Surikov v. Ukraine*, що стосувалася свавільного збору та зберігання роботодавцем відомостей про психічне здоров'я заявника, які мали характер чутливих даних, були застарілими та невідповідними, а також подальше їх використання для розгляду питання про підвищення заявника та розповсюдження колегам заявника в процесі прийняття рішення роботодавцем і в ході публічного слухання. У цьому рішенні ЄСПЛ наголосив, що спосіб, у який законодавство України було розтлумачене і застосоване національними судами, дозволяло зберігати дані про стан психічного здоров'я заявника впродовж тривалого періоду, а також використання цих даних для цілей, не пов'язаних з початковою метою їх збору [154].

Водночас низка справ ЄСПЛ проти України стосується питань проведення негласних слідчих дій, як от прослуховування телефонних розмов. Так, у справах *Berlizev v. Ukraine* and *Lysyuk v. Ukraine* ЄСПЛ встановив порушення ст. 8 ЄКПЛ, оскільки запис телефонних розмов заявників був проведений за відсутності дозволу суду [331; 332]. Окрім того, ЄСПЛ також вирішував справи проти України, які стосувалися захисту персональних даних та свободи вираження поглядів, свободи отримувати та поширювати інформацію. Такою є справа *Sedletska v. Ukraine*, в якій надання судами доступу до інформації щодо вхідних і вихідних з'єднань з мобільного телефону заявниці-журналістки – включаючи дати, час і місцезнаходження її мобільного телефону поблизу вказаних вулиць і місць протягом шістнадцятимісячного періоду – було визнано порушенням статті 10 ЄКПЛ, оскільки цей захід був надмірно непропорційним, не був виправданий «найважливішою вимогою суспільних інтересів» і тому не був необхідним, а також не мав належних процесуальних гарантій, адже судове рішення у справі було ухвалено в ході засідання *ex parte* (без виклику особи) [333]. Водночас ЄСПЛ встановив порушення статті 10 ЄКПЛ у справі *Centre for Democracy and the Rule of Law v. Ukraine* у зв'язку з відмовою Центральної виборчої комісії надати громадській організації-заявнику копії автобіографій лідерів політичних партій, які балотувалися на парламентських виборах, на тій підставі, що вказана інформація була конфіденційною. Примітно, що при відмові у наданні цієї інформації Центральна виборча комісія посилалася, серед іншого, на рішення КСУ від 20 січня 2012 року у справі № 2-рп/2012, в якому наводиться тлумачення терміну «інформація про особисте та сімейне життя особи», яке, як зазначив ЄСПЛ у §107 *«настільки загальне, що дозволяє охопити всю можливу інформацію про особу»* [159; 302].

Зважаючи на те, що рішення ЄСПЛ є обов'язковими та розглядаються як джерело права, відповідно, при розгляді подібних справ висновки ЄСПЛ повинні використовуватися як усталена правова позиція для усіх національних судів. Відтак рішення ЄСПЛ у справах щодо захисту персональних даних та втручання у приватне життя, а також й інші конкуруючі права і свободи людини, сприяють формуванню єдиного підходу до правозастосування та належного впровадження на практиці європейських стандартів захисту персональних даних і відповідних гарантій, які повинні

бути включені в національне законодавство задля запобігання свавільному втручанню в основоположні права людини, включаючи право на захист персональних даних, і забезпечення справедливого балансу між конкуруючими правами людини.

Таким чином, стан виконання Україною своїх зобов'язань у сфері забезпечення та гарантування права на захист персональних даних є безперервним процесом, що постійно розвивається з огляду на впровадження новітніх технологій, глобалізаційні процеси, євроінтеграційний і євроатлантичний вектор розвитку держави та виклики і загрози сучасності, серед іншого, пов'язані й зі збройною агресією проти України. Забезпечення ефективного захисту персональних даних здійснюється шляхом створення належних гарантій для суб'єктів даних і функціонування незалежного органу інституційного контролю, який розглядається як важливий елемент європейських стандартів захисту персональних даних. Відповідно, одним з суттєвих аспектів виконання відповідних міжнародних зобов'язань є оновлення та модернізація вітчизняного законодавства у сфері захисту даних відповідно до сучасних європейських стандартів та його орієнтованість на підходи, висвітлені у практиці ЄСПЛ.

4.3 Захист персональних даних: еволюція законодавства України у процесі його адаптації до *acquis* Європейського Союзу

Розбудова відносин з ЄС як напрям зовнішньої політики України вперше була визначена у Постанові ВРУ від 2 липня 1993 року «Про основні напрями зовнішньої політики України». Згодом євроінтеграційний вектор розвитку України були деталізовані в Угоді про партнерство та співробітництво між Україною і Європейськими Співтовариствами та їх державами-членами від 14 червня 1994 року, яка набула чинності 1 березня 1998 року (далі – УПС), Стратегії інтеграції України до ЄС, схваленій Указом Президента України 11 червня 1998 року, а також Програмі інтеграції України до ЄС, схваленій Указом Президента України 14 вересня 2000 року. Зауважимо, що статтею 51 УПС з ЄС вперше було визначено такий аспект співробітництва як поступова адаптація чинного та майбутнього законодавства України із правом ЄС, шляхом забезпечення «приблизної адекватності законів» у відповідних пріоритетних галузях, перелічених у цій статті, серед іншого, митне право, банківське право, інтелектуальна власність, охорона праці, захист прав споживачів тощо [334]. На основі УПС та Плану дій Україна

– ЄС був започаткований процес адаптації до права ЄС, процедур, стандартів та практики ЄС. Втім, форми, методи та строки адаптації вітчизняного законодавства до права ЄС у вищезазначених не були чітко визначені. Саме для реалізації УПС було затверджено Стратегію інтеграції України до ЄС 1998 року, яка визначила адаптацію законодавства України до права ЄС і забезпечення прав людини як один з основних напрямів інтеграційного процесу [335]. Етапи правової адаптації, які можна визначити радше як заходи з адаптації законодавства, включали імплементацію УПС, укладання галузевих угод, приведення чинного законодавства України у відповідність до права ЄС, створення механізму увідповіднення проєктів актів законодавства України до права ЄС. Як зауважує професор І. В. Яковюк, на початку 2002 р. було прийнято значну кількість нормативних актів у сфері адаптації законодавства України до права ЄС, але на той момент був відсутній спеціальний закон у цій сфері, що значно ускладнювало як правотворчий, так і правозастосовний процес. У зв'язку з цим було прийнято ЗУ «Про Концепцію Загальнодержавної програми адаптації законодавства України до законодавства Європейського Союзу» та ЗУ «Про Загальнодержавну програму адаптації законодавства України до законодавства Європейського Союзу», що містять комплекс взаємопов'язаних завдань з адаптації законодавства України до права ЄС [336, с. 254]. Водночас у 2010 році було прийнято ЗУ «Про засади внутрішньої і зовнішньої політики», який у статті 11 проголосив забезпечення інтеграції України в європейський політичний, економічний, правовий простір з метою набуття членства в ЄС однією з основоположних засад зовнішньої політики України.

Одним з подальших важливих кроків до розвитку на шляху європейської інтеграції України стала Угода про асоціацію з ЄС (далі – УА), підписана у 2014 році. Основні аспекти УА включають співробітництво і зближення в галузі зовнішньої і безпекової політики, а також співробітництво в галузі правосуддя, свободи та безпеки, що впроваджується шляхом наближення українського законодавства до *acquis* ЄС у різних сферах, таких як торгівля, економіка, енергетика, транспорт, стандартизація, соціальні та правові питання, охорона довкілля та інше.

У 2019 році незворотність європейського та євроатлантичного курсу України було закріплено в абзаці п'ятому Преамбули Основного Закону. Відповідно, Україна

задекларувала на вищому політичному рівні курс зближення з ЄС, що передбачає повагу до спільних цінностей, адаптацію законодавства та посилення співробітництва у сфері правосуддя, безпеки, захисту прав людини, а також інших сферах.

Україна 23 червня 2022 року офіційно набула статусу кандидата на членство в ЄС. Передумовою вступу до ЄС є дотримання критеріїв, необхідних для набуття членства, закріплених у Декларації Європейської Ради, ухваленої у Копенгагені 1993 року, так званих Копенгагенських критеріїв, а саме: 1) *політичного критерію*, який передбачає стабільність інституцій, які гарантують демократію, верховенство права, дотримання прав людини, повагу і захист прав меншин; 2) *економічного критерію*, тобто наявність дієвої ринкової економіки та 3) *критерію членства*, який іноді називають юридичним чи інституційним критерієм, тобто здатність брати на себе зобов'язання, пов'язані з членством у ЄС, включаючи дотримання цілей політичного, економічного та валютного союзу. Крім того, у ст. 49 ДЄС у редакції Лісабонського договору 2007 р. передбачені також *географічний критерій*, а саме, що членом ЄС може стати лише «європейська держава», та *ціннісний критерій*, а саме відданість та неухильне дотримання країною-заявницею цінностей, визначених у ст. 2 ДЄС у редакції Лісабонського договору 2007 р. [337, с. 116]. Зауважимо, що третій Копенгагенський критерій членства передбачає обов'язок впровадження європейських стандартів, зокрема й у сфері захисту персональних даних, які, серед іншого, складають сукупність *acquis* ЄС. Як зауважує професор Н. Б. Мушак концепція *acquis* ЄС як основа правопорядку ЄС має комплексний характер, що включає сукупність правових норм, судових рішень, доктринальних понять, рекомендацій, домовленостей тощо, які виникли за час існування європейських інтеграційних об'єднань. Такі норми підлягають беззастережному визнанню державами-членами ЄС, а для третіх країн – виступають важливою умовою посилення економічного та політичного співробітництва з ЄС [338; с. 104]. Відповідно, процес адаптації до права ЄС, насамперед до *acquis* ЄС, й оновлення вітчизняного законодавства, є пріоритетним напрямом в процесі інтеграції України до ЄС. Втім, адаптація законодавства передбачає не лише вдосконалення чинного вітчизняного законодавства, а й розробку проєктів нормативно-правових актів з урахуванням *acquis* ЄС у відповідній сфері. Водночас стверджується, що на доктринальному рівні феномен

acquis ЄС є ширшим, ніж правова концепція «законодавство ЄС», та включає установчі договори ЄС, загальні принципи права ЄС, рішення Суду ЄС тощо.

Аналіз тексту УА в українському перекладі свідчить про те, що в ній використовуються поняття «зближення законодавства» (ст. 56, 403, 405) та «наближення законодавства» (англ. approximation) (ст. 59, 64, 66, 67, 84, 124, 133, 138, 148, 256, 363, 375, 387, 397, 424, 463, 474), які по суті є синонімічними, а також такі терміни як «транспозиція», «(поступове) приведення законодавства у відповідність» (англ. transpose) (ст. 56, 124, 133, 153), «гармонізація законодавства» (англ. harmonization, alingment) (ст. 57, 267, 347, 352, 355, 358, 368, 405), «адаптація законодавства» (англ. adoption) (ст. 53, 58, 114, 150, 152-154) та «встановлення еквівалентних норм» (ст. 66-67) [339]. Використання низки синонімічних та взаємозамінних термінів свідчить про відсутність уніфікованої термінології для позначення процесу адаптації України до права ЄС. У вітчизняній доктрині та практиці відсутній єдиний підхід до використання термінології в контексті адаптації законодавства України до права ЄС, що зумовило одночасне використання й таких понять як «апроксимація законодавства» (від лат. approximatio – зближення), що є синонімічним до поняття «наближення законодавства», а також «імплементація законодавства», що є загальним терміном, який використовується для позначення процесу впровадження у національне законодавство та виконання державою відповідних міжнародно-правових норм, що здійснюється шляхом прийняття нових законів або внесення змін до чинного законодавства, «трансформація законодавства», що позначає процес внесення змін, перегляду і модернізації відповідних правових норм, шляхом прийняття нових законів, зміни чинного законодавства, видалення застарілих норм, гармонізації з міжнародними стандартами, поняття «уніфікація законодавства», що означає процес повного узгодження національного законодавства із правом ЄС тощо. Підсумовуючи, зазначимо, що адаптація законодавства виступає формою і складовою процесу гармонізації законодавства України із правом ЄС, що є поетапним процесом, який досягається за допомогою різних методів.

Щодо процесу адаптації законодавства України до права ЄС, звісно, не втратили актуальності певні недоліки нормативно-правових актів України у цій сфері. Так,

професор І. В. Яковюк, серед іншого, виокремлює: 1) численні суперечливі або застарілі положення; 2) прийняття актів з порушенням правил законодавчої техніки (одним і тим самим термінам надається неоднакове значення, різні поняття вживаються як синоніми); 3) відсутність визначення засадничих категорій (зокрема, нормативно невизначеними залишаються фундаментальні поняття «інтеграція» та «європейська інтеграція») [336, с. 255].

Що стосується питання приведення у відповідність до права ЄС вітчизняного законодавства у сфері захисту персональних даних, то чинний ЗУ «Про захист персональних даних» був ухвалений на основі положень Конвенції № 108 та фактично відтворює положення Директиви 95/46/ЄС. Станом на момент його прийняття, попри деякі недоліки та неточності, вказаний Закон відповідав основним європейським стандартам захисту даних. Відтак, вітчизняне законодавство у сфері захисту персональних даних зорієнтоване на європейські стандарти, закріплені в актах РЄ та ЄС.

Варто зауважити, що у статті 15 УА підкреслено важливість співробітництва між Україною та ЄС з метою забезпечення належного рівня захисту персональних даних відповідно до найвищих європейських та міжнародних стандартів, зокрема відповідних документів РЄ [339]. Крім того, згідно зі ст. 11 ратифікованої в лютому 2017 року Угоди про співробітництво між Україною та Європейською організацією з питань юстиції, кожна сторона забезпечує рівень захисту персональних даних, наданих іншою стороною, який є принаймні еквівалентним тому, що випливає з застосування принципів, що містяться у Конвенції № 108, а також принципів, закладених у Рішенні щодо Євроюсту та в Регламенті Євроюсту щодо захисту даних [340]. Таким чином, «євроорієнтованість» вітчизняного законодавства у сфері захисту персональних даних зумовлена важливістю співробітництва в цій сфері між Україною та ЄС.

Взяття Україною на себе відповідних міжнародних зобов’язань, що випливають як з УА, так і з набуття статусу кандидата на членство в ЄС, вкотре актуалізувало питання щодо необхідності впровадження в Україні нових стандартів захисту персональних даних. Таким чином, з огляду на євроінтеграційний вектор зовнішньої політики України, наразі для адаптації національного законодавства у сфері захисту персональних даних до права ЄС необхідно імплементувати правові стандарти ЄС щодо

захисту персональних даних, закріплені у Загальному регламенті про захист даних, який є основним актом у цій сфері, що значно підвищив рівень захисту персональних даних у державах-членах ЄС і, серед іншого, поширює свої положення екстериторіально на країни поза межами ЄС, а також оновлених Директиві 2016/680 про захист даних правоохоронними органами та Директиві 2016/681 про використання даних записів імен пасажирів, які разом формують так званий Пакет захисту даних. Відповідно, оновлення потребує ЗУ «Про захист персональних даних» та мають бути внесені зміни до інших галузевих законів, у яких норми рамкового закону про захист даних мають бути деталізовані, враховуючи відповідні обмеження щодо мети і функціонального призначення.

Важливим елементом процесу адаптації вітчизняного законодавства до *acquis* ЄС є забезпечення єдності термінологічного інструментарію. У цьому аспекті можна констатувати, що у сфері захисту персональних даних базова термінологія є доволі адаптованою до права ЄС. Враховуючи системний євроінтеграційний підхід, у структурі Кабінету Міністрів України був створений Урядовий офіс координації європейської та євроатлантичної інтеграції, одними з ключових завдань якого є координація процесу адаптації законодавства України до права ЄС, передусім до *acquis* ЄС, імплементація стандартів НАТО, а також забезпечення здійснення перекладу *acquis* ЄС українською мовою, оновлення глосарія термінів *acquis* ЄС.

Варто зауважити, що український переклад Загального регламенту про захист даних є дещо недосконалим. Найбільшим недоліком є те, що у затвердженому перекладі українською мовою замість звичного для національного законодавства терміну «обробка персональних даних», який використовується у вітчизняному законі й в українському перекладі Конвенції № 108 та Директиви 95/46/ЄС, у перекладі Загального регламенту про захист даних з невідомих причин вживається словосполучення «*опрацювання* персональних даних». Крім того, інколи офіційний переклад видається незрозумілим, через використання складних граматичних конструкцій та формулювань, які впливають на сприйняття тексту. До прикладу, що стосується умов визначення добровільності згоди на обробку персональних даних – друге речення пункту 43 Преамбули – використано формулювання «*Презумпція ненадання добровільної згоди*

виникає у разі...» (англ. «Consent is presumed not to be freely given if…»), втім, на наш погляд, виправданим було б використання більш лаконічного формулювання «*Згода не є добровільною, якщо…*». Іншим прикладом може слугувати стаття 9, що регулює порядок обробки чутливих даних, в якій використано формулювання *«для цілі єдиної ідентифікації фізичної особи»* (англ. «for the purpose of uniquely identifying a natural person») [47]. Вочевидь кращим варіантом перекладу було б використання формулювання *«з метою однозначної ідентифікації фізичної особи»*. Таким чином, переклад відповідних термінів, що використовуються в актах ЄС у сфері захисту персональних даних, має бути удосконалений, задля уникнення правової невизначеності та забезпечення ефективного впровадження у внутрішнє право України відповідних норм права ЄС.

Зауважимо, що після набуття 23 червня 2022 року Україною офіційного статусу кандидата в члени ЄС, українським урядом було запущено вебсайт «Пульс угоди» для моніторингу реалізації Україною заходів з виконання Угоди про асоціацію. Попри те, що ВРУ прийнято низку змін до чинного законодавства, що регулює захист персональних даних, включаючи зміни до ЗУ «Про захист персональних даних», зокрема щодо порядку обробки та захисту персональних даних у період дії воєнного стану з огляду на необхідність захисту національних інтересів, а також урегульовано питання порядку обробки геномної інформації та протидії кіберзагрозам, втім стан виконання УА в контексті удосконалення законодавства у сфері захисту персональних даних становить всього 20 % [341].

Наразі на розгляді національного парламенту перебуває проєкт закону від 25.10.2022 № 8153 щодо внесення змін до ЗУ «Про захист персональних даних» (далі – проєкт закону № 8153). Насамперед варто наголосити, що в проєкті закону № 8153 вперше запропоновано на законодавчому рівні закріпити право людини на захист персональних даних, що відповідає основним міжнародним тенденціям у сфері захисту основоположних прав. Проєктом закону № 8153 пропонується також оновлення понятійно-категоріального апарату, зокрема, це стосується заміни категорій «володілець» та «розпорядник» на «оператор» та «контролер», відповідно. Конкретизуються принципи обробки даних, вимоги щодо отримання згоди при обробці

даних у мережі Інтернет, під час відеоспостереження чи відеофіксації публічних заходів, а також обробки даних для цілей прямого маркетингу. Окрім того, передбачається посилення прав суб'єкта даних, шляхом їх закріплення, включаючи й «право на забуття» та право на захист від автоматизованого прийняття рішень, а також встановлення механізму захисту прав у випадку їх порушення контролером та/або оператором. Пропонується конкретизувати права і обов'язки контролерів та операторів, як при обробці даних в Україні, так і при передачі іншим державам чи міжнародним організаціям, а також впроваджується процедура повідомлення контролером про витік персональних даних. Водночас передбачається посилення захисту персональних даних через впровадження вимог Загального регламенту про захист даних щодо призначення в установах і органах посадової особи, відповідальної за захист персональних даних. Важливим оновленням є детальна регламентація особливостей обробки даних у певних сферах, зокрема, при їх обробці роботодавцем, у правоохоронній діяльності та у сфері електронних комунікацій. Новелою виступає закріплення виду та розмірів санкцій за порушення законодавства у сфері захисту даних [342]. Примітно, що в проєкті закону № 8153 здійснюється спроба врегулювати притаманну вітчизняному законодавству розпорошеність норм, категорій та термінів у сфері захисту даних, що використовуються в різних нормативно-правових актах, шляхом прямого зазначення посилання на відповідні терміни та законодавчі акти, в яких наводиться їх визначення.

Зауважимо, що за результатами проведеної правової експертизи проєкту закону № 8153 Комітет ВРУ з питань інтеграції України до ЄС визнав, що останній не суперечить цілям УА та праву ЄС, але потребує доопрацювання, зокрема, з метою врахування положень Загального регламенту про захист даних щодо визначень термінів «персональні дані», «обробка даних» та «картотека персональних даних», які наразі визначені неповною мірою, доповнення положень законопроєкту визначеннями «представник», «зобов'язальні корпоративні правила», а також уточнення певних положень статей 39 та 40 законопроєкту з метою їх увідповіднення до положень статей 35 та 36 Загального регламенту про захист даних [343]. Так само у правовому висновку РЄ щодо проєкту закону № 8153, підсумовується, що документ містить розширену версію положень, що встановлюють всеосяжну правову базу для захисту даних, а також

наголошується, що передбачений законопроєктом загальний підхід досить близький до європейських стандартів, що містяться у Конвенції №108+ та Загальному регламенті про захист даних тощо. Водночас деякі положення рекомендується переглянути, уточнити або внести до них правки, щоб гарантувати їх відповідність зазначеним європейським стандартам [344, с. 70]. Станом на сьогодні законопроєкт все ще не прийнятий, втім нереформованість національного законодавства у сфері захисту персональних даних призводить до панування формального підходу щодо його дотримання відповідними суб'єктами та знижує ефективність гарантування та захисту персональних даних.

Окремо варто звернути увагу на прийнятий в ЄС проєкт Акту про штучний інтелект. Зважаючи на те, що ймовірніше з розвитком і широким впровадженням технологій штучний інтелект потребують регулювання питання забезпечення приватності та захисту персональних даних при застосуванні технологій штучного інтелекту. У цьому аспекті погоджуємося із науковцем В. М. Брижком, який стверджує, що існує потреба у створенні рамкового етичного кодексу у «поведінки» штучного інтелекту з умовами захисту та безпеки приватності персональних даних, адже, серед іншого, у Загальному регламенті про захист даних та проєкті ePrivacy Regulation проблема «штучний інтелект – захист та безпека персональних даних» не розглядається або поки не має чіткого предметного вирішення [306, с. 61]. Примітно, що спроби створення правового регулювання у сфері штучного інтелекту в Україні були започатковані схваленням 2 грудня 2020 року Концепції розвитку штучного інтелекту в Україні, в якій вперше було закріплено визначення, мета, принципи та завдання розвитку технологій штучного інтелекту в Україні [324]. Зважаючи на євроінтеграційні процеси передбачається, що вітчизняне законодавство буде розвинуте і гармонізоване з правом ЄС у цій сфері.

У контексті виконання зобов'язань у сфері адаптації законодавства України та практики Л. Г. Фалалєєва зауважує, що вагоме значення для України має адаптація вітчизняного законодавства і практики до рішень Суду ЄС, адже цей обов'язок національних судових органів безпосередньо випливає з положень Угоди про асоціацію [90, с. 255]. Відповідно, національні суди повинні враховувати усталені правові позиції, викладені у рішеннях Суду ЄС як у процесі тлумачення джерел первинного та

вторинного права ЄС, так і їх застосування з метою захисту основоположних прав, включаючи право на захист персональних даних.

Примітно, що у статті 1 УА визначено як одну з цілей асоціації посилення співробітництва у сфері правосуддя, свободи та безпеки з метою забезпечення верховенства права та поваги до основоположних прав людини, до яких у правопорядку ЄС належить й право на захист персональних даних. Як зауважує професор Т. В. Комарова, хоч Суд ЄС ще жодного разу не тлумачив положення УА, все ж певні положення свідчать про можливість прямої дії її окремих норм, серед іншого, ст. 471 УА, яка регулює порядок доступу фізичних та юридичних осіб до судів та адміністративних органів, може бути використана Судом ЄС для оцінки можливості використання прямої дії положень УА [241, с. 431-432].

Зауважимо, що національні суди періодично посилалися на основоположні принципи права ЄС та деякі елементи *acquis* ЄС, а також рішення Суду ЄС ще до підписання УА. У більшості випадків посилання стосувалися принципів захисту конституційних прав і свобод. До прикладу, КСУ у рішенні від 12 червня 2007 № 2-рп/2007 посилався на положення Регламенту ЄС № 2004/2003 Про статус і фінансування політичних партій на європейському рівні [345]. Як стверджує професор Р. А. Петров, українська судова система (включаючи КСУ) має доволі тривалий досвід застосування *acquis* ЄС як джерела права, серед іншого, визнаючи пріоритет УПС над суперечливими положеннями національного законодавства, а також використовуючи концепцію правової визначеності та розвиваючи принцип законних очікувань, що розвинуті у практиці Суду ЄС [346, с. 55, 61]. Що стосується захисту персональних даних, як підкреслюють В. Венгер, А. Кошман та О. Шевчук, національні суди посилаються переважно на Хартію ЄС для додаткової аргументації, хоч видається більш доцільним посилання на Загальний регламент про захист даних [294, с. 11]. Таким чином, сформульовані у рішеннях Суду ЄС правові позиції варто розглядати як ефективний інструмент для удосконалення вітчизняного законодавства у контексті його адаптації до права ЄС. У цьому контексті варто наголосити й на необхідності вироблення в Україні єдиної судової практики з питань захисту персональних даних відповідно до

європейських стандартів у цій сфері та гармонійного тлумачення вітчизняного законодавства відповідно до усталених стандартів ЄС та практики Суду ЄС.

Таким чином, розвиток національного законодавства про захист персональних даних особливо актуально постав у зв'язку з євроінтеграційними пріоритетами зовнішньої політики України. Процес адаптації вітчизняного законодавства, включаючи сферу захисту персональних даних, є тривалим процесом, який поступово розвивається та який можна умовно розділити на два періоди – перший період, пов'язаний з виконанням УПС та ухваленням Директиви 95/46/ЄС, а другий – з виконанням УА та оновленням законодавства з метою імплементації положень Загального регламенту про захист даних. Водночас УА є частиною національного законодавства, а тому її положення, включаючи зобов'язання за ст. 15 щодо забезпечення належного рівня захисту персональних даних відповідно до європейських стандартів, зокрема відповідних документів РЄ, мають обов'язковий характер. Відтак для забезпечення ефективного захисту персональних даних варто привести законодавство України у відповідність до Загального регламенту про захист даних та інших актів інтеграційного об'єднання у цій сфері, а національні суди мають враховувати законодавчі акти ЄС у сфері захисту персональних даних та практику Суду ЄС з цих питань для забезпечення єдності у правозастосуванні.

Висновки до Розділу 4

Дослідження законодавчих гарантій захисту персональних даних і практики їх забезпечення в Україні, а також оцінка стану впровадження європейських стандартів захисту персональних даних у право України дозволяє зробити такі висновки.

На законодавчому рівні Україна всеохопно підтримує та впроваджує в національну правову систему міжнародні стандарти та практики захисту персональних даних. Захист персональних даних в Україні, як сфера правового регулювання, перебуває на етапі становлення та потребує удосконалення, увідповіднення до новітніх європейських стандартів захисту персональних даних третього покоління – Конвенції № 108+ та Загального регламенту про захист даних.

Законодавству України у сфері захисту персональних даних притаманні наступні ознаки: складна структурованість та розгалуженість відповідних правових норм у різних актах; некоректність або відсутність чіткого визначення конкретного змісту термінів та категорій, які не є повною мірою взаємоузгодженими; неоднозначне інтерпретування законодавчих норм під час правозастосування; застарілість норм вітчизняного законодавства у сфері захисту персональних даних та їх невідповідність європейським стандартам у цій сфері.

З урахуванням європейських стандартів захисту персональних даних, з метою забезпечення термінологічної єдності виправданим є використання саме терміну «персональні дані» для позначення інформації, що містить відомості про ідентифіковану особу чи особу, яку можна ідентифікувати, та підлягає обробці. Водночас вирішальне значення для процесу ідентифікації мають не окремі дані про особу, а саме їх сукупність.

Інституційний механізм публічного контролю у сфері захисту даних, який є важливим механізмом контролю за дотриманням європейських стандартів захисту персональних даних потребує оновлення та увідповіднення вимогам незалежності, об'єктивності, неупередженості та безсторонності.

Стан виконання Україною своїх міжнародно-правових зобов'язань у сфері забезпечення і дотримання права на захист персональних даних є триваючим процесом, що постійно розвивається з огляду на впровадження новітніх технологій, глобалізаційні процеси, євроінтеграційний і євроатлантичний зовнішньополітичні пріоритети розвитку держави, виклики та загрози сучасності, серед іншого, пов'язані зі збройною агресією проти України. Однак недосконаліть національного законодавства у сфері захисту персональних даних сприяє формальному підходу до його дотримання відповідними суб'єктами, знижує ефективність гарантування та захисту персональних даних.

Процес адаптації вітчизняного законодавства до *acquis* ЄС, включаючи сферу захисту персональних даних, є тривалим процесом, який поступово розвивається. Його умовно можна розподілити на два періоди – перший, пов'язаний з виконанням Угоди про партнерство і співробітництво, прийняттям Директиви 95/46/ЄС, положення якої були частково імплементовані у ЗУ «Про захист персональних даних», а другий – з виконанням Угоди про асоціацію між Україною та ЄС та оновленням законодавства з

метою імплементації у законодавство України положень Загального регламенту про захист даних. Угода про асоціацію між Україною та ЄС створила стійку інституційну та правову базу для застосування *acquis* ЄС, включаючи практику Суду ЄС, а також для комплексної адаптації законодавства України до права ЄС. Одним з суттєвих аспектів виконання Україною відповідних міжнародно-правових зобов'язань є оновлення та модернізація законодавства у сфері захисту даних відповідно до сучасних європейських стандартів захисту персональних даних та його орієнтованість на підходи, властиві практиці ЄСПЛ та Суду ЄС.

ВИСНОВКИ

У процесі проведеного дослідження було зроблено такі висновки.

Інформація про людину, насамперед її ім’я, інші відомості про приватне життя завжди розглядалися як важливий елемент для індивідуалізації та інтеграції людини у суспільство. Приватність вперше була закріплена в англо-саксонській правовій системі, де вона окреслюється терміном «прайвесі» (англ. privacy – приватна справа, таємниця, усамітненість) й забезпечує недоторканність приватного життя. Історичний розвиток концепції приватності свідчить про наявність двох основних моделей захисту даних – європейської та американської. Відмінність між концепцією приватності в американській та європейській площині зумовлена підходами до її розуміння – американська концепція приватності полягає у свободі людини, в яку держава не може втручатися (негативна свобода), водночас європейська концепція спрямована на захист честі та гідності людини (позитивна свобода). Ці відмінності є умовними і повинні розглядатися крізь призму історичного розвитку – європейські країни на конституційному рівні визнають права громадян на захист від свавільного втручання уряду в право на повагу до приватного і сімейного життя, недоторканність житла та таємницю кореспонденції, водночас у США право на приватність виникло з судових прецедентів.

Формування підходів до захисту права та приватне життя і права на захист персональних даних перебуває у взаємозв’язку із національним, культурним, історичним та ідеологічним сприйняттям приватності та такого її аспекту як інформаційна приватність. Як наслідок, сформувалися декілька режимів захисту приватності та персональних даних, характерні для європейського регіону (європейська модель захисту даних), зокрема, США та країн Латинської Америки (американська модель захисту даних).

Тривалий час питання захисту персональних даних розглядалося як один з аспектів права на захист приватного життя, а положення щодо захисту приватного життя були сформульовані настільки узагальнено, що не деталізували окремі аспекти визначення права на захист персональних даних і, у такий спосіб, звужували його

зміст. Такий стан став поштовхом до правотворчості держав на національному рівні і, починаючи з 60-70-х років XX ст., в Австрії, Данії, Франції, Німеччині, Люксембурзі, Норвегії, Швеції, а також Канаді та США були ухвалені закони про захист персональних даних і захист приватності.

У міжнародному праві захист приватності пов'язують з визнанням і закріпленням права на захист приватного життя як одного з основоположних прав людини в міжнародно-правових договорах - у статті 12 Загальної декларації прав людини 1948 р., статті 17 МПГПП 1966 р., статті 8 Конвенції про захист прав людини і основоположних свобод 1950 р.

Для усунення розбіжностей, які існували у законодавчих актах окремих держав, та з метою гармонізації підходів до захисту персональних даних, на міжнародному рівні були прийняті спроби систематизації стандартів захисту даних. Однак у міжнародному праві прослідковується значна фрагментація норм щодо захисту персональних даних, що зумовлено відсутністю універсального міжнародного договору у цій сфері, відмінностями у сприйнятті приватності та персональних даних і, відповідно, існуванням конкуруючих правових режимів захисту даних. За відсутності універсального міжнародного договору стандарти захисту персональних даних в основному сформувалися в рамках РЄ та ЄС. У зв'язку з цим у доктрині та практиці широко використовується категорія «європейські стандарти захисту персональних даних», що позначає найбільш узагальнені, керівні положення, принципи, основоположні правові засади у цій сфері. В умовах глобалізаційного розвитку європейські стандарти захисту персональних даних поступово набули значного поширення і сприяли гармонізації норм щодо захисту персональних даних на міжнародному рівні. З огляду на еволюційний розвиток європейських стандартів захисту персональних даних виправданою є їх класифікація на: перше покоління (Керівні принципи ОЕСР 1980 р., Конвенція № 108 у її первинній редакції 1981 р.), друге покоління (Конвенція № 108, оновлена Додатковим протоколом 2001 р., Директива 95/46/ЄС) та третє покоління (оновлена Конвенція № 108+ зі змінами, внесеними Протоколом CETS № 223, Загальний регламент про захист даних 2016 р.).

Ґенеза права на захист персональних даних свідчить, що воно безумовно пов’язане із визнанням та закріпленням права на повагу до приватного життя як основоположного права людини і тривалий час право на захист персональних даних розглядалося лише як один з його аспектів та не було чітко визначене, що створювало прогалину в правовому регулюванні. Поступовому виокремленню та закріпленню як самостійного права людини на захист персональних даних сприяла широкомасштабна комп’ютеризація і цифровізація багатьох сфер суспільного життя, впровадження новітніх технологічних розробок і необхідність у транскордонній передачі великих обсягів даних.

ЄСПЛ та Суд ЄС досліджують норми національного законодавства на предмет їх відповідності європейським стандартам захисту персональних даних та міжнародно-правовим зобов’язанням держави у сфері захисту основоположних прав людини. Вони інтерпретують обсяг персональних даних та принципи їх захисту під час обробки за конкретних обставин кожної справи, що сприяє узагальненню та систематизації європейських стандартів захисту персональних даних, а також дозволяє оцінити їх у світлі динамічних суспільних змін та адаптувати до сучасних реалій.

Право на захист персональних даних значною мірою формувалося внаслідок застосування ЄСПЛ теорії еволюційного тлумачення статті 8 ЄКПЛ, яка гарантує право на захист приватного життя. Втім, незважаючи на високий ступінь взаємозв’язку між цими правами, вони не є тотожними.

З аналізу судової практики зроблено висновок, що у справах щодо захисту персональних даних, окрім традиційного трискладового тесту за статтею 8 ЄКПЛ, ЄСПЛ використовує: 1) *доктрину еволюційного тлумачення*, який сприяє становленню та розвитку права на захист персональних даних в рамках конвенційної системи та дає змогу ЄСПЛ розглядати дедалі складніші та технологічно-новітні справи щодо захисту персональних даних, 2) *доктрину доступності та передбачуваності*, що дозволяє оцінити передбачуваність, доступність, точність та ясність законодавства у сфері захисту даних, 3) *доктрину позитивних та негативних зобов’язань*, що використовується задля оцінки виконання зобов’язань держави у

контексті гарантування права на захист персональних даних, а також 4) *доктрину свободи розсуду,* що використовується для оцінки свободи дій держави щодо виконання своїх зобов'язань за ЄКПЛ у контексті захисту персональних даних. Вагому роль у забезпеченні права на захист персональних даних відіграють 1) *принцип правової визначеності*, який сприяє формуванню єдності та послідовного розвитку законодавства та практики захисту персональних даних, 2) *принцип неілюзорності прав та забезпечення їх практичності й ефективності*, який сприяє наповненню змістом права на захист персональних даних та його практичній реалізації, 3) *принцип пропорційності та забезпечення рівноваги інтересів*, що використовується задля урівноваження конкуруючих прав, гарантованих ЄКПЛ, 4) *принципи автономного та порівняльного тлумачення*, які можуть застосовуватися для тлумачення основних термінів у сфері захисту персональних даних.

Необхідно гарантувати права на захист персональних даних як самостійне право в рамках конвенційної системи шляхом прийняття окремого протоколу до ЄКПЛ, що забезпечило б належний захист таких аспектів права на захист персональних даних як право на забуття, право на заперечення проти обробки чи право на мобільність даних. Така необхідність зумовлена тим, що Конвенція № 108 не передбачає створення самостійного контрольного механізму для захисту гарантованого нею права на захист персональних даних. Водночас в рамках конвенційної системи це право розглядається крізь призму статті 8 ЄКПЛ, що не повною мірою забезпечує достатній рівень захисту суб'єкта даних та його основних прав, оскільки ці питання можуть залишатися поза увагою ЄСПЛ при розгляді справ за статтею 8 ЄКПЛ.

У правопорядку ЄС право на захист персональних даних є одним з основоположних прав людини, яке гарантується ефективним поєднанням різних правових інструментів ЄС, зокрема його установчих договорів, Хартії ЄС, а також актів вторинного права ЄС.

Правове регулювання ЄС у сфері захисту персональних даних вирізняється наявністю значного масиву законодавчих актів, які детально регламентують питання обробки персональних даних та містять стандарти захисту персональних даних,

спрямовані на забезпечення захисту прав людини при обробці її даних. Основним актом ЄС у цій сфері виступає Загальний регламент про захист даних, який скасував раніше чинну Директиву 95/46/ЄС та який розглядається як *lex generalis*.

Провідну роль у забезпеченні ефективної реалізації положень права ЄС у сфері захисту персональних даних відіграє Суд ЄС, який не тільки здійснює тлумачення норм права ЄС у цій сфері, але й сприяє його однаковому застосуванню на всій території ЄС. Суд ЄС оцінює право на захист персональних даних у зв'язку з його безпрецедентною роллю в суспільстві та оцінює втручання в його реалізацію у кожній конкретній справі з огляду на 1) *доктрину свободи розсуду*, яка переважно застосовувалася у контексті тлумачення положень Директиви 95/46/ЄС та оцінки свободи дій держав щодо імплементації її норм у національне законодавство, 2) *принцип верховенства права ЄС* над національним правом його держав-членів. Практичне значення у поєднанні з *принципом верховенства права ЄС* традиційно, мають й такі принципи, розроблені Судом ЄС, як *принцип прямої дії*, що дозволяє особам безпосередньо посилатися на основі норми права ЄС і вимагати їх реалізації через національні суди, *принцип непрямої дії*, згідно з яким національні суди зобов'язані тлумачити національне законодавство відповідно до права ЄС, включаючи всі його джерела права, у тому числі й акти «м'якого права», *принцип відповідальності держави*, що є наслідком достатньо серйозного порушення прав, гарантованих правом ЄС. У контексті захисту персональних даних із зазначеними вище принципами тісно пов'язані й *принцип еквівалентного захисту*, який передбачає забезпечення адекватного рівня захисту права на захист персональних даних у всіх державах-членах ЄС, а також використовується в контексті оцінки можливості передачі даних у країни поза межами ЄС чи міжнародним організаціям; *принцип пропорційності*, який виступає головною передумовою обмеження права на захист персональних даних; *принцип ефективності*, який передбачає, що право ЄС не повинно робити неможливим чи надмірно ускладненим здійснення права на захист персональних даних; *принцип недискримінації*, що використовуватися в контексті обробки чутливих даних та може бути використаний для оцінки ризику алгоритмічної дискримінації.

Принципи, концепції, підходи та інтерпретаційні техніки, що застосовуються Судом ЄС та ЄСПЛ є взаємопов'язаними та взаємодоповнюючими. Послідовність підходів ЄСПЛ та Суду ЄС сприяє належному рівню захисту персональних даних й у випадках використання штучного інтелекту, масового перехоплення даних чи використання інноваційних технологій.

Інтерпретаційні інструменти та методи, що використовуються ЄСПЛ та Судом ЄС є подібними, спрямовуються на досягнення однієї мети – гарантування основоположних прав людини, включаючи право на повагу до приватного життя та право на захист персональних даних. На відміну від Суду ЄС, ЄСПЛ не має юрисдикції скасовувати національні закони чи адміністративну практику, які порушують ЄКПЛ, але може висловити поради щодо їх скасування чи внесення змін. Суд ЄС, навпаки, посилається на принцип верховенства ЄС, принцип прямої дії та принцип відповідальності держави, таким чином зобов'язуючи державу змінити чи анулювати національне законодавство, яке визнано таким, що порушує право ЄС. Водночас ЄСПЛ визнає, що у визначених випадках держави можуть користуватися свободою розсуду щодо регулювання захисту персональних даних, у той час як у рамках ЄС з прийняттям Загального регламенту про захист даних Суд ЄС практично не посилається на свободу розсуду держав, адже зазначений регламент підлягає прямому застосуванню державами-членами ЄС.

Аналіз законодавчих гарантій захисту персональних даних і практики їх забезпечення в Україні дає змогу зробити висновок, що на законодавчому рівні Україна всеохопно підтримує та впроваджує в національну правову систему європейські стандарти та практики захисту персональних даних. Однак нині захист персональних даних в Україні, як сфера правового регулювання, перебуває на етапі становлення та потребує увідповіднення новітнім європейським стандартам захисту персональних даних третього покоління – Конвенції № 108+ та Загальному регламенту про захист даних 2016 р.

Законодавству України у сфері захисту персональних даних притаманні наступні ознаки: складна структурованість та розгалуженість відповідних правових норм у різних актах; некоректність або відсутність чіткого визначення конкретного

змісту термінів та категорій, які не є повною мірою взаємоузгодженими; неоднозначне інтерпретування законодавчих норм під час правозастосування; застарілість норм вітчизняного законодавства у сфері захисту персональних даних та їх невідповідність європейським стандартам у цій сфері.

Неточність формулювання понять «персональні дані», «інформація про особу» та «конфіденційна інформація», «інформація про приватне життя особи» у вітчизняному законодавстві призводить до існування на практиці конкуруючих норм та нерідко до звуження захисту персональних даних, внаслідок його ототожнення із конфіденційною інформацією чи інформацією про приватне життя. З метою забезпечення уніфікації термінологічного апарату у цій сфері виправданим є використання саме терміну «персональні дані» для позначення інформації, що підлягає обробці та містить відомості про ідентифіковану особу чи особу, яку можна ідентифікувати.

Інституційний механізм публічного контролю у сфері захисту даних, який є важливим механізмом контролю за дотриманням європейських стандартів захисту персональних даних потребує оновлення.

Стан виконання Україною своїх міжнародно-правових зобов'язань у сфері забезпечення дотримання права на захист персональних даних є безперервним процесом, що постійно розвивається з огляду на впровадження новітніх технологій, глобалізаційні процеси, євроінтеграційний і євроатлантичний зовнішньополітичні пріоритети держави, виклики та загрози сучасності, серед іншого, пов'язані зі збройною агресією проти України. Угода про асоціацію між Україною та ЄС створила стійку інституційну та правову базу для застосування *acquis* ЄС, включаючи практику Суду ЄС, а також для комплексного підходу до адаптації законодавства України до права ЄС. Одним з суттєвих аспектів виконання Україною відповідних міжнародно-правових зобов'язань є оновлення та модернізація законодавства у сфері захисту персональних даних відповідно до сучасних європейських стандартів та його орієнтованість на підходи, властиві практиці ЄСПЛ та Суду ЄС.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Заблоцький В. Приватність. *Філософський енциклопедичний словник* / ред. кол. В. І. Шинкарук та ін. Інститут філософії імені Григорія Сковороди НАН України. Київ: Абрис, 2002. С. 517.

2. Ємчук Л. В. Конституційно-правове регулювання особистого та сімейного життя людини і громадянина: дис. … канд. юрид. наук: 12.00.02 / ДВНЗ «Ужгород. нац. ун-т». Ужгород, 2015. 225 с.

3. Стефанчук Р. О. Прайвесі. *Юридична енциклопедія* / ред. кол. Ю. С. Шемшученко та ін. Ін-т держави і права ім. В. М. Корецького НАН України. Київ: Українська енциклопедія ім. М. П. Бажана, 2003. Т. 5: П - С. С. 53.

4. Warren S. D., Brandeis L. D. The Right to Privacy. *Harvard Law Review*. 1890. Vol. 4. No. 5. P. 193-220. URL: https://doi.org/10.2307/1321160 (дата звернення: 03.10.2023).

5. Decision of Supreme Court of the United States of 04.06.1928 in Olmstead v. U.S. URL: https://www.loc.gov/item/usrep277438/ (дата звернення: 03.10.2023).

6. Серьогін В. О. Прайвесі як право «бути залишеним у спокої». *Право і Безпека*. 2010. № 3. С. 6-9. URL: http://nbuv.gov.ua/UJRN/Pib_2010_3_3 (дата звернення: 03.10.2023).

7. Prosser W. L. Privacy. *California Law Review*. Vol. 48 No. 3. P. 383–423. URL: https://doi.org/10.2307/3478805 (дата звернення: 03.10.2023).

8. DeCew J. Privacy. *The Stanford Encyclopedia of Philosophy* / ed. by Edward N. Zalta. 2018. URL: https://plato.stanford.edu/archives/spr2018/entries/privacy/ (дата звернення: 03.10.2023).

9. Banisar D., Davies S. Global Trends in Privacy Protection: An International Survey of Privacy, Data Protection, and Surveillance Laws and Developments. *UIC John Marshall Journal of Information Technology & Privacy Law*. 1999. Vol. 18 No. 1. P. 1-112. URL: https://repository.law.uic.edu/jitpl/vol18/iss1/1/ (дата звернення: 03.10.2023).

10. Савчин М. В. Конституційне право України: підручник. Київ: Правова єдність, 2009. 1008 с.

11. Горпинюк О. П. Інформаційна приватність та її захист від злочинних посягань в Україні : монографія. Львів: ПП «Видавництво «БОНА», 2014. 324 с.

12. Strömholm S. Right of privacy and rights of the personality: a comparative survey. Stockholm, P. A. Norstedt & Soners Fürlag, 1967. 246 p. URL: https://www.icj.org/wp-content/uploads/1967/06/right-to-privacy-working-paper-publication-1967-eng.pdf (дата звернення: 03.10.2023).

13. Whitman J. Q. The Two Western Cultures of Privacy: Dignity versus Liberty. *Yale Law Journal*. 2004. Vol. 113. P. 1151-1221. URL: https://digitalcommons.law.yale.edu/cgi/viewcontent.cgi?article=1647&context=fss_papers (дата звернення: 03.10.2023).

14. Universal Declaration of Human Rights of 10.12.1948. URL: https://www.un.org/en/about-us/universal-declaration-of-human-rights (дата звернення: 03.10.2023).

15. International Covenant on Civil and Political Rights of 16.12.1966. URL: https://treaties.un.org/doc/treaties/1976/03/19760323%2006-17%20am/ch_iv_04.pdf (дата звернення: 03.10.2023).

16. UN Human Rights Committee. CCPR General Comment No. 16: Article 17 (Right to Privacy), The Right to Respect of Privacy, Family, Home and Correspondence, and Protection of Honour and Reputation of 08.04.1988. URL: https://www.refworld.org/docid/453883f922.html (дата звернення: 03.10.2023).

17. Decision of Human Rights Committee in Sayadi and Vinck v. Belgium of 22.10.2008, Comm. 1472/2006, CCPR/C/94/D/1472/2006. URL: https://juris.ohchr.org/Search/Details/1477 (дата звернення: 03.10.2023).

18. Decision of Human Rights Committee in Andrea Vandom v. Republic of Korea of 12.07.2018, Comm. 2273/2013, CCPR/C/123/D/2273/2013. URL: https://juris.ohchr.org/Search/Details/2496 (дата звернення: 03.10.2023).

19. OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data of 23.09.1980. URL: https://www.oecd.org/internet/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm (дата звернення: 03.10.2023).

20. Коваленко Ю. О. Еволюція європейських стандартів захисту персональних даних. *Актуальні проблеми законодавства України: пріоритетні напрями його*

вдосконалення: матеріали міжн. наук.-практ. конф. (м. Одеса, 9-10 жовт. 2020 р.). Одеса, 2020. С. 13-16.

21. UN Guidelines concerning computerized personal data files, as adopted by General Assembly resolution 45/95 of 14.12.1990. https://www.refworld.org/docid/3ddcafaac.html (дата звернення: 03.10.2023).

22. UN General Assembly Resolution A/RES/68/167 The right to privacy in the digital age adopted on 18.12.2013. URL: http://undocs.org/A/RES/68/167 (дата звернення: 03.10.2023).

23. UN General Assembly Resolution A/C.3/69/L.26/Rev.1 The right to privacy in the digital age of 19.11.2014. URL: https://undocs.org/en/A/C.3/69/L.26/Rev.1 (дата звернення: 03.10.2023).

24. UN General Assembly Resolution A/C.3/71/L.39/Rev.1 The right to privacy in the digital age of 16.11.2016. URL: https://undocs.org/A/C.3/71/L.39/Rev.1 (дата звернення: 03.10.2023).

25. UN General Assembly Resolution A/RES/75/176 The right to privacy in the digital age of 16.12.2020. URL: https://undocs.org/A/RES/75/176 (дата звернення: 03.10.2023).

26. European Convention on Human Rights of 04.11.1950, as amended by Protocols Nos. 11, 14 and 15, supplemented by Protocols Nos. 1, 4, 6, 7, 13 and 16. URL: https://www.echr.coe.int/documents/d/echr/convention_ENG (дата звернення: 03.10.2023).

27. American Convention on Human Rights, "Pact of San Jose, Costa Rica" (B-52), of 22.11.1969. URL: http://www.oas.org/dil/treaties_B-32_American_Convention_on_Human_Rights.pdf (дата звернення: 03.10.2023).

28. Declaration of Principles on Freedom of Expression in Africa, African Commission on Human and Peoples' Rights of 17 - 23 October 2002. URL: http://hrlibrary.umn.edu/achpr/expressionfreedomdec.html (дата звернення: 03.10.2023).

29. Declaration of Principles on Freedom of Expression in Africa, African Commission on Human and Peoples' Rights of 10 November 2019. URL: https://achpr.au.int/en/node/902 (дата звернення: 03.10.2023).

30. UN OHCHR. Special Rapporteur on the right to privacy. International standards. *OHCHR.* URL:

https://www.ohchr.org/EN/Issues/Privacy/SR/Pages/Internationalstandards.aspx (дата звернення: 03.10.2023).

31. Мішуровська С. Т. Міжнародно-правовий захист права на приватне життя (сучасна практика): автореф. дис. … канд. юрид. наук: 12.00.11 / Нац. юр. акад. ім. Я. Мудрого. Харків, 2011. 21 с.

32. Kovalenko Y. The place of the right to data protection in the existent human rights framework. *Права людини як індикатор розвитку сучасної держави* : матеріали міжн. наук.-практ. конф. (м. Київ, 13 груд. 2021 р.). Київ: «Видавництво Людмила», 2021. С. 16-18

33. Коваленко Ю. О. До питання становлення права на захист персональних даних у міжнародному праві. *Актуальні дослідження правової та історичної науки (випуск 24)*: матеріали міжн. наук.-практ. конф. (м. Тернопіль, 21 лип. 2020 р.). Тернопіль, 2020. С. 30-33.

34. Explanatory Report to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data. *Council of Europe*. URL: https://rm.coe.int/16800ca434 (дата звернення: 03.10.2023).

35. Сопілко І. М. Генезис змісту категорії «персональні дані». *Юридичний вісник. Повітряне і космічне право*. 2013. № 4. С. 62-66. URL: http://nbuv.gov.ua/UJRN/Npnau_2013_4_14 (дата звернення: 03.10.2023).

36. Gelman R. Fair Information Practices: A Basic Hustory. Washington, 2022. 59 p. URL: https://bobgellman.com/rg-docs/rg-FIPShistory.pdf (дата звернення: 03.10.2023).

37. van der Sloot B. Legal Fundamentalism: Is Data Protection Really a Fundamental Right? *Data Protection and Privacy: (In)visibilities and Infrastructures* / ed. by Leenes R., van Brakel R., Gutwirth S., De Hert P. URL: https://www.springer.com/gp/book/9783319507958 (дата звернення: 03.10.2023).

38. Теремецький В. І., Цвірюк Д. В. Застосування зарубіжного досвіду правового захисту персональних даних в Україні. *Часопис Академії адвокатури України*. Том 7 № 2 (23) 2014. С. 73-82. URL: http://nbuv.gov.ua/UJRN/Chaau_2014_7_2_11 (дата звернення: 03.10.2023).

39. Пазюк А. В. Захист прав людини стосовно обробки персональних даних: міжнародні стандарти. Київ: Інтертехнодрук, 2000. 69 с. URL: http://cyberpeace.org.ua/files/zahist_prav_ludini_stosovno_obrobki_personal_nih_danih-kniga1.pdf (дата звернення: 03.10.2023).

40. Council of Europe Convention No. 108 for the Protection of Individuals with regard to Automatic Processing of Personal Data of 28.01.1981. URL: https://rm.coe.int/1680078b37 (дата звернення: 03.10.2023).

41. Пазюк А. В. Міжнародно-правовий захист права людини на приватність персоніфікованої інформації: дис. ... канд. юрид. наук: 12.00.11 / Київ. нац. ун-т ім. Т. Шевченка. Київ, 2004. 205 с.

42. Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. *Official Journal of the European Union*. L 281. 23.11.1995 P. 0031–0050. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A31995L0046 (дата звернення: 03.10.2023).

43. Мельник К. С. Правові механізми захисту персональних даних в Європейському Союзі. *Правова інформатика*. 2013. №4 (40). С. 55-61. URL: http://ippi.org.ua/sites/default/files/13mksdes.pdf (дата звернення: 03.10.2023).

44. Фалалєєва Л. Г. Хартія Європейського Союзу про основоположні права 2007. *Енциклопедія міжнародного права*: у 3 т. / Ін-т держави і права ім. В. М. Корецького НАН України; редкол.: Ю. С. Шемшученко, В. Н. Денисов та ін.; Т. 3: М–Я. Київ: Академперіодика, 2019. С. 905-911.

45. Charter of Fundamental Rights of the European Union. *Official Journal of the European Union*. C 326. 26.10.2012. P. 391–407. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A12012P%2FTXT (дата звернення: 03.10.2023).

46. González Fuster G., Gellert R. The fundamental right of data protection in the European Union: in search of an uncharted right. *International Review of Law Computers & Technology*. 2012. Vol. 26 No. 1. P. 73-82. URL: https://doi.org/10.1080/13600869.2012.646798 (дата звернення: 03.10.2023).

47. 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) (Text with EEA relevance). *Official Journal of the European Union*. L 119, 04.05.2016, p. 1–88. URL: https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=celex%3A32016R0679 (дата звернення: 03.10.2023).

48. Greenleaf G. Renewing Convention 108: The CoE's 'GDPR Lite' Initiatives. *Privacy Laws & Business International Report*. 2016. P. 1-9. URL: https://ssrn.com/abstract=2892947 (дата звернення: 03.10.2023).

49. Modernised Convention for the Protection of Individuals with Regard to the Processing of Personal Data (ETS No. 108) of 18.05.2018. URL: https://search.coe.int/cm/Pages/result_details.aspx?ObjectId=09000016807c65bf#globalcontainer (дата звернення: 03.10.2023).

50. Draft Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No. 108) and its explanatory report of 15.11.2017. URL: https://pace.coe.int/pdf/36ab138256f0a983334eaf01dd430b7fba151cf54efc705ad1897211f6ccbece/doc.%2014437.pdf (дата звернення: 03.10.2023).

51. African Union Convention on Cyber Security and Personal Data Protection of 27.06.2014. URL: https://au.int/sites/default/files/treaties/29560-treaty-0048_-_african_union_convention_on_cyber_security_and_personal_data_protection_e.pdf (дата звернення: 03.10.2023).

52. List of countries which have signed, ratified/acceded to the African Union Convention on Cyber Security and Personal Data Protection as of 02.10.2020. *African Union.* URL: https://au.int/sites/default/files/treaties/29560-sl-AFRICAN_UNION_CONVENTION_ON_CYBER_SECURITY_AND_PERSONAL_DATA_PROTECTION.pdf (дата звернення: 03.10.2023).

53. Turianskyi Y. Africa and Europe: Cyber Governance Lessons. *SAIIA Policy Insights*. 2020. No.77. P. 1-14. URL: https://media.africaportal.org/documents/Policy-Insights-77-turianskyi.pdf (дата звернення: 03.10.2023).

54. Коваленко Ю. О. Становлення та розвиток європейських стандартів захисту персональних даних. *Наукові записки Інституту законодавства Верховної Ради України*. 2020. № 5. С. 59-67.

55. Размєтаєва Ю. С. Доктрина та практика захисту прав людини: навч. посіб. Київ: Вид-во «ФОП Голембовська О.О.», 2018. 364 с. URL: https://nlu.edu.ua/wp-content/uploads/2021/05/phd_1_copy.pdf (дата звернення: 03.10.2023).

56. Размєтаєва Ю. С. Розумні очікування у сфері приватності у цифрову епоху. *Правові новели. Науковий юридичний журнал*. 2020. № 12. С. 12–18. URL: http://legalnovels.in.ua/journal/12_2020/4.pdf (дата звернення: 03.10.2023).

57. Сухорольський П. М. Право на захист персональних даних як нове фундаментальне право людини в інформаційному суспільстві. *Wyzwania społeczeństwa informacyjnego. Polskie i ukraińskie doświadczenia* / ed. by Kancik-Kołtun E. Lublin: Wydawnictwo Uniwersytetu Marii Curie-Skłodowskiej, 2018. P. 15–25. URL: http://ena.lp.edu.ua:8080/bitstream/ntb/47391/1/Sukhorolskyi2018.pdf (дата звернення: 03.10.2023).

58. Tzanou M. Data protection as a fundamental right next to privacy? ‘Reconstructing’ a not so new right. *International Data Privacy Law*. 2013. Vol. 3 No. 2. P. 88-99. URL: https://doi.org/10.1093/idpl/ipt004 (дата звернення: 03.10.2023).

59. Kokott J., Sobotta C. The distinction between privacy and data protection in the jurisprudence of the CJEU and the ECtHR. *International Data Privacy Law*. 2013. Vol. 3 No. 4. P. 222–228 URL: https://doi.org/10.1093/idpl/ipt017 (дата звернення: 03.10.2023).

60. Lynskey O. Deconstructing data protection: the ‘added-value’ of a right to data protection in the EU legal order. *International and Comparative Law Quarterly*. 2014. Vol. 63 No. 3. P. 569–597. URL: https://core.ac.uk/download/pdf/207501264.pdf (дата звернення: 03.10.2023).

61. Mostert M., Bredenoord L. A., van der Sloot B., van Delden J. M. J. From Privacy to Data Protection in the eu: Implications for Big Data Health Research. *European Journal of Health Law*. 2018. Vol. 25 (1). P. 43-55. URL: https://doi.org/10.1163/15718093-12460346 (дата звернення: 03.10.2023).

62. de Hert P., Gutwirth S. Privacy, Data Protection and Law Enforcement. Opacity of the Individual and Transparency of Power. *Privacy and the criminal law* / ed. by Claes E., Duff A., Gutwirth S. Antwerpen, 2006. P. 61-104. URL: https://www.researchgate.net/publication/254800085_Privacy_Data_Protection_and_Law_Enforcement_Opacity_of_the_Individual_and_Transparency_of_Power (дата звернення: 03.10.2023).

63. de Andrade N. N. G. Data Protection, Privacy and Identity: Distinguishing Concepts and Articulating Rights. *Privacy and Identity Management for Life. Privacy and Identity* / ed. by Fischer-Hübner S., Duquenoy P., Hansen M., Leenes R., Zhang G. Berlin, 2010. P. 90-107. URL: https://doi.org/10.1007/978-3-642-20769-3_8 (дата звернення: 03.10.2023).

64. David M., Murthy G. Making Data Work for the Poor: New Approaches to Data Protection and Privacy. Washington, 2020. 24 p. URL: https://www.cgap.org/sites/default/files/publications/2020_01_Focus_Note_Making_Data_Work_for_Poor_0.pdf (дата звернення: 03.10.2023).

65. Decision of Supreme Court of the United States of 07.06.1965 in Griswold v. Connecticut. URL: https://supreme.justia.com/cases/federal/us/381/479/ (дата звернення: 03.10.2023).

66. McKay C. Complying with International Data Protection Law. *University of Cincinnati Law Review*. 2018. Vol. 84 No. 2. P. 421-450. URL: https://scholarship.law.uc.edu/uclr/vol84/iss2/4 (дата звернення: 03.10.2023).

67. Mészáros J. Two different approaches of the data protection law: the European Union and the United States. *Jog- És Politikatudományi Folyóirat Journal Of Legal And Political Sciences Ix. Évfolyam*. 2015. Vol. 9, No. 1. P. 1-12. URL: http://dieip.hu/wp-content/uploads/2015-1-04.pdf (дата звернення: 03.10.2023).

68. Серьогін В. О. Секторальний захист інформаційного прайвесі в Сполучених Штатах Америки. *Вісник Харківського національного університету імені В. Н. Каразіна*. 2019. № 27. С. 55-63. https://periodicals.karazin.ua/law/article/view/13112 (дата звернення: 03.10.2023).

69. Брижко В. М., Радянська А. І., Швець М. Я. Порівняльно-правове дослідження відповідності законодавства України законодавству ЄС у сфері персональних даних. Київ: Тріумф, 2006. 256 с.

70. Кардаш А. В. Конституційно-правовий захист інформації про особу (порівняльно-правовий аспект): дис. … канд. юрид наук: 12.00.02 / Нац. юр. ун-т ім. Я. Мудрого. Харків, 2019. 244 с.

71. Guadamuz A. Habeas Data vs the European Data Protection Directive. *The Journal of Information, Law and Technology (JILT)*. 2001. No. 3. P. 1-24. URL: https://era.ed.ac.uk/bitstream/handle/1842/2258/habeasdata.pdf;sequence=1 (дата звернення: 03.10.2023).

72. Relation between Privacy Protection, Data Protection and Habeas Data. *Organization of American States*. URL: http://www.oas.org/dil/data_protection_privacy_habeas_data.htm (дата звернення: 03.10.2023).

73. Working Party «Article 29» Opinion 1/99 concerning the level of data protection in the United States and the ongoing discussions between the European Commission and the United States Government of 26.01.1999. URL: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/1999/wp15_en.pdf (дата звернення: 03.10.2023).

74. Case C 362/14, Maximillian Schrems v. Data Protection Commissioner, Judgement of the Court (Grand Chamber) of 6 October 2015. ECLI:EU:C:2015:650. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62014CJ0362 (дата звернення: 03.10.2023).

75. Weiss Martin A., Archick K. U.S.-EU Data Privacy: From Safe Harbor to Privacy Shield. *Congressional Research Service*. 2016. P. 8-11. URL: https://fas.org/sgp/crs/misc/R44257.pdf (дата звернення: 03.10.2023).

76. Case C-311/18, Data Protection Commissioner v. Facebook Ireland Ltd, Maximillian Schrems, Judgement of the Court (Grand Chamber) of 16 July 2020. ECLI:EU:C:2020:559. URL:
http://curia.europa.eu/juris/document/document.jsf?text=&docid=228677&pageIndex=0&d

oclang=en&mode=req&dir=&occ=first&part=1&cid=9777234 (дата звернення: 03.10.2023).

77. President of the United States of America. Executive Order on Enhancing Safeguards for United States Signals Intelligence Activities. *The White House.* URL: https://www.whitehouse.gov/briefing-room/presidential-actions/2022/10/07/executive-order-on-enhancing-safeguards-for-united-states-signals-intelligence-activities/ (дата звернення: 03.10.2023).

78. Rules on international data transfers. *European Commission.* URL: https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/rules-international-data-transfers_en (дата звернення: 03.10.2023).

79. Kittichaisaree K., Kuner C. The Growing Importance of Data Protection in Public International Law. *EJIL:Talk!* 14 October 2015. URL: https://www.ejiltalk.org/the-growing-importance-of-data-protection-in-public-international-law/ (дата звернення: 03.10.2023).

80. Geenleaf G. The UN should adopt Data Protection Convention 108 as a global treaty: Submission on 'the right to privacy in the digital age' to the UN High Commission for Human Rights, to the Human Rights Council, and to the Special Rapporteur on the Right to Privacy. URL: https://www.ohchr.org/Documents/Issues/DigitalAge/ReportPrivacyinDigitalAge/GrahamGreenleafAMProfessorLawUNSWAustralia.pdf (дата звернення: 03.10.2023).

81. Buttarelli G. Convention 108: from a European Reality to a Global Treaty. *Council of Europe International Conference*. Strasbourg, 2016. URL: https://edps.europa.eu/sites/edp/files/publication/16-06-17_speech_strasbourg_coe_en.pdf (дата звернення: 03.10.2023).

82. Тихомиров О. О., Породько В. В., Полонська О. І. Правове регулювання захисту персональних даних: ел. навч. посіб. URL: http://zpd.inf.ua/ (дата звернення: 03.10.2023).

83. Бем М. В., Городиський І. М. Стандарти захисту персональних даних в соціальній сфері. Львів, 2018. 110 с.

84. Handbook on European data protection law. Luxembourg : Publications Office of the European Union, 2018. 408 p. URL: http://fra.europa.eu/sites/default/files/fra_uploads/fra-coe-edps-2018-handbook-data-protection_en.pdf (дата звернення: 03.10.2023).

85. Бєлова Ю. Д. Цивільні правовідносини щодо персональних даних: дис. … докт. філ. за спец. 081 «Право» / Хмельн. ун-т управл. та права ім. Л. Юзькова. Хмельницький, 2021. 244 с.

86. Working Party «Article 29» Opinion № 4/2007 on the concept of personal data of 20.06.2007. URL: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp136_en.pdf (дата звернення: 03.10.2023).

87. OECD Privacy Guidelines OECD/LEGAL/0188 of 23.09.1980, as amended on 11.07.2013 URL: https://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm (дата звернення: 03.10.2023).

88. Бем М. В., Городиський І. М., Саттон Г., Родіоненко О. М. Захист персональних даних: правове регулювання та практичні аспекти: наук.-практ. посіб. Київ : К.І.С., 2015. 220 с. URL: https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=090000168059920c (дата звернення: 03.10.2023).

89. Фалалєєва Л. Г. Рада Європи. *Енциклопедія міжнародного права*: у 3 т. / редкол.: Ю. С. Шемшученко, В. Н. Денисов (співголови) та ін.; Ін-т держави і права ім. В. М. Корецького НАН України. Київ: Академперіодика, 2019. Т. 3: М–Я. С. 661-666.

90. Фалалєєва Л. Г. Захист основоположних прав у інтеграційному правопорядку Європейського Союзу: монографія. Київ: ФОП Кандиба Т. П., 2020. 455 с.

91. Мазур М. В., Тагієв С. Р., Беніцький А. С., Кострицький В. В. Тлумачення та застосування Конвенції про захист прав й основоположних свобод Європейським судом з прав людини та судами України: навч. посіб. Луганськ: РВВ ЛДУВС, 2005. 600 с.

92. Parliamentary Assembly of Council of Europe Resolution 721 Data processing and the protection of human rights of 1 February 1980. URL: https://pace.coe.int/pdf/a4217a3f4a268a6213d14ee8d89453dad75d5c5f3326667a8259ffe25682ae848428feba12/resolution%20721.pdf (дата звернення: 03.10.2023).

93. Parliamentary Assembly of Council of Europe Reccomedation 890 Protection of personal data of 1 February 1980. URL: http://assembly.coe.int/nw/xml/XRef/Xref-XML2HTML-en.asp?fileid=14924&lang=en (дата звернення: 03.10.2023).

94. Byström N. The European Convention on Human Rights needs a Protocol on data protection: dissertation abstract. Helsinki, 2014. URL: https://helda.helsinki.fi/handle/10138/156726 (дата звернення: 03.10.2023).

95. Kovalenko Y. The Right to Privacy and Protection of Personal Data: Emerging Trends and the Implications for Development in the Jurisprudence of the European Court of Human Rights. *Masaryk University Journal of Law and Technology*. 2022. Vol. 16. No. 1. P. 37-57.

96. European Convention on Mutual Assistance in Criminal Matters (CETS No. 30), of 20.04.1959. *European Treaty Series*. 1959. No. 30. URL: https://rm.coe.int/16800656ce (дата звернення: 03.10.2023).

97. Convention on Cybercrime (CETS No. 185) Budapest, 23.11.2001. European Treaty Series. 2001. No. 185. URL: https://rm.coe.int/1680081561 (дата звернення: 03.10.2023).

98. Explanatory report to the Council of Europe Convention on access to official documents (CETS No. 205), Tromsø, 18.06.2009. URL https://rm.coe.int/16800d3836 (дата звернення: 03.10.2023).

99. Data protection. Normative instruments - Parliamentary Assembly. *Council of Europe.* URL: https://www.coe.int/en/web/data-protection/legal-instruments (дата звернення: 03.10.2023).

100. Reservations and Declarations for Treaty No.005 - Convention for the Protection of Human Rights and Fundamental Freedoms. *Council of Europe*. URL: https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/005/declarations?p_auth=EBn2HCJC (дата звернення: 03.10.2023).

101. Digital solutions to fight Covid-19. 2020 Data Protection Report. Council of Europe, October 2020. *Council of Europe.* URL: https://rm.coe.int/prems-120820-gbr-2051-digital-solutions-to-fight-covid-19-text-a4-web-/16809fe49c (дата звернення: 03.10.2023).

102. Kovalenko Y. O. Right to data protection in the times of COVID-19: challenges and prospects in the ECtHR. *Сучасне правотворення: питання теорії та практики*:

матеріали міжн. наук.-практ. конф. (м. Дніпро, 4-5 черв. 2021 р.). Дніпро: ГО «Правовий світ», 2021. С. 145-149.

103. Ventrella E. Privacy in emergency circumstances: data protection and the COVID-19 pandemic. *ERA Forum*. 2020. Vol. 21. P. 379–393.

104. Personal data of deceased persons. *Two birds*. URL: https://www.twobirds.com/en/in-focus/general-data-protection-regulation/gdpr-tracker/deceased-persons (дата звернення: 03.10.2023).

105. Second Additional Protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence. Draft Protocol (T-CY (2020)7) of 28.05.2021. URL: https://rm.coe.int/0900001680a2aa1c (дата звернення: 03.10.2023).

106. Chart of signatures and ratifications of Treaty 224. Second Additional Protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence (CETS No. 224). Status as of 08.10.2023. *Council of Europe*. URL: https://www.coe.int/en/web/conventions/full-list?module=signatures-by-treaty&treatynum=224 (дата звернення: 03.10.2023).

107. CAI - Committee on Artificial Intelligence. *Council of Europe*. URL: https://www.coe.int/en/web/artificial-intelligence/cai (дата звернення: 03.10.2023).

108. Карвацька С. Б. Інтерпретація норм міжнародного права: теоретичні та практичні аспект: дис. … д-ра юрид. наук: 12.00.01 / Київ. нац. ун-т ім. Т. Шевченка. Київ, 2020. 555 с.

109. Beegrave L. A. Data Protection Pursuant to the Right to Privacy in Human Rights Treaties. 1998. 28 p. (Preprint. International Journal of Law and Information Technology). URL:https://www.uio.no/studier/emner/jus/jus/JUR5630/v11/undervisningsmateriale/Human_rights.pdf (дата звернення: 03.10.2023).

110. van der Sloot B. Privacy as human flourishing: Could a shift towards virtue ethics strengthen privacy protection in the age of Big Data? *JIPITEC*. 2014. Vol.5. URL: https://www.jipitec.eu/issues/jipitec-5-3-2014/4097 (дата звернення: 03.10.2023).

111. Case of Tyrer v. the United Kingdom, application no. 5856/72, Judgement of European Court of Human Rights of 25 April 1978. URL: https://hudoc.echr.coe.int/fre?i=001-57587 (дата звернення: 03.10.2023).

112. Case of Airey v. Ireland, application no. 6289/73, Judgement of European Court of Human Rights of 09 March 1977. URL: https://hudoc.echr.coe.int/eng?i=001-57420 (дата звернення: 03.10.2023).

113. Mowbray A. R. An Examination of the European Court of Human Rights' Approach to Overruling its Previous Case Law. 2009. 29 p. (Preprint, Human Rights Law Review). URL: https://nottingham-repository.worktribe.com/output/1014665/an-examination-of-the-european-court-of-human-rights-approach-to-overruling-its-previous-case-law (дата звернення: 03.10.2023).

114. van der Sloot B. Privacy as Personality Right: Why the ECtHR's Focus on Ulterior Interests Might Prove Indispensable in the Age of "Big Data". *Utrecht Journal of International and European Law*. 2015. Vol. 31. No. 80. P. 25–50. URL: https://doi.org/10.5334/ujiel.cp (дата звернення: 03.10.2023).

115. Case of Leander v. Sweden, application no. 9248/81, Judgement of European Court of Human Rights 26 March 1987. URL: https://hudoc.echr.coe.int/eng?i=001-57519 (дата звернення: 03.10.2023).

116. Case of Amann v. Switzerland, application no. 27798/95, Judgement of European Court of Human Rights (Grand Chamber) of 16 February 2000. URL: https://hudoc.echr.coe.int/eng?i=001-58497 (дата звернення: 03.10.2023).

117. Case of Garnaga v. Ukraine, application no. 20390/07, Judgment of European Court of Human Rights of 16 May 2003. URL: https://hudoc.echr.coe.int/eng?i=001-119681 (дата звернення: 03.10.2023).

118. Case of Odièvre v. France, application no. 42326/98, Judgment of European Court of Human Rights of 13 February 2003. URL: https://hudoc.echr.coe.int/eng?i=001-60935 (дата звернення: 03.10.2023).

119. Case of L. H. v. Latvia, application no. 52019/07, Judgment of European Court of Human Rights of 29 April 2014. URL: https://hudoc.echr.coe.int/eng?i=001-142673 (дата звернення: 03.10.2023).

120. Case of S. and Marper v. the United Kingdom, application nos. 30562/04 and 30566/04, Judgment of European Court of Human Rights (Grand Chamber) of 04 December 2008. URL: https://hudoc.echr.coe.int/eng?i=001-90051 (дата звернення: 03.10.2023).

121. Case of Von Hannover v. Germany (no. 2), application nos. 40660/08 and 60641/08, Judgment of European Court of Human Rights (Grand Chamber) of 07 February 2012. URL: https://hudoc.echr.coe.int/eng?i=001-109029 (дата звернення: 03.10.2023).

122. Case of Sõro v. Estonia, application no. 22588/08, Judgment of European Court of Human Rights of 03 September 2015. URL: https://hudoc.echr.coe.int/eng?i=001-156518 (дата звернення: 03.10.2023).

123. Case of Drelon v. France, application no. 3153/16 and 27758/18, Judgment of European Court of Human Rights of 08 September 2022. URL: https://hudoc.echr.coe.int/eng?i=001-219069 (дата звернення: 03.10.2023).

124. Roagna I. Protecting the right to respect for private and family life under the European Convention on Human Rights. Council of Europe, Strasbourg, 2012. 106 p. URL: https://rm.coe.int/16806f1554 (дата звернення: 03.10.2023).

125. van der Sloot B. The Quality of Law: How the European Court of Human Rights Gradually Became a European Constitutional Court for Privacy Cases. *JIPITEC*. 2020. Vol. 11 (2). URL: https://www.jipitec.eu/issues/jipitec-11-2-2020/5098 (дата звернення: 03.10.2023).

126. Case of Malone v. the United Kingdom, application no. 8691/79, Judgment of European Court of Human Rights of 2 August 1984. URL: https://hudoc.echr.coe.int/eng?i=001-57533 (дата звернення: 03.10.2023).

127. Case of Rotaru v. Romania, application no. 28341/95, Judgement of European Court of Human Rights (Grand Chamber) of 04 May 2000. URL: https://hudoc.echr.coe.int/eng?i=001-58586 (дата звернення: 03.10.2023).

128. Case of Weber and Saravia v. Germany, application no. 54934/00, Decision of European Court of Human Rights of 29 June 2006. URL: https://hudoc.echr.coe.int/eng?i=001-76586 (дата звернення: 03.10.2023).

129. Case of Roman Zakharov v. Russia, application no. 47143/06, Judgement of European Court of Human Rights (Grand Chamber) of 04 December 2015.URL: https://hudoc.echr.coe.int/eng?i=001-159324 (дата звернення: 03.10.2023).

130. Андрущенко К. А. Правова природа концепції «margin of appreciation»: дис. …. канд. юр. наук.: 12.00.11 / Київ. нац. ун-т ім. Т. Шевченка. Київ, 2017. 226 с.

131. Byström N. The Data Subject and the European Convention on Human Rights: Access to Own Data. *EDILEX*. 2016. P. 209-246. URL: https://www.edilex.fi/viestintaoikeuden-vuosikirja/181000010?classIds[]=508&offset=8701&perpage=50&sort=relevance&searchSrc=1&advancedSearchKey=1187643 (дата звернення: 03.10.2023).

132. Case of Hämäläinen v. Finland, application no. 37359/09, Judgment of European Court of Human Rights (Grand Chamber) of 16 July 2014. URL: https://hudoc.echr.coe.int/eng?i=001-145768 (дата звернення: 03.10.2023).

133. Case of M. K. v. France, application no. 30148/96, Decision of European Court of Human Rights of 19 September 1997. URL: https://hudoc.echr.coe.int/app/conversion/pdf/?library=ECHR&id=001-87707&filename=M.K.%20v.%20FRANCE.pdf (дата звернення: 03.10.2023).

134. Case of Big Brother Watch and Others v. the United Kingdom, application nos. 58170/13, 62322/14 and 24960/15, Judgment of European Court of Human Rights (Grand Chamber) of 25 May 2021. URL: https://hudoc.echr.coe.int/eng?i=001-210077 (дата звернення: 03.10.2023).

135. Case of Centrum för rättvisa v. Sweden, application no. 35252/08, Judgment of European Court of Human Rights (Grand Chamber) of 25 May 2021. URL: https://hudoc.echr.coe.int/eng?i=001-210078 (дата звернення: 03.10.2023).

136. Case of Gaskin v. the United Kingdom, application no. 10454/83, Judgment of European Court of Human Rights of 07 July 1989. URL: https://hudoc.echr.coe.int/eng?i=001-57491 (дата звернення: 03.10.2023).

137. Case of Palomo Sánchez and Others v. Spain, application nos. 28955/06, 28957/06, 28959/06 and 28964/06, Judgment of European Court of Human Rights (Grand Chamber) of 12 September 2011. URL: https://hudoc.echr.coe.int/eng?i=001-106178 (дата звернення: 03.10.2023).

138. Case of Liebscher v. Austria, application no. 5434/17, Judgment of European Court of Human Rights of 06 April 2021. URL: https://hudoc.echr.coe.int/eng?i=001-209035 (дата звернення: 03.10.2023).

139. Case of Ciubotaru v. Moldova, application no. 27138/04, Judgment of European Court of Human Rights of 27 April 2010. URL: https://hudoc.echr.coe.int/eng?i=001-98445 (дата звернення: 03.10.2023).

140. Case of Bărbulescu v. Romania, application no. 61496/08, Judgment of European Court of Human Rights (Grand Chamber) of 12 January 2016. URL: https://hudoc.echr.coe.int/eng?i=001-159906 (дата звернення: 03.10.2023).

141. Case of Peck v. the United Kingdom, application no. 44647/98, Judgment of European Court of Human Rights of 28 January 2003. URL: https://hudoc.echr.coe.int/eng?i=001-60898 (дата звернення: 03.10.2023).

142. Case of Uzun v. Germany, application no. 35623/05, Judgment of European Court of Human Rights of 02 September 2010. URL: https://hudoc.echr.coe.int/eng?i=001-100293 (дата звернення: 03.10.2023).

143. Case of Benedik v. Slovenia, application no. 62357/14, Judgment of European Court of Human Rights of 24 Aoril 2018. URL: https://hudoc.echr.coe.int/eng?i=001-182455 (дата звернення: 03.10.2023).

144. Case of Z v. Finland, application no. 22009/93, Judgment of European Court of Human Rights of 25 February 1997. URL: https://hudoc.echr.coe.int/eng?i=001-58033 (дата звернення: 03.10.2023).

145. Case of M. K. v. Ukraine, application no. 24867/13, Judgment of European Court of Human Rights of 15 September 2022. URL: https://hudoc.echr.coe.int/eng?i=001-219198 (дата звернення: 03.10.2023).

146. Case of Copland v. the United Kingdom, application no. 62617/00, Judgment of European Court of Human Rights of 03 April 2007. URL: https://hudoc.echr.coe.int/eng?i=001-79996 (дата звернення: 03.10.2023).

147. Case of Vukota-Bojić v. Switzerland, application no. 61838/10, Judgment of European Court of Human Rights of 18 October 2016. URL: https://hudoc.echr.coe.int/eng?i=001-167490 (дата звернення: 03.10.2023).

148. Лутковська В., Кушнір І., Лук’яненко Ж., Крикливенко Б. Міжнародні стандарти прав людини. Київ: Український інститут з прав людини, 2019. 145 с. URL:

https://www.irf.ua/content/files/international_human_rights_standards._journalism.pdf (дата звернення: 03.10.2023).

149. Case of K. H. and Others v. Slovakia, application no. 32881/04, Judgment of European Court of Human Rights of 28 April 2009. URL: https://hudoc.echr.coe.int/eng?i=001-92418 (дата звернення: 03.10.2023).

150. Case of Dalea v. France, application no. 964/07, Decision of European Court of Human Rights of 02 October 2002. URL: https://hudoc.echr.coe.int/eng#{%22tabview%22:[%22document%22],%22itemid%22:[%2001-97520%22]} (дата звернення: 03.10.2023).

151. Kovalenko Y. Balancing right to personal data protection towards other fundamental rights through the prism of the case law of the ECtHR and the CJEU. *Visegrad Journal on Human Rights*. 2022. No. 2. P. 52-57.

152. Case of L. L. v. France, application no. 7508/02, Judgment of European Court of Human Rights of 10 October 2010. URL: https://hudoc.echr.coe.int/eng?i=001-77356 (дата звернення: 03.10.2023).

153. Case of Panteleyenko v. Ukraine, application no. 11901/02, Judgment of European Court of Human Rights of 29 June 2006. URL: https://hudoc.echr.coe.int/eng?i=001-76114 (дата звернення: 03.10.2023).

154. Case of Surikov v. Ukraine, application no. 42788/06, Judgment of European Court of Human Rights of 26 January 2017. URL: https://hudoc.echr.coe.int/eng?i=001-170462 (дата звернення: 03.10.2023).

155. Case of Sinan Işık v. Turkey, application no. 21924/05, Judgment of European Court of Human Rights of 02 February 2010. URL: https://hudoc.echr.coe.int/eng?i=001-97087 (дата звернення: 03.10.2023).

156. Case of Alexandridis v. Greece, application no. 19516/06, Judgment of European Court of Human Rights of 21 February 2008. URL: https://hudoc.echr.coe.int/eng?i=001-85189 (дата звернення: 03.10.2023).

157. Case of Dimitras and Others v. Greece, application nos. 42837/06, 3237/07 and 3269/07, Judgment of European Court of Human Rights of 03 June 2010. URL: https://hudoc.echr.coe.int/eng?i=001-99014 (дата звернення: 03.10.2023).

158. Case of Biancardi v. Italy, application no. 77419/16, Judgment of European Court of Human Rights of 25 November 2021. URL: https://hudoc.echr.coe.int/eng?i=001-213827 (дата звернення: 03.10.2023).

159. Case of Centre for Democracy and the Rule of Law v. Ukraine, application no. 10090/16, Judgment of European Court of Human Rights of 26 March 2020. URL: https://hudoc.echr.coe.int/eng?i=001-201896 (дата звернення: 03.10.2023).

160. McBride J. The doctrines and methodology of interpretation of the European Convention on Human Rights by the European Court of Human Rights. Council of Europe, Strasbourg, 2021. URL: https://rm.coe.int/echr-eng-the-doctrines-and-methodology-of-interpretation-of-the-europe/1680a20aee (дата звернення: 03.10.2023).

161. Case of Haralambie v. Romania, application no. 21737/03, Judgment of European Court of Human Rights of 27 October 2009. URL: https://hudoc.echr.coe.int/eng?i=001-95397 (дата звернення: 03.10.2023).

162. Case of P. G. and J. H. v. the United Kingdom, application no. 44787/98, Judgment of European Court of Human Rights of 25 September 2001. URL: https://hudoc.echr.coe.int/eng?i=001-59665 (дата звернення: 03.10.2023).

163. Case of Bulgakov v. Ukraine, application no. 59894/00, Judgment of European Court of Human Rights of 11 September 2007. URL: https://hudoc.echr.coe.int/eng?i=001-82241 (дата звернення: 03.10.2023).

164. Case of Alkaya v. Turkey, application no. 42811/06, Judgment of European Court of Human Rights of 9 October 2012. URL: https://hudoc.echr.coe.int/eng?i=001-114031 (дата звернення: 03.10.2023).

165. Case of Antović and Mirković v. Montenegro, application no. 70838/13, Judgment of European Court of Human Rights of 28 November 2017. URL: https://hudoc.echr.coe.int/eng?i=001-178904 (дата звернення: 03.10.2023).

166. Case of Breyer v. Germany, application no. 50001/12, Judgment of European Court of Human Rights of 30 January 2020. URL: https://hudoc.echr.coe.int/eng?i=001-200442 (дата звернення: 03.10.2023).

167. Case of Khelili v. Switzerland, application no. 16188/07, Judgment of European Court of Human Rights of 18 October 2011. URL: https://hudoc.echr.coe.int/eng?i=001-107033 (дата звернення: 03.10.2023).

168. Case of Association “21 December 1989” and others v. Romania, application no. 33810/07, Judgment of European Court of Human Rights of 24 May 2011. URL: https://hudoc.echr.coe.int/eng?i=001-104864 (дата звернення: 03.10.2023).

169. Case of M. N. and Others v. San Marino, application no. 28005/12, Judgment of European Court of Human Rights of 7 July 2015. URL: https://hudoc.echr.coe.int/eng?i=001-155819 (дата звернення: 03.10.2023).

170. Case of G. S. B. v. Switzerland, application no. 28601/11, Judgment of European Court of Human Rights of 22 December 2015. URL: https://hudoc.echr.coe.int/eng?i=001-159732 (дата звернення: 03.10.2023).

171. Case of Brito Ferrinho Bexiga Villa-Nova v. Portugal, application no. 69436/10, Judgment of European Court of Human Rights of 1 December 2015. URL: https://hudoc.echr.coe.int/eng?i=001-158949 (дата звернення: 03.10.2023).

172. Case of National Federation of Sportspersons’ Associations and Unions (FNASS) and others v. France, application nos. 48151/11 and 77769/13, Judgment of European Court of Human Rights of 18 January 2018. URL: https://hudoc.echr.coe.int/eng?i=001-180442 (дата звернення: 03.10.2023).

173. Case of P. and S. v. Poland, application no. 57375/08, Judgment of European Court of Human Rights of 30 October 2012. URL: https://hudoc.echr.coe.int/eng?i=001-114098 (дата звернення: 03.10.2023).

174. Case of L. B. v Hungary, application no. 36345/16, Judgment of European Court of Human Rights of 12 January 2021. URL: https://hudoc.echr.coe.int/eng?i=001-207132 (дата звернення: 03.10.2023).

175. Case of L. B. v Hungary, application no. 36345/16, Judgment of European Court of Human Rights (Grand Chamber) of 9 March 2023. URL: https://hudoc.echr.coe.int/eng?i=001-223675 (дата звернення: 03.10.2023).

176. Case of Kırdök and Others v. Turkey, application no. 14704/12, Judgment of European Court of Human Rights of 3 December 2019. URL: https://hudoc.echr.coe.int/eng?i=001-199183 (дата звернення: 03.10.2023).

177. Case of Rodina v. Latvia, application nos. 48534/10 and 19532/15, Judgment of European Court of Human Rights of 14 May 2020. URL: https://hudoc.echr.coe.int/eng?i=001-202437 (дата звернення: 03.10.2023).

178. Guide to the Case-Law of the of the European Court of Human Rights : Data protection. 2022. URL: https://www.echr.coe.int/documents/d/echr/fs_data_eng (дата звернення: 03.10.2023).

179. Case of Willems v. the Netherlands, application no. 57294/16, Decision of European Court of Human Rights of 9 November 2021. URL: https://hudoc.echr.coe.int/eng?i=001-214169 (дата звернення: 03.10.2023).

180. Case of Cakicisoy and Others v. Cyprus, application no. 6523/12, Decision of European Court of Human Rights of 23 September 2014. URL: https://hudoc.echr.coe.int/eng?i=001-147481 (дата звернення: 03.10.2023).

181. Case of Mehmedovic v. Switzerland, application no. 17331/11, Decision of European Court of Human Rights of 11 December 2018. .URL: https://hudoc.echr.coe.int/eng?i=001-189472 (дата звернення: 03.10.2023).

182. Case of Khadija Ismayilova v. Azerbaijan, application nos. 65286/13 and 57270/14, Judgment of European Court of Human Rights of 10 January 2019. URL: https://hudoc.echr.coe.int/eng?i=001-188993 (дата звернення: 03.10.2023).

183. Case of Bernh Larsen Holding AS and Others v. Norway, application no. 24117/08, Judgment of European Court of Human Rights of 14 March 2013. URL: https://hudoc.echr.coe.int/eng?i=001-117133 (дата звернення: 03.10.2023).

184. Case of Liberty and Others v. the United Kingdom, application no. 58243/00, Judgment of European Court of Human Rights of 1 July 2008. URL: https://hudoc.echr.coe.int/eng?i=001-87207 (дата звернення: 03.10.2023).

185. Case of Satakunnan Markkinapörssi Oy and Satamedia Oy v. Finland, application no. 931/13, Judgment of European Court of Human Rights (Grand Chamber) of 27 June 2017. URL: https://hudoc.echr.coe.int/eng?i=001-175121 (дата звернення: 03.10.2023).

186. Case of Catt v. the United Kingdom, application no. 43514/15, Judgment of European Court of Human Rights of 24 January 2019. URL: https://hudoc.echr.coe.int/eng?i=001-189424 (дата звернення: 03.10.2023).

187. Case of Klass and Others v. Germany, application no. 5029/71, Judgment of European Court of Human Rights of 6 September 1978. URL: https://hudoc.echr.coe.int/eng?i=001-57510 (дата звернення: 03.10.2023).

188. Case of Ekimdzhiev and Others v. Bulgaria, application no. 70078/12, Judgment of European Court of Human Rights of 11 January 2022. URL: https://hudoc.echr.coe.int/eng?i=001-214673 (дата звернення: 03.10.2023).

189. Case of Kopp v. Switzerland, application no. 23224/94, Judgment of European Court of Human Rights of 25 March 1998. URL: https://hudoc.echr.coe.int/eng?i=001-58144 (дата звернення: 03.10.2023).

190. Case of Köpke v. Germany, application no. 420/07, Decision of European Court of Human Rights of 22 December 2006. URL: https://hudoc.echr.coe.int/eng?i=001-101536 (дата звернення: 03.10.2023).

191. Case of Hambardzumyan v. Armenia, application no. 43478/11, Judgment of European Court of Human Rights of 5 December 2019. URL: https://hudoc.echr.coe.int/eng?i=001-198708 (дата звернення: 03.10.2023).

192. Case of Ben Faiza v. France, application no. 31446/12, Judgment of European Court of Human Rights of 8 February 2018. URL: https://hudoc.echr.coe.int/eng?i=001-180657 (дата звернення: 03.10.2023).

193. Case of Glukhin v. Russia, application no. 11519/20, Judgment of European Court of Human Rights of 4 July 2023. URL: https://hudoc.echr.coe.int/eng?i=001-225655 (дата звернення: 03.10.2023).

194. Case of Dmitrov-Kazakov v. Bulgaria, application no. 11379/03, Judgment of European Court of Human Rights of 10 February 2011. URL: https://hudoc.echr.coe.int/eng?i=001-103259 (дата звернення: 03.10.2023).

195. Case of Shimovolos v. Russia, application no. 30194/09, Judgment of European Court of Human Rights of 21 June 2011. URL: https://hudoc.echr.coe.int/eng?i=001-105217 (дата звернення: 03.10.2023).

196. Case of Gardel v. France, application no. 16428/05, Judgment of European Court of Human Rights of 17 December 2009. URL: https://hudoc.echr.coe.int/eng?i=001-96457 (дата звернення: 03.10.2023).

197. Case of M. D. and Others v. Spain, application no. 36584/17, Judgment of European Court of Human Rights of 28 June 2022. URL: https://hudoc.echr.coe.int/eng?i=001-218034 (дата звернення: 03.10.2023).

198. Case of Biriuk v. Lithuania, application no. 23373/03, Judgment of European Court of Human Rights of 25 November 2008. URL: https://hudoc.echr.coe.int/eng?i=001-89827 (дата звернення: 03.10.2023).

199. Case of Hájovský v. Slovakia, application no. 7796/16, Judgment of European Court of Human Rights of 1 July 2021. URL: https://hudoc.echr.coe.int/eng?i=001-210766 (дата звернення: 03.10.2023).

200. Case of Antović and Mirković v. Montenegro, application no. 70838/13, Judgment of European Court of Human Rights of 28 November 2017. URL: https://hudoc.echr.coe.int/eng?i=001-178904 (дата звернення: 03.10.2023).

201. Case of López Ribalda and Others v. Spain, application nos. 1874/13 and 8567/13, Judgment of European Court of Human Rights (Grand Chamber) of 17 October 2019. URL: https://hudoc.echr.coe.int/eng?i=001-197098 (дата звернення: 03.10.2023).

202. Case of Mockutė v. Lithuania, application no. 66490/09, Judgment of European Court of Human Rights of 27 February 2018. URL: https://hudoc.echr.coe.int/eng?i=001-181202 (дата звернення: 03.10.2023).

203. Case of Vasil Vasilev v. Bulgaria, application no. 7610/15, Judgment of European Court of Human Rights of 16 November 2021. URL: https://hudoc.echr.coe.int/eng?i=001-213201 (дата звернення: 03.10.2023).

204. Case of Karabeyoğlu v. Turkey, application no. 30083/10, Judgment of European Court of Human Rights of 7 June 2016. URL: https://hudoc.echr.coe.int/fre?i=001-163926 (дата звернення: 03.10.2023).

205. Case of P. N. v. Germany, application no. 74440/17, Judgment of European Court of Human Rights of 11 June 2020. URL: https://hudoc.echr.coe.int/eng?i=001-202758 (дата звернення: 03.10.2023).

206. Case of Gaugrahan v. the United Kingdom, application no. 45245/15, Judgment of European Court of Human Rights of 13 February 2020. URL: https://hudoc.echr.coe.int/fre?i=001-200817 (дата звернення: 03.10.2023).

207. Case of Trajkovski and Chipovski v. North Macedonia, application nos. 53205/13 and 63320/13, Judgment of European Court of Human Rights of 13 February 2020. URL: https://hudoc.echr.coe.int/eng?i=001-200816 (дата звернення: 03.10.2023).

208. Case of Ayçaguer v. France, application no. 8806/12, Judgment of European Court of Human Rights of 22 June 2017. URL: https://hudoc.echr.coe.int/eng?i=001-175007 (дата звернення: 03.10.2023).

209. Muraviov V., Sviatun O. Protection of Human Rights in the European Union. *The Convergence of the Fundamental Rights Protection in Europe* : ed. by Rainer A. Dordrecht, 2016. P. 185–197. URL: https://doi.org/10.1007/978-94-017-7465-9_10 (дата звернення: 03.10.2023).

210. Consolidated versions of the Treaty on European Union and the Treaty on the Functioning of the European Union. *Official Journal of the European Union*. C 202/01. Vol. 59. 7 June 2016. URL: https://eur-lex.europa.eu/legalcontent/EN/TXT/HTML/?uri=OJ:C:2016:202:FULL&from=EN (дата звернення: 03.10.2023).

211. Granger M.-P., Irion K. The right to protection of personal data: the new posterchild of European Union citizenship? *Civil Rights and EU Citizenship /* ed by de Vries, S., de Waele, H., Granger, M.-P. Cheltenham : Edward Elgar Publishing, 2018. 309 p. URL: https://doi.org/10.4337/9781788113441.00019 (дата звернення: 03.10.2023).

212. Cases C-203/15 and C-698/15, Tele2 Sverige v. Post-och telestyrelsen and Secretary of State for the Home Department v. Tom Watson and Others, Judgement of Court (Grand Chamber) of 21 December 2016. ECLI:EU:C:2016:970. URL: https://curia.europa.eu/juris/liste.jsf?num=C-203/15 (дата звернення: 03.10.2023).

213. Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data. *Official Journal of the European Union.* L 8. 12.01.2001. P. 1-22. URL: https://eur-

lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32001R0045 (дата звернення: 03.10.2023).

214. Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications). *Official Journal of the European Union.* L 201. 31.07.2002 P. 37-47. URL: https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A32002L0058 (дата звернення: 03.10.2023).

215. Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009 amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and Regulation (EC) No 2006/2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws (Text with EEA relevance). *Official Journal of the European Union*. L 337. 18.12.2009. P. 11–36. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32009L0136 (дата звернення: 03.10.2023).

216. Commission Regulation (EU) No 611/2013 of 24 June 2013 on the measures applicable to the notification of personal data breaches under Directive 2002/58/EC of the European Parliament and of the Council on privacy and electronic communications. *Official Journal of the European Union.* L 173, 26.06.2013, P. 2–8. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32013R0611 (дата звернення: 03.10.2023).

217. Directive 2006/24/ЄС of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC. *Official Journal of the European Union.* L 105. 13.04.2006. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32006L0024 (дата звернення: 03.10.2023).

218. Case C-293/12, Digital Rights Ireland Ltd v. Minister for Communications, Marine and Natural Resourcesand Others and Kärntner Landesregierung and Others, Judgment of the

Court (Grand Chamber) of 8 April 2014. ECLI:EU:C:2014:238. URL: https://curia.europa.eu/juris/documents.jsf?num=C-293/12 (дата звернення: 03.10.2023).

219. Council Framework Decision 2008/977/JHA of 27 November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters. *Official Journal of the European Union.* L 350. 30.12.2008. P. 60–71. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32008F0977 (дата звернення: 03.10.2023).

220. Directive (EU) 2016/680 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 by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data and repealing Council Framework Decision 2008/977/JHA. *Official Journal of the European Union.* L 119. 4.05.2016. P. 89–131. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32016L0680 (дата звернення: 03.10.2023).

221. Radtke T. The concept of Joint Control under the Data Protection Law Enforcement Directive 2016/680 in contrast to the GDPR. *JIPITEC*. 2021. Vol. 11. P.242-252. URL: https://www.jipitec.eu/issues/jipitec-11-3-2020/5189 (дата звернення: 03.10.2023).

222. Quintel T. Article 29 Data Protection Working Party Opinion on the Law Enforcement Directive. *European Data Protection Law Review*. 2018. Vol. 4, No. 1, P.104-109. URL: https://edpl.lexxion.eu/article/EDPL/2018/1/15 (дата звернення: 03.10.2023).

223. Leiser M. R., Custers B. H. M. The Law Enforcement Directive: Conceptual Issues of EU Directive 2016/680. *European Data Protection Law Review*. 2019. Vol. 5. No. 3. P. 367-378. URL: https://scholarlypublications.universiteitleiden.nl/handle/1887/79246 (дата звернення: 03.10.2023).

224. Directive (EU) 2016/681 of the European Parliament and of the Council, of 27 April 2016 On the use of passenger name record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime. *Official Journal of the European Union.* L 119, 4.05.2016, P. 132–149. URL: https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A32016L0681 (дата звернення: 03.10.2023).

225. Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (Text with EEA relevance). *Official Journal of the European Union.* L 295. 21.11.2018. P. 39–98. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32018R1725 (дата звернення: 03.10.2023).

226. Tracol X. Chapter V of Regulation (EU) 2018/1725 on transfers of personal data by Union institutions and bodies to third states and international organisations. *ERA Forum*. 2021. Vol. 22. P. 541–556. URL: https://doi.org/10.1007/s12027-021-00679-1 (дата звернення: 03.10.2023).

227. Directive (EU) 2019/1937 of the European Parliament and of the Council on the protection of persons who report breaches of Union law of 23 October 2019. *Official Journal of the European Union.* L 305, 26.11.2019, P. 17–56. URL: https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A32019L1937 (дата звернення: 03.10.2023).

228. Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts of 21.04.2021 2021/0106(COD). URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52021PC0206 (дата звернення: 03.10.2023).

229. EU AI Act: first regulation on artificial intelligence. *News European Parliament.* URL: https://www.europarl.europa.eu/news/en/headlines/society/20230601STO93804/eu-ai-act-first-regulation-on-artificial-intelligence (дата звернення: 03.10.2023).

230. Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive). *Official Journal of the European Union.* L 333. 27.12.2022. P. 80–152. URL: https://eur-lex.europa.eu/eli/dir/2022/2555/oj (дата звернення: 03.10.2023).

231. Hustinx P. European Leadership in Privacy and Data Protection. *European Data Protection Board.* URL: https://edps.europa.eu/sites/edp/files/publication/14-09-08_article_uji_castellon_en.pdf (дата звернення: 03.10.2023).

232. Sayenko Kharenko. Analysis of Data Privacy Laws and Legislation in Ukraine Final Report (the «Memorandum»). Kyiv, 2020. URL: https://ecpl.com.ua/wp-content/uploads/2020/09/ENG_09142020-_CEP_Final-Report.pdf (дата звернення: 03.10.2023).

233. 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". Brussels, 4.11.2010. URL: https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2010:0609:FIN:EN:PDF (дата звернення: 03.10.2023).

234. Press release, 25 January 2012, Commission proposes a comprehensive reform of data protection rules to increase users' control of their data and to cut costs for businesses. *European Commission.* URL: https://ec.europa.eu/commission/presscorner/detail/en/IP_12_46 (дата звернення: 03.10.2023).

235. European Data Protection Board Guidelines Adopted 3 / 2018 on the territorial scope of the GDPR (Article 3) of 12 November 2019. URL: https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_3_2018_territorial_scope_after_public_consultation_en.pdf (дата звернення: 03.10.2023).

236. European Data Protection Board Guidelines 05/2020 on consent under Regulation 2016/679 of 04 May 2020. URL: https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202005_consent_en.pdf (дата звернення: 03.10.2023).

237. Case C-131/12, Google Spain SL, Google Inc. v Agencia Española de Protección de Datos, Mario Costeja González, Judgment of the Court (Grand Chamber) of 13 May 2014. ECLI:EU:C:2014:317. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62012CJ0131 (дата звернення: 03.10.2023).

238. Reding V. The EU Data Protection Reform 2012: Making Europe the Standard Setter for Modern Data Protection Rules in the Digital Age Innovation Conference Digital, Life, Design. URL: https://ec.europa.eu/commission/presscorner/detail/en/SPEECH_12_26 (дата звернення: 03.10.2023).

239. European Data Protection Board, Guidelines 4 / 2019 on Article 25 Data Protection by Design and by Default of 20 October 2020. URL: https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201904_dataprotection_by_design_and_by_default_v2.0_en.pdf (дата звернення: 03.10.2023).

240. Сорока С. В. Суд Європейського Союзу як вища судова інстанція ЄС. *Мультимедійний підручник «Управління в ЄС та політика європейської інтеграції»*. URL: https://eugov.chmnu.edu.ua/ (дата звернення: 03.10.2023).

241. Комарова Т. В. Суд Європейського Союзу: розвиток судової системи та практики тлумачення права ЄС: монографія. Харків: Право, 2018. 528 с.

242. Pavelek O., Zajickova D. Personal Data Protection in the Decision-Making of the CJEU Before and After the Lisbon Treaty. *TalTech Journal of European Studies*. 2021. Vol. 11, No. 2. P. 167-188. URL: https://www.researchgate.net/publication/356254530_Personal_Data_Protection_in_the_Decision-Making_of_the_CJEU_Before_and_After_the_Lisbon_Treaty (дата звернення: 03.10.2023).

243. C-29/69, Erich Stauder v City of Ulm – Sozialamt. Judgment of the Court of 12 November 1969. ECLI:EU:C:1969:57. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A61969CJ0029 (дата звернення: 03.10.2023).

244. González Fuster G., Hijmans H. The EU rights to privacy and personal data protection: 20 years in 10 questions. Discussion paper. Brussels, 2019. URL: https://brusselsprivacyhub.eu/events/20190513.Working_Paper_Gonza%CC%81lez_Fuster_Hijmans.pdf (дата звернення: 03.10.2023).

245. Craig P., de Búrca G. EU Law: Texts, Cases and Materials (Seventh Ed.). Oxford: Oxford University Press, 2020. 1219 p.

246. Joined Cases C-92/09 and C-93/09, Volker und Markus Schecke GbR (C-92/09) and Hartmut Eifert (C-93/09) v. Land Hessen, Case C-92/09, Judgment of the Court (Grand

Chamber) of 9 November 2010. ECLI:EU:C:2010:662. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62009CA0092 (дата звернення: 03.10.2023).

247. Vogiatzoglou P., Valcke P. Two decades of Article 8 CFR: A critical exploration of the fundamental right to personal data protection. (Preprint. UK: Edward Elgar Publishing. 2022). 40 p. URL: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3978830 (дата звернення: 03.10.2023).

248. Case C-101/01, Criminal proceedings against Bodil Lindqvist, Judgment of the Court of 6 November 2003. ECLI:EU:C:2003:596. URL: http://curia.europa.eu/juris/liste.jsf?num=C-101/01 (дата звернення: 03.10.2023).

249. Case C-291/12, Michael Schwarz v. Stadt Bochum, Judgment of the Court of 17 October 2013, ECLI:EU:C:2013:670. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:62012CJ0291 (дата звернення: 03.10.2023).

250. Case C-70/10, Scarlet Extended SA v. Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM), Judgment of the Court of 24 November 2011. ECLI:EU:C:2011:771. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62010CJ0070 (дата звернення: 03.10.2023).

251. Case C-582/14, Patrick Breyer v. Bundesrepublik Deutschland, Judgment of the Court of 19 October 2016. ECLI:EU:C:2016:779. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62014CJ0582 (дата звернення: 03.10.2023).

252. Case C-434/16, Peter Nowak v. Data Protection Commissioner, Judgment of the Court of 20 December 2017. ECLI:EU:C:2017:994. URL: http://curia.europa.eu/juris/liste.jsf?language=en&num=C-434/16 (дата звернення: 03.10.2023).

253. Case C-184/20, OT v. Vyriausioji tarnybinės etikos komisija, Judgment of the Court (Grand Chamber) of 1 August 2022. ECLI:EU:C:2022:601.URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62020CJ0184 (дата звернення: 03.10.2023).

254. Court of Justice of the European Union. Protection of personal data. Fact sheet. URL: https://curia.europa.eu/jcms/upload/docs/application/pdf/2018-10/fiche_thematique_-_donnees_personnelles_-_en.pdf (дата звернення: 03.10.2023).

255. Case C-77/21, Digi Távközlési és Szolgáltató Kft. v. Nemzeti Adatvédelmi és Információszabadság Hatóság, Judgment of the Court of 20 October 2022. ECLI:EU:C:2022:805. URL: https://curia.europa.eu/juris/document/document.jsf?text=&docid=267405&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=365738 (дата звернення: 03.10.2023).

256. Case C-28/08, European Commission v. the Bavarian Lager Co. Ltd., Judgment of the Court (Grand Chamber) of 29 June 2010. ECLI:EU:C:2010:378. URL:http://curia.europa.eu/juris/liste.jsf?language=en&num=C-28/08 (дата звернення: 03.10.2023).

257. Case C-673/17, Bundesverband der Verbraucherzentralen und Verbraucherverbände – Verbraucherzentrale Bundesverband eV v. Planet49 GmbH, Judgment of the Court (Grand Chamber) of 1 October 2019. ECLI:EU:C:2019:801. URL: https://eur-lex.europa.eu/legal-content/GA/TXT/?uri=CELEX:62017CJ0673 (дата звернення: 03.10.2023).

258. Case C-61/19, Orange România SA v. Autoritatea Națională de Supraveghere a Prelucrării Datelor cu Caracter Personal (ANSPDCP), Judgment of the Court of 11 November 2020. ECLI:EU:C:2020:901. URL: https://curia.europa.eu/juris/document/document.jsf?docid=233544&doclang=EN (дата звернення: 03.10.2023).

259. Joined Cases C-465/00, C-138/01 and C-139/01, Rechnungshof (C-465/00) v. Österreichischer Rundfunk and Others and Christa Neukomm (C-138/01) and Joseph Lauermann (C-139/01) v. Österreichischer Rundfunk, Judgment of the Court of 20 May 2003. ECLI:EU:C:2003:294. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62000CJ0465 (дата звернення: 03.10.2023).

260. Joined Cases C-317/04 and C-318/04, European Parliament v. Council of the European Union and Commission of the European Communities, Judgment of the Court of 30 May 2006. ECLI:EU:C:2006:346. URL: https://curia.europa.eu/juris/liste.jsf?num=C-317/04&language=en (дата звернення: 03.10.2023).

261. Case C-73/07, Tietosuojavaltuutettu v. Satakunnan Markkinapörssi Oy and Satamedia Oy, Judgment of the Court (Grand Chamber) of 16 December 2008. ECLI:EU:C:2008:727.

URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62007CJ0073 (дата звернення: 03.10.2023).

262. Case C-212/13, František Ryneš v. Úřad pro ochranu osobních údajů, Judgment of the Court of 11 December 2014. ECLI:EU:C:2014:2428. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=ecli%3AECLI%3AEU%3AC%3A2014%3A2428 (дата звернення: 03.10.2023).

263. Case C 154/21, RW v. Österreichische Post AG, Judgment of the Court of 12 January 2023, ECLI:EU:C:2023:3. URL: https://curia.europa.eu/juris/document/document.jsf?docid=269146&doclang=en (дата звернення: 03.10.2023).

264. Dalla Corto L. On proportionality in the data protection jurisprudence of the CJEU. *International Data Privacy Law*. 2022. Vol. 12. No. 4. URL: https://doi.org/10.1093/idpl/ipac014 (дата звернення: 03.10.2023).

265. Herlin-Karnell E. EU Data Protection And The Principle Of Proportionality. *Nordic Journal Of European Law*. 2021. No. 2. P. 66-74. URL: https://journals.lub.lu.se/njel/article/download/23782/21038/58760 (дата звернення: 03.10.2023).

266. European Data Protection Board Guidelines on assessing the proportionality of measures that limit the fundamental rights to privacy and to the protection of personal data of 19 December 2019. URL: https://edps.europa.eu/sites/edp/files/publication/19-12-19_edps_proportionality_guidelines_en.pdf (дата звернення: 03.10.2023).

267. Case C 708/18, TK v. Asociaţia de Proprietari bloc M5A ScaraA, Judgment of the Court of 11 December 2019. EU:C:2019:1064. URL: https://curia.europa.eu/juris/documents.jsf?critereEcli=ECLI:EU:C:2019:1064 (дата звернення: 03.10.2023).

268. Brkan M. The Essence of the Fundamental Rights to Privacy and Data Protection: Finding the Way Through the Maze of the CJEU's Constitutional Reasoning. *German Law Journal*. 2019. No. 20. P.864-883. URL: https://doi.org/10.1017/glj.2019.66 (дата звернення: 03.10.2023).

269. Case C-283/11, Sky Österreich GmbH v. Österreichischer Rundfunk, Judgment of the Court (Grand Chamber) of 22 January 2013. ECLI:EU:C:2013:28. URL: https://curia.europa.eu/juris/liste.jsf?num=C-283/11 (дата звернення: 03.10.2023).

270. Case C-275/06, Productores de Música de España (Promusicae) v Telefónica de España SAU, Judgement of the Court of 29 January 2008. ECLI: EU:C:2008:54. URL: https://curia.europa.eu/juris/liste.jsf?language=en&num=C-275/06 (дата звернення: 03.10.2023).

271. Case C-73/16, Peter Puškár v. Finančné riaditeľstvo Slovenskej republiky and Kriminálny úrad finančnej správy, Judgment of the Court of 27 September 2017. EU:C:2017:725. URL: https://curia.europa.eu/juris/liste.jsf?language=en&num=C-73/16 (дата звернення: 03.10.2023).

272. Case C-345/17, Sergejs Buivids v. Datu valsts inspekcija, Judgment of the Court of 14 February 2019. ECLI:EU:C:2019:122. URL: https://curia.europa.eu/juris/liste.jsf?num=C-345/17 (дата звернення: 03.10.2023).

273. Case C-399/11, Stefano Melloni v Ministerio Fiscal, Judgment of the Court of 26 February 2013. ECLI:EU:C:2013:107. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62011CJ0399 (дата звернення: 03.10.2023).

274. Case C-524/06, Heinz Huber v. Bundesrepublik Deutschland, Judgment of the Court (Grand Chamber) of 16 December 2008. ECLI:EU:C:2008:724. URL: https://curia.europa.eu/juris/liste.jsf?language=en&jur=C,T,F&num=c-524/06 (дата звернення: 03.10.2023).

275. Коваленко Ю. О. До питання застосування Судом Європейського Союзу доктрини свободи розсуду та доктрини верховенства права ЄС в контексті захисту персональних даних. *Topical issues of modern jurisprudence*: *international scientific conference* (Częstochowa, Republic of Poland, 5–6 April 2023). Riga, Latvia: «Baltija Publishing», 2023. P. 224-228

276. Joined Cases C-468/10 and C-469/10, Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) (C 468/10), Federación de Comercio Electrónico y Marketing Directo (FECEMD) (C 469/10) v. Administración del Estado, Joined Cases C-468/10 and C-469/10. Judgment of the Court of 24 November 2011. ECLI:EU:C:2011:777.

URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62010CJ0468 (дата звернення: 03.10.2023).

277. Лазовські А. Верховенство права Європейського Союзу: юридична авантюра, що окупилася. *Право України*. 2019. № 6 (57). С.35-52.

278. Смирнова К., Березовська І. Розвиток доктрини прямої дії міжнародних угод у праві Європейського Союзу. *Право України*. 2019. № 6 (57). С.15-35.

279. Рекомендації для українських органів державного управління щодо наближення до права ЄС. Київ, 2018. Доступно за посиланням: https://eu-ua.kmu.gov.ua/sites/default/files/inline/files/legal_approximation_guidelines_ukr_new.pdf (дата звернення: 03.10.2023).

280. Case of Bosphorus Hava Yolları Turizm ve Ticaret Anonim Şirketi v. Ireland, application no. 45036/98, Judgment of European Court of Human Rights of 30 June 2005. URL: https://hudoc.echr.coe.int/fre?i=001-69564 (дата звернення: 03.10.2023).

281. Case C-71/14, East Sussex County Council v. Information Commissioner and Others, Judgment of the Court of 6 October 2015. ECLI:EU:C:2015:656. URL: https://curia.europa.eu/juris/liste.jsf?language=en&num=C-71/14 (дата звернення: 03.10.2023).

282. Case C-460/20, TU, RE v. Google LLC, Judgment of the Court of 8 December 2022. ECLI:EU:C:2022:962. URL: https://curia.europa.eu/juris/document/document.jsf?text=&docid=268429&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=548 (дата звернення: 03.10.2023).

283. Case C-132/21, BE v. Nemzeti Adatvédelmi és Információszabadság Hatóság, Judgment of the Court of 12 January 2023. ECLI:EU:C:2023:2. URL: https://curia.europa.eu/juris/document/document.jsf?text=&docid=269145&pageIndex=0&doclang=EN&mode=req&dir=&occ=first&part=1&cid=1209 (дата звернення: 03.10.2023).

284. Joined Cases C-511/18, C-512/18 and C-520/18, La Quadrature du Net and Others v. Premier ministre and Others, Judgement of 06 October 2020. ECLI:EU:C:2020:791. URL: https://curia.europa.eu/juris/document/document.jsf?text=&docid=232084&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=1264850 (дата звернення: 03.10.2023).

285. European Commission White Paper on Artificial Intelligence A European approach to excellence and trust of 19 February 2020. URL: https://commission.europa.eu/system/files/2020-02/commission-white-paper-artificial-intelligence-feb2020_en.pdf (дата звернення: 03.10.2023).

286. Ufert F. AI Regulation Through the Lens of Fundamental Rights: How Well Does the GDPR Address the Challenges Posed by AI? *European Papers*. 2020. Vol. 5, No. 2. P. 1087-1097. URL: https://www.europeanpapers.eu/es/system/files/pdf_version/EP_EF_2020_I_035_Fabienne_Ufert_00394.pdf (дата звернення: 03.10.2023).

287. Про захист персональних даних: Закон України від 01.06.2010 р. № 2297-VI. URL: https://zakon.rada.gov.ua/laws/show/2297-17 (дата звернення: 03.10.2023).

288. Жорж М., Саттон Г. Аналіз Закону України про захист персональних даних. Страсбург: Рада Європи, 2012. URL: http://za.inf.ua/bo/jorj_PDanaiz.pdf (дата звернення: 03.10.2023).

289. Про інформацію: Закон України від 02.10.1992 р. № 2657-XII. URL: https://zakon.rada.gov.ua/laws/show/2657-12 (дата звернення: 03.10.2023).

290. Про доступ до публічної інформації: Закон України від 13.01.2011 р. № 2939-VI. URL: https://zakon.rada.gov.ua/laws/show/2939-17 (дата звернення: 03.10.2023).

291. Про доступ до судових рішень: Закон України від 22.12.2005 р. № 3262-IV. URL: https://zakon.rada.gov.ua/laws/show/3262-15#Text (дата звернення: 03.10.2023).

292. Про збір та облік єдиного внеску на загальнообов'язкове державне соціальне страхування: Закон України від 08.07.2010 р. № 2464-VI. URL: https://zakon.rada.gov.ua/laws/show/2464-17#Text (дата звернення: 03.10.2023).

293. Камінська Н. В. Захист персональних даних: проблеми внутрішньодержавного, наднаціонального і міжнародно-правового регулювання. *Науковий вісник Національної академії внутрішніх справ*. 2015. № 3. С.106 - 114.

294. Венгер В., Кошман А., Шевчук О. Аналіз судової практики щодо застосування законодавства України про захист персональних даних. Київ, 2021. URL: https://rm.coe.int/report-dp-2021-2web-/1680aa5225 (дата звернення: 03.10.2023).

295. Концевой Р. С. До питання визначення поняття «персональні дані». *Інформація і право*. 2012. № 2. С. 23-28. URL: http://nbuv.gov.ua/UJRN/Infpr_2012_2_6 (дата звернення: 03.10.2023).

296. Погорілко В.Ф. Інформація про особу. *Юридична енциклопедія*: у 6 т. / ред.кол.: Ю. С. Шемшученко та ін.; Ін-т держави і права ім. В. М. Корецького НАН України. Київ: Українська енциклопедія, 2002. Т. 2: Н-П. 744 с.

297. 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.

298. Романюк І. І. Охорона права на персональні дані в Україні (цивільно-правовий аспект). дис. … канд. юрид. наук : 12.00.03 / Київ. нац. ун-т ім. Т. Шевченка. Київ, 2015. 267 с.

299. Серебряник О. О. Інформація про особу як об'єкт цивільних прав : дис. ... канд. юрид. наук: 12.00.03 / Ів.-Франк. ун-т права ім. Короля Д. Галицького. Івано-Франківськ, 2016. 209 с.

300. Тунік А. В. Правові основи захисту персональних даних : автореф. дис. … канд. юр. наук: 12.00.07 / Нац. авіац. ун-т. Київ, 2012. 25 с.

301. Буртник Х. Конфіденційна інформація, інформація про особу та персональні дані: співвідношення і регулювання. *Центр демократії та прав людини.* URL: https://cedem.org.ua/analytics/konfidentsijna-informatsiya-informatsiya-pro-osobu-ta-personalni-dani-spivvidnoshennya-i-regulyuvannya/ (дата звернення: 03.10.2023).

302. 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 № 2-рп/2012 від 20.01.2012. URL: https://zakon.rada.gov.ua/laws/show/v002p710-12#Text (дата звернення: 03.10.2023).

303. Стефанчук Р. О. Персоніфікована інформація. *Юридична енциклопедія*: у 6 т. / ред. кол.: Ю. С. Шемшученко та ін.; Ін-т держави і права ім. В. М. Корецького НАН України. Київ: Українська енциклопедія, 2002. Т. 4: Н-П. С. 507.

304. Обуховська Т. І. Державні механізми забезпечення захисту персональних даних в Україні: дис. … канд. наук з держ. управл.: 25.00.02 / Нац. акад. держ. управл. при Президентові України. Київ, 2016. 229 с.

305. Радкевич О. П. Зміст поняття персональна інформація і її різновиди. *Інформаційна безпека людини, суспільства, держави*. 2012. № 3 (10). С. 39–43.

306. Брижко В. М. Модальність правової визначеності у сфері захисту та безпеки приватності персональних даних. *Інформація і право*. 2021. № 4(39). С. 52-69.

307. Бем М. В., Городиський І. М. Захист персональних даних: правове регулювання та практичні аспекти: наук.-практ. посіб. 2021. 160 с. URL: https://rm.coe.int/handbook-pers-data-protect-2021-web/1680a37a69 (дата звернення: 03.10.2023).

308. Постанова Великої Палати Верховного Суду у справі № 806/3265/17 від 19.09.2018 р. URL: https://reyestr.court.gov.ua/Review/76822787 (дата звернення: 03.10.2023).

309. Городиський І. М. Сучасний стан виконання Україною міжнародних зобов'язань із захисту персональних даних. *Інтеграція України в Європейське інформаційне суспільство: виклики та завдання*: монографія / за заг. ред. А. В. Пазюк. Київ: ФОП Клименко, 2014. 212 с. URL: https://rm.coe.int/1680599369 (дата звернення: 03.10.2023).

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

311. Аналіз законопроекту 5628. *Українська Гельсінська спілка з прав людини*. URL: https://www.helsinki.org.ua/wp-content/uploads/2021/09/Analiz-zakonoproiektu-5628_A5.pdf (дата звернення: 03.10.2023).

312. Щорічна доповідь Уповноваженого ВРУ з прав людини про стан додержання та захисту прав людини в Україні у 2022 році. URL: https://ombudsman.gov.ua/report-2022/informatsiini-prava#zakhyst-personalnykh-danykh (дата звернення: 03.10.2023).

313. Венгер В., Заярний О. Правовий аналіз основних моделей інституалізації державного контролю у сфері персональних даних та доступу до публічної інформації в Україні. Київ, 2020. 30 с. URL: https://rm.coe.int/legal-analysis-data-ua/16809ee077 (дата звернення: 03.10.2023).

314. Про Національну комісію з питань захисту персональних даних та доступу до публічної інформації: Проєкт Закону України від 18.10.2021 р. № 6177. URL: http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=72992 (дата звернення: 03.10.2023).

315. Аналіз проєкту Закону України «Про Національну комісію з питань захисту персональних даних та доступу до публічної інформації» № 6177. *Українська Гельсінська спілка з прав людини*. URL: https://www.helsinki.org.ua/articles/analiz-proiektu-zakonu-ukrainy-pro-natsionalnu-komisiiu-z-pytan-zakhystu-personalnykh-danykh-ta-dostupu-do-publichnoi-informatsii-6177/ (дата звернення: 03.10.2023).

316. Коваленко Ю. Геномна інформація людини (ДНК): облік в умовах воєнного стану та ризики під час обробки. *Закон і Бізнес*. 2022. URL: https://zib.com.ua/ua/153699.html (дата звернення: 03.10.2023).

317. Про державну реєстрацію геномної інформації людини: Закон України від 09.07.2022 № 2391-IX. URL: https://zakon.rada.gov.ua/laws/show/2391-20#Text (дата звернення: 03.10.2023).

318. Євроатлантичний вектор України: національна доповідь / ред. кол. С. І. Пирожков, І. О. Кресіна, А. І. Кудряченко, Ю. С. Шемшученко та ін.; Ін-т держави і права ім. В. М. Корецького, Нац. акад. наук України. Київ: Національна академія наук України, 2019. 328 с.

319. Про Річну національну програму під егідою Комісії Україна — НАТО на 2021 рік: Указ Президента України від 11 травня 2021 року №189/2021. URL: https://www.president.gov.ua/documents/1892021-38845 (дата звернення: 03.10.2023).

320. Савчук К. О., Проценко І. М. Особливості правового регулювання членства в Організації Північноатлантичного договору. *Часопис Київського університету права*. 2019. № 3. С. 258-265.

321. Переверзєва О. С. Захист персональних даних в Інтернеті в державах Європейського Союзу. *Юридичний науковий електронний журнал*. 2023. № 5. С. 529-531.

322. Войцеховський А. В. Кібербезпека як напрям євроатлантичної інтеграції України. *Право і безпека у контексті європейської та євроатлантичної інтеграції*: зб.

ст. та тез наук. повідомл. за матеріалами дискус. панелі II Харків. міжнар. юрид. форуму (м. Харків, 28 верес. 2018 р.) / ред. кол: Ю.Г. Барабаш, Т.М. Анакіна, Д.В. Аббакумова. Харків: Право, 2018. С. 42-48.

323. Коваленко Ю. О. Виконання Україною міжнародно-правових зобов'язань у сфері захисту персональних даних в контексті євроатлантичної інтеграції. *Science and Technology: LVII International Scientific and Practical Conference* (Great Britain, Birmingham, 14 - 15 September 2023). Birmingham, Great Britain: «Nika Publishing», 2023. P. 19-24.

324. Концепція розвитку штучного інтелекту в Україні, схвалена Розпорядженням Кабінету Міністрів України від 02 грудня 2020 р. № 1556-р. URL: https://zakon.rada.gov.ua/laws/show/1556-2020-%D1%80#Text (дата звернення: 03.10.2023).

325. Про виконання рішень та застосування практики Європейського суду з прав людини: Закон України від 23.02.2006 р. № 3477-IV. URL: https://zakon.rada.gov.ua/laws/show/3477-15#Text (дата звернення: 03.10.2023).

326. Case of Scozzari and Giunta v. Italy, application nos. 39221/98 and 41963/98, Judgment of European Court of Human Rights (Grand Chamber) of 13 July 2000. URL: https://hudoc.echr.coe.int/eng?i=001-58752 (дата звернення: 03.10.2023).

327. Mushak N., Muraviov V. Legal Issues of the Implementation of the Convention for the Protection of Human Rights and Fundamental Freedoms 1950 in Ukraine. *Access to Justice in Eastern Europe*. 2021. Vol. 4. No. 1. P. 8-22.

328. Оніщенко Н. М. Контроль за забезпеченням прав людини: дихотомія впливу. *Правова держава*. 2019. № 30. С. 24–29.

329. Мазур О., Грицаєнко Л. Виконання рішень Європейського суду з прав людини: виклики для України в контексті зарубіжного досвіду. *Науковий часопис Національної академії прокуратури України*. 2019. № 1 (21). С. 32–41.

330. Committee of Ministers of Council of Europe 1377th meeting (June 2020) (DH) - Action plan (22/05/2020) - Communication from Ukraine concerning the case of Zaichenko v. Ukraine (no. 2) (Application No. 45797/09). URL: https://hudoc.exec.coe.int/eng?i=DH-DD(2020)458E (дата звернення: 03.10.2023).

331. Case of Berlizev v. Ukraine, application no. 43571/12, Judgment of European Court of Human Rights of 13 July 2000. URL: https://hudoc.echr.coe.int/eng?i=001-210850 (дата звернення: 03.10.2023).

332. Case of Lysyuk v. Ukraine, application no. 72531/13, Judgment of European Court of Human Rights of 14 October 2021. URL: https://hudoc.echr.coe.int/eng?i=001-212137 (дата звернення: 03.10.2023).

333. Case of Sedletska v. Ukraine, application no. 42634/18, Judgment of European Court of Human Rights of 1 April 2021. URL: https://hudoc.echr.coe.int/eng?i=001-208882 (дата звернення: 03.10.2023).

334. Угода про партнерство та співробітництво між Україною і Європейськими Співтовариствами та їх державами-членами, ратифікована Законом України від 14.06.1994 р. № 237/94-ВР. URL: https://zakon.rada.gov.ua/laws/show/998_012#Text (дата звернення: 03.10.2023).

335. Стратегія інтеграції України до Європейського Союзу 1998 р. URL: https://zakon.rada.gov.ua/laws/show/615/98#Text (дата звернення: 03.10.2023).

336. Яковюк І. В. Правові основи європейської інтеграції та її вплив на державно-правовий розвиток України: дис. … д-ра юрид. наук: 12.00.01 / Нац. юр. ун-т ім. Я. Мудрого. Харків, 2013. 474 с.

337. Фалалєєва Л. Г. Роль Копенгагенських критеріїв у реалізації цінностей Європейського Союзу. *Наукові записки Інституту законодавства Верховної Ради України.* 2017. № 1. С. 114-122.

338. Мушак Н. Acquis у правовій системі Європейського Союзу. *Вісник Київського національного університету ім.Тараса Шевченка*. 2016. № 1. С. 101-105.

339. Угода про асоціацію між Україною, з однієї сторони, та Європейським Союзом, Європейським співтовариством з атомної енергії і їхніми державами-членами, з іншої сторони, ратифікована Законом України від 27.06.2014 р. № 1678-VII. URL: https://zakon.rada.gov.ua/laws/show/984_011 (дата звернення: 03.10.2023).

340. Угода про співробітництво між Україною та Європейською організацією з питань юстиції, ратифікована Законом від 08.02.2017 р. № 1839-VIII. URL: https://zakon.rada.gov.ua/laws/show/984_024-16#Text (дата звернення: 03.10.2023).

341. Моніторинг реалізації плану заходів з виконання Угоди. Удосконалення законодавства про захист персональних даних з метою приведення його у відповідність з Регламентом (ЄС) 2016/679. Пульс Угоди. URL: https://pulse.kmu.gov.ua/ua/streams/human-rights-justice-and-anticorupption/2020-substream5-95 (дата звернення: 03.10.2023).

342. Проєкт закону №8153 від 25.10.2022 щодо внесення змін до Закону України «Про захист персональних даних». URL: https://itd.rada.gov.ua/billInfo/Bills/pubFile/1517426 (дата звернення: 03.10.2023).

343. Комітет з питань інтеграції України до Європейського Союзу. Висновок щодо проєкту закону про захист персональних даних. URL: https://itd.rada.gov.ua/billInfo/Bills/pubFile/1562145 (дата звернення: 03.10.2023).

344. Правовий висновок Ради Європи щодо проєкту Закону №8153. URL: https://rm.coe.int/opinion-on-the-draft-law-on-personal-data-protection-final-ukr/1680ab9e07 (дата звернення: 03.10.2023).

345. Рішення Конституційного Суду України у справі за конституційним поданням 70 народних депутатів України щодо відповідності Конституції України (конституційності) положень частини першої статті 10, пункту 3 частини другої, частин п’ятої, шостої статті 11, статті 15, частини першої статті 17, статті 24, пункту 3 розділу VI «Заключні положення» Закону України «Про політичні партії в Україні» (справа про утворення політичних партій в Україні) від 12 червня 2007 № 2-рп/2007. URL: https://zakon.rada.gov.ua/laws/show/v002p710-07#Text (дата звернення: 03.10.2023).

346. Petrov R. The Impact of the Court of Justice of the European Union on the legal system of Ukraine. *Право України.* 2019. № 6. С. 53-68. URL: https://ekmair.ukma.edu.ua/items/d7ad7bc8-100c-4560-ab40-94ee0c2a0607 (дата звернення: 03.10.2023).

ДОДАТОК А

СПИСОК ПУБЛІКАЦІЙ ЗДОБУВАЧА ЗА ТЕМОЮ ДИСЕРТАЦІЇ, В ЯКИХ ОПУБЛІКОВАНІ ОСНОВНІ НАУКОВІ РЕЗУЛЬТАТИ

Список публікацій, в яких опубліковані основні наукові результати дисертації:

1. Коваленко Ю. О. Становлення та розвиток європейських стандартів захисту персональних даних. *Наукові записки Інституту законодавства Верховної Ради України*. 2020. № 5. С. 59-67.
2. Kovalenko Y. The Right to Privacy and Protection of Personal Data: Emerging Trends and the Implications for Development in the Jurisprudence of the European Court of Human Rights. *Masaryk University Journal of Law and Technology*. 2022. Vol. 16. No. 1. P. 37-57 (*Scopus*).
3. Kovalenko Y. Balancing right to personal data protection towards other fundamental rights through the prism of the case law of the ECtHR and the CJEU. *Visegrad Journal on Human Rights*. 2022. No. 2. P. 52-57.

Наукові публікації, які засвідчують апробацію матеріалів дисертації:

4. Коваленко Ю. О. До питання становлення права на захист персональних даних у міжнародному праві. *Актуальні дослідження правової та історичної науки (випуск 24)*: матеріали міжн. наук.-практ. конф. (м. Тернопіль, 21 лип. 2020 р.). Тернопіль, 2020. С. 30-33.
5. Коваленко Ю. О. Еволюція європейських стандартів захисту персональних даних. *Актуальні проблеми законодавства України: пріоритетні напрями його вдосконалення*: матеріали міжн. наук.-практ. конф. (м. Одеса, 9-10 жовт. 2020 р.). Одеса, 2020. С. 13-16.
6. Kovalenko Y. O. Right to data protection in the times of COVID-19: challenges and prospects in the ECtHR. *Сучасне правотворення: питання теорії та практики*: матеріали міжн. наук.-практ. конф. (м. Дніпро, 4-5 черв. 2021 р.). Дніпро: ГО «Правовий світ», 2021. С. 145-149.

7. Kovalenko Y. The place of the right to data protection in the existent human rights framework. *Права людини як індикатор розвитку сучасної держави*: матеріали міжн. наук.-практ. конф. (м. Київ, 13 груд. 2021 р.). Київ: «Видавництво Людмила», 2021. С. 16-18.

8. Коваленко Ю. Геномна інформація людини (ДНК): облік в умовах воєнного стану та ризики під час обробки. *Закон і Бізнес*. 2022. URL: https://zib.com.ua/ua/153699.html (дата звернення: 03.10.2023).

9. Коваленко Ю. О. До питання застосування Судом Європейського Союзу доктрини свободи розсуду та доктрини верховенства права ЄС в контексті захисту персональних даних. *Topical issues of modern jurisprudence*: *international scientific conference* (Częstochowa, Republic of Poland, 5–6 April 2023). Riga, Latvia: «Baltija Publishing», 2023. P. 224-228.

10. Коваленко Ю. О. Виконання Україною міжнародно-правових зобов'язань у сфері захисту персональних даних в контексті євроатлантичної інтеграції. *Science and Technology: LVII International Scientific and Practical Conference* (Great Britain, Birmingham, 14 - 15 September 2023). Birmingham, Great Britain: «Nika Publishing», 2023. P. 19-24.