**Київський національний університет імені Тараса Шевченка**
**Міністерство освіти і науки України**

**Київський національний університет імені Тараса Шевченка**
**Міністерство освіти і науки України**

Кваліфікаційна наукова праця на правах рукопису

**МАРТИНОВА АННА МИКОЛАЇВНА**

УДК 339.1:342.721:681.302

# ДИСЕРТАЦІЯ
# АДМІНІСТРАТИВНО-ПРАВОВЕ ЗАБЕЗПЕЧЕННЯ ОБІГУ ТА ЗАХИСТУ БІОМЕТРИЧНИХ ПЕРСОНАЛЬНИХ ДАНИХ

Спеціальність - 081 – Право; Галузь знань – 08 Право

Подається на здобуття наукового ступеня доктора філософії

Дисертація містить результати власних досліджень. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело
_____ **А. М. Мартинова**

Науковий керівник **– ЗАЯРНИЙ Олег Анатолійович**, доктор юридичних наук, доцент, професор кафедри інтелектуальної власності та інформаційного права навчально-наукового інституту права Київського національного університету імені Тараса Шевченка



Київ – 2022

# АНОТАЦІЯ

*Мартинова А. М* Адміністративно-правове забезпечення обігу та захисту біометричних персональних даних. – Кваліфікаційна наукова праця на правах рукопису.

Дисертація на здобуття наукового ступеня доктора філософії за (081-Право). – Навчально-науковий інститут права Київського національного університету імені Тараса Шевченка, Київ, 2022.

У дисертації проведене дослідження особливостей адміністративноправового забезпечення захисту та обігу біометричних персональних даних в Україні, чинників, які впливають на його формування, виявленно складові реалізації адміністративного-правового забезпечення захисту та обігу біометричних персональних даних в Україні, повноваження органів, установ та організацій, що реалізують адміністративно-правове забезпечення захисту та обігу біометричних персональних даних в Україні та зарубіжних країнах, та на основі зарубіжного досвіду - розробці науково обґрунтованих рекомендацій щодо вдосконалення адміністративного-правового забезпечення захисту та обігу біометричних персональних даних та розробки організаційно-правових форм його практичного втілення в Україні.

У контексті дослідження понятійно-категоріального апарату визначено наступні поняття: «персональні дані», «біометричні персональні дані», «право на захист біометричних персональних даних», «правовий статус», «захист персональних даних», «біометричні дані», «генетичні дані» тощо.

У дисертаційній роботі визначено межі, підстави та процедури правомірної обробки та обігу персональних даних за законодавством України і Європейського Союзу. Досліджено зміст права на захист біометричних персональних даних, як складової адміністративно-правового статусу фізичної особи. Надано характеристику нормативним засадам формування і реалізації відповідного правового механізму в Україні та зарубіжних країнах. Наведено

особливості правовідносин у сфері адміністративно-правового забезпечення обігу та захисту біометричних персональних даних та досліджено інструменти адміністративно-правового забезпечення правомірного обігу та захисту біометричних персональних даних.

У дисертації розкрито, що сучасний стан дослідження використання, обігу та захисту біометричних персональних даних став передумовою розвитку у науці таких явищ як «інтернет речей» та «хмарні технології», та наголошено на потребі нормативного врегулювання технічного захисту біометричних персональних даних при проектуванні, використанні та знищенні Інтернету речей, необхідності розробки порядку обробки та технічного захисту біометричних персональних даних власників та споживачів інтернету речей.

Досліджено, що суспільні відносини, що стосуються права захисту біометричних персональних даних, хоч і є в основному інформаційними, але мають у своїй структурі ще конституційні правовідносини та адміністративно-правові, адже до адміністративно-правових відносин саме і належить правовий статус фізичної особи – суб`єкта біометричних персональних даних. Зазначено, що у національному законодавстві право на захист біометричних персональних даних є структурним елементом конституційного права на недоторканість особистого життя, яке означає виключення можливості здійснення будь-яких операцій чи дій з біометричними персональними даними за відсутності згоди субєкта відповідних даних.

Дисертаційна робота містить характеристику адміністративно-правового забезпечення правомірного обігу та захисту права на конфіденційність біометричних персональних даних Уповноваженим Верховної Ради України з прав людини (процедура, засоби та умови реалізації).

У праці визначено захист права на конфіденційність біометричних персональних даних адміністративними судами України та захист біометричних даних в практиці Європейського Суду з прав людини та основні напрями її імплементації у правозастосовчу діяльність органів судової влади України.

У роботі було запропоновано визначення понять «біометричні персональні дані» та «право на захист біометричних персональних даних», класифікацію біометричних персональних даних, а також пропозиції до покращення захисту та обігу біометричних персональних даних шляхом внесення змін до чинного законодавства України у відповідній сфері.

У дисертації визначено пропозиції внесення змін до законодавства, проаналізовано законопроект, зареєстрований у Верховній Раді України та зпропоновано удосконалення чинного законодавства у сфері адміністративно-правового забезпечення захисту та обігу біометричних персональних даних в Україні на основі зарубіжного досвіду.

***Ключові слова:*** «адміністративно-правове забезпечення», «база даних», «біометричні дані», «біометричні параметри», «біометрична ідентифікація», «володілець біометричних даних», «генетичні дані», «захист біометричних даних», «конфіденційна інформація про фізичну особу, «мета обробки біометричних даних», «персональні дані», «підстави обробки біометричних даних», право на захист біометричних персональних даних, «реєстр біометричних даних», «суб'єкт персональних даних».

# СПИСОК ПУБЛІКАЦІЙ ЗДОБУВАЧА ЗА ТЕМОЮ ДИСЕРТАЦІЇ

Наукові праці, в яких опубліковані основні наукові результати дисертації:

1. Бойко А. М. Право на забуття: деякі аспекти теорії і практики. *Журнал східноєвропейського права.* 2018. №48. С. 124-131. DOI: ISSN 2409-6415

2. Бойко А. М. Законодавство Європейського Союзу у сфері захисту персональних даних. *Юридичний електронний журнал: електрон. наук. фахове вид.* 2019. № 4. С.96-99. DOI: //doi.org/10.32782/2524-0374/2019-4/24

3. Бойко А. М. Межі правомірного обігу біометричних персональних даних за законодавством України. *Науковий юридичний журнал «Правові новели».* 2020. №10. С. 142-146. DOI: //doi.org/10.32847/ln.2020.10.20

4. Бойко А. М. Захист біометричних персональних даних Уповноваженим Верховної Ради України з прав людини. *Юридичний електронний журнал: електрон. наук. фахове вид.* 2021. № 2. С. 160-163. DOI: //doi.org/10.32782/2524-0374/2021-2/37

5. Бойко А. М. Міжнародне законодавство та принципи у сфері захисту біометричних персональних даних. *Науково-теоретичний журнал "Evropský politický a právní diskurz": міжнародне наук.* Фахове вид. 2021. С. 52-56.

6. Бойко А. М. Правовий режим захисту біометричних персональних даних California consumer privacy act. *Юридичний електронний журнал: електрон. наук. фахове вид.* № 10/2021. С. 369-371. DOI: //doi.org/10.32782/2524-0374/2021-10/94

7. Boyko A. M. General features of biometric personal data processing. *Visegrad Journal on Human Rights.* № 41/2021. С. 41-43.

Наукові праці, які засвідчують апробацію матеріалів дисертації:

8. Бойко А. М. Право на забуття як гарантія невтручання в особисте сімейне життя людини. *Актуальні питання державотворення в Україні. Матеріали Міжнародної науково-практичної конференції студентів, аспірантів та молодих вчених від 19 травня 2017 року.* Том-1. С. 257-258.

9. Бойко А. М. Окремі аспекти правового регулювання обробки персональних даних у соціальних мережах. *Актуальні питання розвитку юридичної науки та практики. Матеріали міжнародної науково-практичної конференції від 18 травня 2018 року.* Том 1. С. 304-305.

10. Бойко А. М. Адміністративно-правове забезпечення захисту біометричних персональних даних Уповноваженим Верховної Ради України з прав людини. *Актуальні проблеми захисту інформаційних прав особи в умовах технологічних викликів та цифрової реальності. Матеріали науково-практичної конференції від 17-18 вересня 2019 року*. С. 72-75.

## SUMMARY

*Martynova A. M.* Administrative and legal support for the circulation and protection of biometric personal data. - Qualified scientific work on the rights of the manuscript.

Thesis for a Doctor of Philosophy Degree in Specialty 12.00.04 “Administrative Law and Process; finance law; information law ”(081-Law). - Institute of Law, Taras Shevchenko National University of Kyiv, Kyiv, 2022.

The dissertation identifies the features of administrative and legal support for the protection and circulation of biometric personal data in Ukraine, factors influencing its formation, identifying components of the implementation of administrative and legal support for the protection and circulation of biometric personal data in Ukraine, powers of bodies, institutions and organizations administrative and legal support for the protection and circulation of biometric personal data in Ukraine and foreign countries, and on the basis of foreign experience - development of scientifically sound recommendations for improving administrative and legal support for protection and circulation of biometric personal data and development of organizational and legal forms of its implementation in Ukraine.

In the context of the study of the conceptual and categorical apparatus, the following concepts are defined: "personal data", "biometric personal data", "right to protection of biometric personal data", "legal status", "protection of personal data", "biometric data", "genetic data" »Etc.

The dissertation defines the limits and methods of lawful circulation of personal data under the laws of Ukraine and the European Union. The content of the right to protection of biometric personal data as a component of the administrative and legal status of an individual is studied. The characteristic of normative bases of administrative and legal maintenance of circulation and protection of biometric personal data according to the legislation of Ukraine and the European Union is given. Peculiarities of legal relations in the field of administrative and legal support of circulation and protection of biometric personal data are given and the tools of

administrative and legal support of lawful circulation and protection of biometric personal data are investigated.

The dissertation reveals that the current state of research on the use, circulation and protection of biometric personal data has become a prerequisite for the development in science of phenomena such as "Internet of Things" and "cloud technology", and emphasizes the need for regulation of technical protection of biometric personal data destruction of the Internet of Things, the need to develop a procedure for processing and technical protection of biometric personal data of owners and consumers of the Internet of Things.

It is investigated that public relations concerning the right to protection of biometric personal data, although mostly informational, but have in their structure still constitutional and administrative relations, because administrative-legal relations include the legal status of an individual - sub` the object of biometric personal data. It is noted that in national law the right to protection of biometric personal data is a structural element of the constitutional right to privacy, which means the exclusion of any transactions or actions with biometric personal data without the consent of the data subject.

The dissertation contains the characteristics of administrative and legal support of lawful circulation and protection of the right to confidentiality of biometric personal data by the Commissioner of the Verkhovna Rada of Ukraine for Human Rights (procedure, means and conditions of implementation).

The paper identifies the protection of the right to confidentiality of biometric personal data by administrative courts of Ukraine and the protection of biometric data in the case law of the European Court of Human Rights and the main directions of its implementation in law enforcement activities of the judiciary of Ukraine.

The paper proposes the definition of "biometric personal data" and "the right to protection of biometric personal data", classification of biometric personal data, as well as proposals to improve the protection and circulation of biometric personal data by amending current legislation in Ukraine.

The dissertation identifies proposals for amendments to the legislation, analyzes the bill registered in the Verkhovna Rada of Ukraine and proposes to improve the current legislation in the field of administrative and legal protection and circulation of biometric personal data in Ukraine based on foreign experience.

***Key words:*** biometric data, genetic data, biometric personal data, personal data, database, biometric personal data base, right to protection of biometric personal data, Internet of Things, database, cloud database, personal data protection, personal biometric subject data.

**LIST OF BUILDERS PUBLICATIONS ON THE THERMAL DIRECTORY**

In which the main scientific results of the dissertation are published:


1. Boyko A. M. The right to forget: some aspects of theory and practice. *Journal of Eastern European Law.* 2018. - №48. - P. 124-131.

2. *Boyko A. M.* European Union legislation in the field of personal data protection. *Legal electronic journal: electronic. Science. specialties type.* 2019. № 4. P.96-99. DOI: //doi.org/10.32782/2524-0374/2019-4/24

3. *Boyko A. M.* Limits of lawful circulation of biometric personal data under the legislation of Ukraine. *Scientific legal journal "Legal short stories".* 2020. №10. Pp. 142-146. DOI: //doi.org/10.32847/ln.2020.10.20

4. *Boyko A. M.* Protection of biometric personal data by the Commissioner of the Verkhovna Rada of Ukraine for Human Rights. *Legal electronic journal: electronic. Science. specialties type.* 2021. № 2. P. 160-163. DOI: //doi.org/10.32782/2524-0374/2021-2/37

5. *Boyko A. M.* International legislation and principles in the field of biometric personal data protection. *Scientific and theoretical journal "European political and legal discourse": international science. Specialties type.* 2021. P. 52-56.

6. *Boyko A. M.* Legal regime for the protection of biometric personal data CALIFORNIA CONSUMER PRIVACY ACT. *Legal electronic journal: electronic. Science. specialties type.* № 10/2021. P. 369-371. DOI: //doi.org/10.32782/2524-0374/2021-10/94

7. *Boyko A. M.* GENERAL FEATURES OF BIOMETRIC PERSONAL DATA PROCESSING. *Visegrad Journal on Human Rights.* № 41/2021. P. 41-43.

Which certify the approbation of the dissertation materials:

8. *Boyko A. M.* The right to be forgotten as a guarantee of non-interference in a person's personal family life. *Current issues of state formation in Ukraine. Proceedings of the International scientific-practical conference of students, graduate students and young scientists from May 19, 2017.* Volume 1. Pp. 257-258.

9. *Boyko A. M.* Some aspects of legal regulation of personal data processing in social networks. *Current issues of legal science and practice. Proceedings of the international scientific-practical conference of May 18, 2018. Volume 1.* pp. 304-305.

10. *Boyko A. M.* Administrative and legal support for the protection of biometric personal data by the Verkhovna Rada of Ukraine Commissioner for Human Rights. *Current issues of protection of personal information rights in the context of technological challenges and digital reality. Proceedings of the scientific-practical conference from September 17-18, 2019.* Pp. 72-75.

**ЗМІСТ**

# ВСТУП

*Актуальність теми.* У контексті інформатизації життєдіяльності суспільства та стрімкого розвитку інформаційних технологій постає необхідність адміністративно-правового забезпечення обігу і захисту біометричних персональних даних, а особливо наявність потреби ефективного правового регулювання вищезазначеного питання, що складає актуальність теми дисертаційної роботи.

В сучасних умовах розвитку різних сфер суспільного життя збільшується рівень використання біометричних персональних даних, та їх обіг, а разом із тим – наявний ризик порушення прав особи у контексті використання та обігу біометричних персональних даних, так як відсутнє в Україні належне нормативно-правове регулювання обігу та захисту біометричних даних особи.

У сфері використання персональних даних, зокрема біометричних даних, виникає значна кількість правопорушень та судових спорів, що пояснюється недостатньо ефективним правовим регулюванням захисту біометричних персональних даних, увагою з боку відповідних суб'єктів правовідносин до питання адміністративно-правового захисту біометричних персональних даних.

Крім того, під час активного розвитку сучасних державних ресурсів, що дають можливість користуватись адміністративними послугами через електронні гаджети, зокрема розвитку «Держави у смартфоні», посилюються ризики витоку персональних даних через необізнаність громадян у правилах безпечного висвітлення власних персональних даних.

Юридичне визначення біометричних даних з точки зору захисту даних визначає умови, за яких персональні дані можуть кваліфікуватися як «біометричні дані», а не умови, за яких «біометричні дані» стають персональними даними. Поняття біометричних даних визначається як вид персональних даних. Визначення поєднує технічні критерії біометричних даних (наприклад, технічну обробку біометричних характеристик) із

правовими критеріями, застосовними до персональних даних (наприклад, функцію «унікальної ідентифікації»). Однак цьому визначенню бракує точності, коли воно стосується функцій «біометричного розпізнавання».

Термінологія, яка використовується біометричною спільнотою для опису цих функцій, тобто біометрична ідентифікація та перевірка особи, не використовується повторно в юридичному визначенні біометричних даних. Натомість слід зробити висновок, що дієслова «дозволити» та «підтвердити» відповідно стосуються функцій «біометричної ідентифікації» та «підтвердження особи».

Що стосується критерію «унікальної ідентифікації», то він встановлює поріг ідентифікації, застосовний до біометричних даних. На відміну від «загальних» персональних даних, біометричні дані мають стосуватися ідентифікованої особи. Інші «біометричні дані», тобто ті, які стосуються особи, яку можна ідентифікувати, юридично не кваліфікуються як біометричні дані, але все одно можуть вважатися персональними даними, якщо вони відповідають іншим критеріям, застосовним до персональних даних. Нова система захисту даних створює нову юридичну категорію біометричних даних, які можна кваліфікувати як «біометричні персональні дані», щоб відобразити їх характер як персональних даних.

Вищезазначена проблема і є передумовою необхідності дослідження даного питання, є фактом актуальності відповідної теми, актуальності особливостей як адміністративно-правового захисту біометричних персональних даних, так загалом законодавчого закріплення врегулювання відносин між суб'єктами правовідносин у сфері використання, обігу чи захисту біометричних персональних даних в Україні.

*Зв'язок роботи з науковими програмами, планами.* Дисертаційне дослідження виконано на кафедрі інтелектуальної власності та інформаційного права Навчально-наукового інституту права Київського національного університету імені Тараса Шевченка.

Дисертаційне дослідження виконано відповідно до: Пріоритетних тематичних напрямів наукових досліджень і науково технічних розробок на період до 2020 року, затверджених постановою Кабінету Міністрів України від 07 вересня 2011 року № 942; Пріоритетних напрямів розвитку правової науки на 2016–2020 роки, затверджених постановою Загальних Зборів Національної академії правових наук України від 03 березня 2016 року; Національної стратегії у сфері прав людини, затвердженої Указом Президента України від 25 серпня 2015 року № 501/2015; Плану дій з реалізації Національної стратегії у сфері прав людини на період до 2020 року, затвердженого розпорядженням Кабінету Міністрів України від 23 листопада 2015 року № 1393-р, оновленого Плану дій з реалізації Національної стратегії у сфері прав людини на період до 2023 року, а також відповідно до науково-дослідної теми «Розробка системного вчення про основні права людини з метою втілення в Україні європейських правових цінностей у контексті розбудови громадянського суспільства» № 19 БФ 042-01, яка досліджується в Інституті права Київського національного університету імені Тараса Шевченка з 1 січня 2019 року по 31 грудня 2021 року.Тему дисертаційного дослідження було затверджено рішенням Вченої ради юридичного факультету Київського національного університету імені Тараса Шевченка, протокол № 4 від 29 листопада 2017 року.

*Мета і завдання дослідження.* Мета дисертаційного дослідження полягає у розробці теоретичних засад адміністративно-правового забезпечення правомірної обробки і захисту біометричних персональних даних в Україні на основі кращих стандартів Держав-членів Європейського Союзу та Ради Європи, формулювання на цій основі пропозицій з удосконалення законодавства України з відповідних питань.

Досягнення визначеної мети зумовило необхідність вирішення таких *завдань:*

– розкрити змістпоняття та види біометричних персональних даних, розкрити їхні юридичні властивості;

– визначитимежі та способи правомірного обігу персональних даних за законодавством України і Європейського Союзу;

– охарактеризувати право на захист біометричних персональних даних, як складова адміністративно-правового статусу фізичної особи;

– дослідити нормативні засади адміністративно-правового забезпечення обігу та захисту біометричних персональних даних за законодавством України та Європейського Союзу;

– виявитиособливості правовідносин у сфері адміністративно-правового забезпечення обігу та захисту біометричних персональних даних;

– дослідити інструменти адміністративно-правового забезпечення правомірного обігу та захисту біометричних персональних даних;

– проаналізувати адміністративно-правове забезпечення правомірного обігу та захисту права на конфіденційність біометричних персональних даних Уповноваженим Верховної Ради України з прав людини: процедури, засоби та умови реалізації;

– розкрити змістзахист права на конфіденційність біометричних персональних даних адміністративним судами України;

– дослідити право на захист біометричних даних з позиційпрактикиЄвропейського Суду з прав людини та основні напрями її імплементації у правозастосовчу діяльність органів судової влади України.

*Об'єктом дисертаційного дослідження* є суспільні відносини у сфері адміністративно-правового забезпечення обробки та захисту біометричних персональних даних.

*Предметом дослідження* є адміністративно-правове забезпечення захисту та обігу біометричних персональних даних за законодавством України і зарубіжних країн.

*Методи дослідження.* Методологічною основою дисертаційного дослідження є сукупність сучасних методів наукового пізнання, застосування яких ґрунтується на системному та діалектичному підходах. Це дає змогу дослідити сутність адміністративно-правового забезпечення захисту та обігу

біометричних персональних даних у процесі дослідження історії їх становлення, зарубіжного досвіду функціонування.

У роботі застосовуються такі методи наукового пізнання, як: логіко-семантичний – для аналізу та поглиблення понятійного апарату; класифікації та групування – для систематизації наукових поглядів щодо сутності адміністративно-правового забезпечення захисту та обігу біометричних персональних даних; історичний та порівняльно-правовий – для аналізу історії становлення адміністративно-правового забезпечення захисту та обігу біометричних персональних даних в Україні; на основі методу правового моделювання, логіко-семантичного методу формулювались положення щодо моделі адміністративно-правового забезпечення захисту та обігу біометричних персональних даних в Україні.

Специфіка завдань даного дисертаційного дослідження зумовила особливе значення системно-структурного методу аналізу при з'ясуванні видів та форм реалізації адміністративно-правового забезпечення захисту та обігу біометричних персональних даних в Україні та зарубіжних країнах.

*Стан наукової розробки теми.* Тема дисертаційного дослідження має багатоаспектний характер, що викликає необхідність звернення до різних галузей знань, а саме – інформаційного права, права інтелектуальної власності, адміністративного права, авторського права, конституційного права, міжнародного права, теорії держави та права, філософії, політології, теорії прав людини татехнічних наук у контексті механізмів захисту біометричних даних.

*Аналіз останніх досліджень у сфері* адміністративно-правового забезпечення обігу і захисту біометричних персональних даних підтверджує відсутність достатньої кількості наукових праць та занепокоєння науковців та правників у визначеній темі.

У контексті дослідження методології та понятійно-категоріального апарату інституту персональних даних, питань використання, захисту та обігу персональних даних було використано праці таких науковців: Арістової І. В.,

Заярний О. А., Кормич Б. А., Карпачова Н. І., Баранов А., О. В. Кохановської, О.О. Городова, В.О. Копилова, Є.В. Петрова, О.О. Підопригори, О.А. Підопригори, О.П. Сергєєва, В.С. Цимбалюка, О.І. Харитонової та інших науковців.

У контексті дослідження особливостей та механізму адміністративно-правового забезпечення захисту та обігу біометричних персональних даних, а також дослідження питань технічного захисту чи механізмів захисту біометричних даних було використано праці таких науковців: І. Арістової, А. Баранова, О. С. Іоффе, Н. І. Карпачової, О. В. Кохановської, Л. О. Красавчикової, О. О. Красавчикова, Л. В. Красицької, В.О. Копилова, Р. А. Майданика, М. С. Малеїна, М. М. Малеїної, Л. В. Малюги, Ю. В. Носіка, О.О. Підопригори, О.А. Підопригори, Є. В. Петрова, М. А. Придворова, Й. О. Покровського, З. В. Ромовської, О. П. Сергеєва, Р. О. Стефанчука, Н. В. Устименко О.І. Харитонової та інших.

У контексті дослідження адміністративно-правового статусу фізичної особи, як такої яка має право на захист біометричних персональних даних було використано праці таких наступних науковців: В. Б. Авер'янова, А. М. Авторгова, Н. О. Армаша, Д. М. Бахраха, Ю. П. Битяка, В.Брижка, Т. О. Гуржія, Я. В. Журавля, В. В. Зуя, Д. С. Каблова, С. Ф. Константінова, Л. В. Крупнової, І.Куспляка, О. В. Литвина, У. І. Ляховича, О. О. Пабата, Ю. Н. Старілова, С. В. Шестакова, Н. В. Янюка та інших.

Значна кількість публікацій з даної тематики присвячена загальним аспектам інституту персональних даних, відтак питанню адміністративного-правового забезпечення захисту та обігу біометричних персональних даних не приділено належної уваги науковців.

*Наукова новизна отриманих результатів* полягає у проведенні сучасного, комплексного дослідження адміністративно-правового забезпечення обігу та захисту біометричних персональних даних з використанням методологічного апарату і оцінки накопиченого і практичного матеріалу. Наукова новизна

визначається також досягнутим у процесі вирішення поставлених завдань положеннями, які запропоновані автором особисто.

*Вперше:*

– здійснено дослідження адміністративно-правового забезпечення обігу та захисту біометричних персональних даних у контексті дисертаційного дослідження, що допомогло запропонувати зміст механізму адміністративно-правового забезпечення обігу та захисту біометричних даних:

- запропоновано закріпити обов'язок операторів баз даних ліцензуватись перш ніж використовувати біометричні персональні дані шляхом доповнення відповідним пунктом статтю 9 Закону України «Про захист персональних даних»;
- ми пропонуємо внести зміни до Закону України «Про захист персональних даних» шляхом доповнення статтею 9-1, яка б організувала діяльність баз даних окремо державної форми власності, та окремо приватної форми власності, з запровадженням відповідного державного органу, який би здійснював облік баз даних всіх форм власності, що працюватимуть з біометричними персональними даними;
- у контексті додержання законодавства про захист персональних даних пропонуємо статтю 22 Закону України «Про захист персональних даних» доповнити частиною другою наступного змісту: «2. Уповноважений Верховної Ради України з прав людини не зупиняє провадження по справі у разі розгляду її судом»;
- ч. 1 ст. 22 Закону України «Про захист персональних даних» доповнити пунктом 3, а саме додати до суб'єктів контролю за додержанням законодавства про захист персональних даних громадський контроль;
- запропоновано закріпити законодавчо процедуру постійного моніторингу певним державним органом дотримання законодавства про захист персональних даних та чітко визначити у законі України «Про захист персональних даних» відповідальність;

- пропонуємо, у контексті реалізації принципу електронного урядування, надати можливість подавати електронні скарги до суду та до Уповноваженого Верховної Ради України з прав людини про порушення законодавства у контексті захисту персональних даних(вже існує кілька років!).

*удосконалено:*

– визначення понять «персональні дані», «біометричні дані», «суб'єкт персональних даних», «право на захист біометричних персональних даних»;

– питання розподілу повноважень між Уповноваженим Верховної Ради України та судом у контексті здійснення контролю за дотриманням законодавства про захист персональних даних;

– визначено необхідність навести визначення поняття «контроль за забезпеченням захисту персональних даних» у статті 2 Закону України «Про захист персональних даних», адже відповідне словосполучення у Законі використовується, однак не визначається;

*набуло подальшого розвитку:*

– наукова характеристика адміністративно-правового забезпечення обігу та захисту біометричних персональних даних (конкретизувати в чому саме);

– необхідність доповнити положення статті 2 Закону України «Про захист персональних даних» визначенням поняття «біометричні дані» як особисті дані, отримані внаслідок специфічної технічної обробки, що стосуються фізичних, фізіологічних та поведінкових характеристик фізичної особи, які дозволяють або підтверджують унікальну ідентифікацію цієї фізичної особи;

– наукові положення у контексті конституційно-правового, інформаційного та адміністративного регулювання суспільних відносин у сфері захисту та обігу біометричних персональних даних;

– необхідним є прийняття проекту Закону України «Про захист персональних даних» (реєстраційний № 5628 від 07.06.2021), яким

передбачена, зокрема, особлива обробка даних, пов’язаних з притягненням осіб до кримінальної відповідальності, правопорушень, кримінальних проваджень та судимості, а також пов'язаних із цим заходів безпеки, може здійснюватись у випадках, передбачених законом, який містить належні гарантії для захисту прав і свобод суб’єкта персональних даних згідно з Конституцією та міжнародними договорами, згода на обов’язковість яких надана Верховною Радою України. Контроль за обробкою персональних даних, пов’язаних з притягненням осіб до кримінальної відповідальності, правопорушень, кримінальних проваджень та судимості, а також пов'язаних із цим заходів безпеки, здійснюється контролюючим органом у затвердженому ним порядку, та яким передбачено врегульовувати питання надання/отримання згода суб’єкта персональних даних на обробку його персональних даних тощо.

***Практичне значення отриманих результатів*** полягає в тому, що сформульовані в дисертації наукові положення, висновки й рекомендації упроваджено та можуть бути використані в:

- правотворчій та правозастосовній діяльності – у контексті розроблення проектів змін, доповнень до чинного законодавства, концепцій, правотворчих пропозицій та ініціатив, відповідних проектів нормативно-правових актів з метою ефективності регулювання повноважень органів місцевого самоврядування на основі зарубіжного досвіду, які були розроблені автором дисертації [Додаток А];
- освітньому процесі й науково-дослідній діяльності – теоретичні та практичні рекомендації, висновки та пропозиції, сформульовані в даному дослідженні, можуть бути використані для розробки навчальних програм, лекцій, підручників, тестових завдань і дидактичних матеріалів з начальних дисциплін «Адміністративне право», «Інформаційне право», «Теорія держави і права», «Історія держави і права», а також під час проведення усіх видів занять із зазначених дисциплін (акт впровадження Інституту права Київського національного університету імені Тараса Шевченка ) [Додаток Б];

- право-виховній та право-роз’яснювальній діяльності – для правового виховання і підвищення рівня правової свідомості та культури громадян, державних та муніципальних службовців.

*Апробація результатів дисертації.* Теоретичні і практичні висновки та положення, що містяться в дисертації, оприлюднено на таких міжнародних і всеукраїнських науково-практичних конференціях.

The right to be forgotten as a guarantee of non-interference in a person's personal family life. Current issues of state formation in Ukraine. Proceedings of the International scientific-practical conference of students, graduate students and young scientists from May 19, 2017. Volume 1. P. 257-258.

Some aspects of legal regulation of personal data processing in social networks. Current issues of legal science and practice. Proceedings of the international scientific-practical conference of May 18, 2018. Volume 1. P. 304-305.

*Структура дисертації* визначена її метою та завданням. Робота складається зі вступу, трьох розділів, що охоплюють 9 підрозділів, висновків та списку використаних джерел і становить 169 сторінок.

# РОЗДІЛ І. ЗАГАЛЬНО-ТЕОРЕТИЧНІ ЗАСАДИ АДМІНІСТРАТИВНО-ПРАВОВОГО ЗАБЕЗПЕЧЕННЯ ОБІГУ ТА ЗАХИСТУ БІОМЕТРИЧНИХ ПЕРСОНАЛЬНИХ ДАНИХ

## 1.1. Визначення поняття «біометричні персональні дані»

Розвиток інформаційного суспільства та новітні світові технології є піставою використання біометричних персональних даних у повсякненному житті та державними органами, установами, підприємствами та організаціями з метою упорядкування державних механізмів, надання послуг чи обслуговування особи загалом. Використання біометричних даних особи все більше потребує регулювання з боку держави та міжнародного регулювання, а існуюче законодавство у відповідній сфері потребує постійного оновлення зважаючи на стрімкий розвиток визначеної галузі.

Україна на шляху євроінтеграції має відповідати рівню законодавчого регулювання захисту біометричних персональних даних зокрема, адже саме дослідження адміністративно-правового забезпечення обігу та захисту біометричних персональних даних є актуальним питанням в умовах євроінтеграції та децентралізації, а досвід зарубіжних країн, які ефективно врегульовують забезпечення обігу та захисту біометричних персональних даних дозволить зробити висновки про недоліки та переваги регулювання на законодавчому рівні відповідного питання в Україні, а також проаналізувати ефективність та результативність повноважень органів державної влади зарубіжних країн у контексті забезпечення обігу та захисту біометричних персональних даних.

Завдяки біометричним персональним даним існує ефективний механізм перевірки чи встановлення особи, тож з технічної точки зору біометрія визначається як «автоматичне розпізнавання людей на основі їх біологічних та поведінкових характеристик».

На відміну від інших персональних даних, біометричні дані не лише надають інформацію про людину, а й забезпечують унікальний зв'язок із цією людиною і, отже, можуть бути ідентифікатором. Ця функція використовувалась у ряді програм. Найбільш глибоке застосування – це контроль доступу до приміщень або пристроїв, наприклад, використання відбитків пальців для розблокування смартфона чи будинку.

Що стосується виникнення поняття «біометричні персональні дані» слід зазначити, що у європейських країнах відповідне виникнення датується 2007 роком на офіційному рівні. Поняття біометричних даних не можна знайти ні в Конвенції 108, ні в Директиві про захист даних, двох європейських основоположних документах у сфері захисту персональних даних. Адже у момент їх відповідного прийняття, у 1981 році та у 1995 році відбувся вплив біометричних технологій на захист даних на європейському рівні, який не обговорювався широко. Лише на початку 2000 року європейські органи почали обговорювати цю тему. Перші документи та звіти на цю тему демонструють вагання європейських країн щодо точного статусу та визначення біометричних даних [145; 146; 147].

У 2003 році Робоча група із захисту фізичних осіб щодо обробки персональних даних (A29WP) випустила робочий документ з біометрії, в якому розглядалося застосування правил захисту даних до біометричних систем. Під час обговорення застосування Директиви про захист даних до біометричних даних було оцінено їхній статус з точки зору персональних даних. Перші висновки щодо природи біометричних даних неясні. З одного боку, визнавалось, що біометричні дані за своєю природою є персональними даними, оскільки вони завжди стосуються особи, яку можна «загалом ідентифікувати». Але з іншого боку, вважалось, що біометричні дані не завжди є персональними даними. Документом зазначено, зокрема, про біометричні шаблони, які можуть не становити особисті дані, якщо вони «зберігаються таким чином, що контролер чи будь-яка інша особа не можуть використовувати жодні розумні засоби для ідентифікації суб’єкта даних» [149].

Робоча група не надала жодних чітких критеріїв для розмежування випадків, коли біометричні дані (зокрема, у формі біометричного шаблону) є персональними даними, від випадків, коли вони не є. У наступному Висновку щодо розвитку біометричних технологій, Висновок 3/2012, Робоча група не надала додаткових пояснень. Лише повторювалось, що «у більшості випадків біометричні дані є персональними даними» без подальшого аналізу визначення або формату біометричних даних [147].

Переглядаючи різні думки та звіти щодо захисту даних і біометричних даних, вражає відсутність визначення поняття «біометричні дані». Визначення цього терміну з'явилося досить пізно в дискусіях щодо біометричних даних і технологій. Зокрема, Робочою групою досліджувався статус біометричних даних з точки зору захисту даних ще до визначення цього поняття. Лише у 2007 році Робоча група дала визначення поняття у Висновку 4/2007 щодо поняття персональних даних. У цьому висновку біометричні дані розглядаються з наукової точки зору та визначаються як «біологічні властивості, фізіологічні характеристики, риси життя або повторювані дії, де ці особливості та/або дії є унікальними для цієї особи та піддаються вимірюванню, навіть якщо шаблони, що використовуються на практиці технічно виміряти важко [148].

Крім того, Робочою групою стверджувалось, що біометричні дані мають подвійну природу: вони водночас є частиною інформації про особу та складають (унікальний) зв'язок між цією особою та його біометричні характеристики. Однак це визначення не пов'язує «біометричні дані» з «персональними даними». Разом з тим визначення біометричних даних, яке спочатку містилося в пропозиціях щодо Пакету реформ із захисту даних, також не було пов'язано з персональними даними.

У своїх висновках і звітах європейські органи не чітко використовували терміни «біометричні дані» та «біометрія». Однак систематичний аналіз цих двох понять показує, що «біометричні дані» є як технічним, так і юридичним поняттям, тоді як «біометрія» є лише технічним поняттям [149].

У будь-якому випадку, ці два поняття не є синонімами. Термін «біометрія» був запозичений із галузі біометричного розпізнавання. Таким чином, у контексті захисту даних його слід використовувати лише у спосіб, визначений біометричною спільнотою, тобто як «метод автоматичного розпізнавання» на основі біометричних характеристик [150].

Термін «біометричні дані», зі свого боку, охоплює технічне перетворення біометричних характеристик у формати, які можна використовувати для біометричного розпізнавання. Технічне визначення не потребує посилання на конкретну особу. І навпаки, у контексті захисту даних це посилання має вирішальне значення для визначення того, чи є технічні «біометричні дані» персональними даними [151].

Біометричні дані – це перш за все персональні дані. Це означає, що перед юридичною кваліфікацією «біометричних» цей тип даних має відповідати критеріям, застосовним до загальної категорії персональних даних. Визначення персональних даних у статті 4 Загального регламенту захисту даних дуже схоже на початкове визначення, що міститься в статті 2 Директиви про захист даних.

Це поняття справді визначається ідентичними термінами, як «будь-яка інформація, що стосується ідентифікованої або ідентифікованої фізичної особи («суб'єкта даних»). Різниця між цими двома полягає в описі того, що таке «особа, яку можна ідентифікувати». Стаття 4 Загального регламенту захисту даних містить ширший перелік можливих ідентифікаційних факторів (включно з генетичною ідентичністю) і додає приклади ідентифікаторів (таких як ім'я, ідентифікаційний номер, дані про місцезнаходження та онлайн-ідентифікатор).

Проте це визначення не стосується поняття біометричної особи чи біометричного ідентифікатора. Поріг, за яким визначається ідентифікація особи, залишається низьким: особу не потрібно ідентифікувати, а лише зробити ідентифікованою. Як і в статті 2 Директиви про захист даних, прикметник «ідентифікований» не має визначення.

Згідно з тлумаченням Робочої групи (A29WP) у висновку 4/2007, «ідентифікований» слід розуміти як «виділений» або «виділений» від групи

людей. Таким чином, ідентифікація особи в контексті захисту даних не вимагає встановлення її особи.

Термін «ідентифікований» відрізняється від «ідентифікованого», оскільки перший відноситься до особи, яку ще не ідентифікували, але яку можна ідентифікувати через поєднання іншої інформації. Декларація 26 GDPR повторює тест «ідентифікованості», який спочатку містився в Директиві про захист даних. Цей тест стосується «усіх засобів, які, ймовірно, обґрунтовано можуть бути використані» для ідентифікації особи.

Пункт 26 Загального регламенту захисту даних також встановлює перелік факторів, які слід брати до уваги для оцінки ідентифікації особи. Цей список базується на факторах, запропонованих Робочою групою у висновку 4/2007. Серед цих факторів є ті, що стосуються «доступної технології на момент обробки та технологічного розвитку».

Як і Директива про захист даних, Загальний регламент захисту даних регулює обробку персональних даних. Обробка персональних даних визначена в статті 4 Загального регламенту захисту даних наступним чином: будь-яка операція або набір операцій, які виконуються з персональними даними або наборами персональних даних за допомогою автоматизованих засобів чи ні, таких як збір, запис, організація, структурування, зберігання, адаптація або зміна, пошук, консультація, використання, розкриття шляхом передачі, розповсюдження або іншим чином надання доступу, вирівнювання або комбінування, обмеження, видалення або знищення. Нормативне визначення біометричних даних містить посилання на технічну обробку. Він не визначає, що слід розуміти під «конкретною технічною обробкою», за винятком того, що метою такої обробки має бути однозначна ідентифікація особи. Щоб зрозуміти технічну обробку, якій піддаються біометричні характеристики, і їх перетворення в дані, у наступних параграфах пояснюються технічні етапи біометричного розпізнавання та біометричні шаблони, які з них випливають.

Відносно фізичних, фізіологічних або поведінкових характеристик фізичної особи. Цей критерій стосується визначення біометричних

характеристик. Він визнає широкий спектр вимірюваних характеристик людини, які можна використовувати для біометричного розпізнавання: це охоплює фізичні та фізіологічні атрибути (такі як відбиток пальця, обличчя чи райдужна оболонка ока), а також поведінкові атрибути (такі як голос, хода чи підпис). Різниця між фізіологічними та фізичними характеристиками не дуже чітка. Багато експертів із біометричного розпізнавання посилаються лише на два типи характеристик: або фізичні та поведінкові характеристики, або фізіологічні та поведінкові характеристики.

Вони надають однакові приклади для фізичних і фізіологічних: відбитки пальців, обличчя, геометрія долоні. Цей критерій є ключовим елементом правової кваліфікації біометричних даних. Він описує цілі використання біометричних характеристик, з яких витягуються біометричні дані. Він також встановлює поріг для ідентифікації, застосовний до біометричних даних як категорії персональних даних. Він базується на розумінні різниці значення між біометричною ідентифікацією та ідентифікацією в контексті захисту даних.

Біометричні характеристики самі по собі не вважаються біометричними даними. Біометричними даними вважаються лише особисті дані, «отримані» в результаті їх обробки. Таким чином, до біометричних даних можна віднести не обличчя людини, а зображення її обличчя (картинки). Так само біометричними даними буде класифікуватися не кінчик його або її пальця, а зображення відбитка пальця. Це логічний висновок, оскільки «біометричні дані», як це визначено законом, це перш за все «персональні дані». Щоб бути захищеними згідно з правилами захисту даних, персональні дані мають бути принаймні частиною системи файлів або оброблятися автоматичними засобами.

Самі біометричні характеристики не можуть бути оброблені. Тільки дані, отримані з цих характеристик, можуть. Юридичне визначення «біометричних даних» містить два приклади таких даних: зображення обличчя та дактилоскопічні дані. Що стосується зображень обличчя, не всі фотографії будуть кваліфікуватися як «біометричні дані», а лише ті, які «дозволяють унікальну ідентифікацію або автентифікацію» особи.

Щоб визначити, чи підходить зображення обличчя для біометричного розпізнавання, слід брати до уваги різні чинники або параметри, такі як світло, експозиція, розташування або роздільна здатність камери. Ці параметри логічно не детально описані в Загальному регламенті захисту даних, оскільки вони пов’язані з технологічним розвитком розпізнавання облич. Що стосується дактилоскопічних даних, Загальний регламент захисту даних не містить посилання чи визначення. Інший законодавчий інструмент щодо транскордонного обміну профілями ДНК і відбитками пальців для боротьби з тероризмом і злочинністю, Прюмське рішення, дає визначення. Дактилоскопічні дані визначаються як такі, що охоплюють «зображення відбитків пальців, латентні зображення відбитків пальців, відбитки долонь, латентні відбитки долонь і шаблони таких зображень».

Аналіз різних компонентів юридичного поняття «біометричні дані» показує, що лише персональні дані, отримані в результаті спеціальної обробки біометричних характеристик і стосуються ідентифікованої особи, будуть кваліфікуватися як «персональні дані». Коли ці дані однозначно ідентифікують особу, вона виграє від захисту, наданого конфіденційним даним.

Біометрія не є маргінальною технологією і її використання постійно зростає. Біометричні технології, які, як передбачається, матимуть найбільший ринковий потенціал у період з 2016 по 2025 рік, включають датчики відбитків пальців, розпізнавання голосу/мовлення, розпізнавання райдужної оболонки ока та розпізнавання облич.

Сьогодні багато людей використовують деякі з цих технологій щодня. Згідно з нещодавнім дослідженням споживчого сприйняття біометрії, 82% тих, хто має доступ до технології, оснащеної датчиками відбитків пальців, використовують ці датчики.

Біометричні дані можуть містити інформацію делікатного характеру, таку як стан здоров'я, схильність до захворювань, расове або етнічне походження. Одержання цієї додаткової інформації залежить від датчиків, що використовуються для збирання біометричних характеристик, а також від

алгоритмів, які використовуються для обробки необробленої форми цих характеристик.

Однак біометричні ознаки можуть розкривати не тільки очевидну для людського ока інформацію, таку як стать, етнічне походження, деформації тіла або шкірні захворювання.

Завдяки областям медицини, біостатистики та машинного навчання, що постійно розвиваються, необроблені біометричні характеристики можуть бути проаналізовані для отримання інформації про ще не виявлені захворювання, поточний психічний і біологічний стан або ймовірний рівень виконання деяких завдань. Такі можливості збільшують показову цінність таких даних. Вони також викликають питання про масштаби таких розширених орієнтовних значень біометричних даних, їх вплив на вразливість суб'єктів даних та загальний вплив на захист конфіденційності в галузі біометрії.

Законодавча система адміністративно-правового забезпечення обігу і захисту біометричних персональних даних в Україні передбачає складну модель державного управління, в якій паралельно функціонують дві підсистеми публічного управління: обіг та захист, організація якого здійснюється. І під час обігу персональних даних і під час їх захисту необхідно забезпечувати реалізацію прав особи, організувати обіг і захист біометричних персональних даних так, щоб обіг не був підставою захисту, а обидві інституції функціонували ефективно паралельно [17].

Питання адміністративно-правового обігу та захисту біометричних персональних даних є актуальним з огляду на відсутність ефективного регулювання державою як персональних даних, так і відповідно біометричних персональних даних. Інститут захисту біометричних персональних даних в Україні є відносно новим та мало дослідженим, тож порівняльний аналіз регулювання та захисту біометричних персональних даних на законодавчому рівні у зарубіжних країнах для України є необхідним, лише перейманням успішного зарубіжного досвіду якнайшвидше держави можуть забезпечити порядок у відповідній галузі [23].

Відсутність кодифікації загалом всіх норм, що стосуються організації біометричних персональних даних в Україні зумовлює труднощі у пошуку необхідної норми для особи, яка не має юридичної освіти, що прямо суперечить принципам законодавчої доступності та правової свідомості суспільства. У процесі євроінтеграції держава має виправляти подібні недоліки та прямувати на шляху відкритості, доступності законодавства до населення, тим більше у тих сферах, що стосуються кожної особи, як громадянина, так і не громадянина України.

Адміністративно-правове забезпечення обігу та захисту біометричних персональних даних слід розпочати з понятійно-категоріального апарату визначеної теми, а саме надати визначення поняттям «персональні дані» та «захист персональних даних», визначенню поняття «біометричні персональні дані» та надати визначення іншим похідних від зазначених поняттям у правовій доктрині та чинному законодавстві України.

Біометричні персональні дані є особливим видом даних, які юридично виступають у формі виключного права власності, монополія на які обмежується законом в інтересах дотримання прав та основних свобод інших осіб, а також – дотримання балансу прав людини, суспільства і держави.

Відповідно до ст. 2 Закону України «Про захист персональних даних» персональні дані - відомості чи сукупність відомостей про фізичну особу, яка ідентифікована або може бути конкретно ідентифікована [88]. Разом з тим, законодавство України не завжди узгоджується із нормами Закону «Про захист персональних даних».

В свою чергу, захистом персональних даних є захист відомостей про особу, що ідентифікована або таку, що може бути ідентифікованою [88].

Науковці В.М. Брижко, О.М. Гальченко, В.С. Цимбалюк, О.А. Орєхов, А.М. Чорнобров визначають поняття «персональні дані» як окремі відомості про фізичну особу чи сукупність таких відомостей про фізичну особу, які вже є ідентифікованими або можуть бути ідентифікованими [19, с. 145].

Видані на ім`я певної особи документи, підписані відповідною особою документи, інформація, яка була зібрана державними органами влади та органами місцевого самоврядування про відповідну особу шляхом реалізації повноважень відповідних органів державної влади та органів місцевого самоврядування загалом – це також персональні дані. Але, варто зауважити, що органи державної влади та органи місцевого самоврядування мають право збирати відомості про певну особу з урахуванням певних винятків.

Щодо вищезазначених винятків слід навести офіційне тлумачення Конституційним судом України частини 4 статті 23 Закону України «Про інформацію», адже відповідно до даного тлумачення не дозволяється, збирати, зберігати, використовувати та поширювати конфіденційну інформацію про особу, у випадках, коли вона не попереджена та не надала згоду, окрім випадків, коли така інформація збирається, зберігається, використовується та поширюється в інтересах національної безпеки, економічного добробуту, прав та свобод людини [22].

Важливо визначити поняття «конфіденційна інформація», адже останнє за ознаками має пряме відношення до досліджуваних нами біометричних персональних даних. Таким чином конфіденційною інформацією вважаються відомості щодо освіти, сімейного стану, релігійності, стану здоров'я, дати і місця народження, майнового стану та інших персональних даних щодо особи у відповідності до Рішення Конституційного Суду України у справі щодо офіційного тлумачення статей 3, 23, 31, 47, 48 Закону України «Про інформацію» та статті 12 Закону України «Про прокуратуру» від 30 жовтня 1997 року № 5-зп (справа К.Г. Устименка № 18/203-97).

У статті 2 Закону України «Про захист персональних даних» наводиться визначення таких понять як «база персональних даних», «персональні дані» тощо, але жодне із цих визначень понять не містять згадки про біометричні дані, біометричні документи особи, навіть тоді, коли вони є необхідними у визначеннях відповідних понять, [88] наприклад, стаття 2 відповідного Закону визначає базу персональних даних як іменовану сукупність упорядкованих

персональних даних в електронній формі та/або у формі картотек персональних даних, але жодної згадки про біометричні документи нема тоді, коли в Україні вже масово використовуються електронні документи осіб.

А також стаття 2 Закону надає визначення персональним даним як відомостям чи сукупності відомостей про фізичну особу, яка ідентифікована або може бути конкретно ідентифікована тоді, коли згадки про біометричні відомості про особу відсутні у даному нормативно закріпленому визначенні [88].

Щодо визначення поняття «персональні дані» в зарубіжних країнах континентальної правової системи, зокрема в Німеччині, Закон Німеччини «Про подальший розвиток обробки даних і захисту даних» від 20 грудня 1990 року визначає персональні дані як конкретні дані про особисті або майнові відносини встановленої або установлюваної фізичної особи [19, с. 146].

Варто наголосити, що в Україні біометричні персональні дані активно використовуються державними органами, юридичними особами приватного права тощо, про що свідчать процедура оформлення українських паспортів і закордонних паспортів, використання біометричних даних є очевидним, тому до відомостей персонального характеру Комітетом по стандартам України, в ДСТУ 3389-96 визначено «ідентифікаційну картку особи як носій біометричної інформації», тобто хоча б якесь нормативне регулювання на рівні підзаконних нормативно-правових актів в Україні наявне, але це не можна назвати повноцінним врегулюванням відносин щодо зберігання, використання, поширення тощо біометричних даних в Україні [30, с. 43-47].

Дослідження питання біометричних персональних даних передбачає необхідність звертатись до визначення похідних понять, які мають спільну ознаку персональні дані, які відповідно потребують захисту і безпеки. Таким чином, пропонуємо визначити поняття «інформаційна безпека», адже, якщо проаналізувати мету адміністративно-правового забезпечення обігу та захисту біометричних персональних даних, то вся суть визначеної теми полягає

загалом у інформаційній безпеці, якої так прагне як наша країна так і міжнародні сусіди.

Інформаційне суспільство розвивається наразі разом із правовою і демократичної державністю, шляхом використання інформаційно-комунікаційних технологій в системі публічного управління, баз даних загалом, та біометричних персональних даних зокрема, що потребує забезпечення належного рівня інформаційної безпеки, зокрема функціонування реєстру пацієнтів в електронній системі охорони здоров'я [79; 38; 135; 29, с. 102-108].

В. Брижко, Л. Задорожня та М. Коваль пропонують визначати поняття «інформаційна безпека» як у широкому так і у вузькому розумінні. У вузькому розумінні інформаційну безпеку розглядають як захист інформації, захист таємниці, комерційної інформації, з обмеженим доступом, персональних даних тощо, а в широкому розумінні інформаційну безпеку визначають як захист інформаційних систем, які фактично є засобом передачі інформації [87, с. 21].

Дещо інакше запропоновано визначення поняття у законах, зокрема Закон України «Про основи національної безпеки» містить визначення поняття «національна безпека», але з контексту слід припустити, що інформаційною безпекою вважається необхідність своєчасного вжиття заходів, адекватних характеру і масштабам загроз національним інтересам.

Всі види безпеки, в тому числі й інформаційна, пов'язуються зі станом захищеності життєво важливих інтересів її об'єктів, причому об'єктами називаються: по-перше, людина і громадянин − їхні конституційні права і свободи; по-друге, суспільство − його духовні, морально-етичні, культурні, історичні, інтелектуальні та матеріальні цінності, інформаційне і навколишнє природне середовище і природні ресурси; по-третє, держава − її конституційний лад, суверенітет, територіальна цілісність і недоторканність [47, с. 74-78].

Але, у контексті інформаційної безпеки, варто погодитись із Солодкою О. М. щодо того, що саме підвищення участі громадськості у процесах удосконалення зв'язку між суспільством та державою, адже відповідний контроль громадськості є важливою передумовою інформаційної політики у контексті забезпечення та зміцнення інформаційної безпеки в Україні [114, с. 41].

Визначивши поняття «інформаційна безпека», яке за ознаками стосується також і досліджуваного нами поняття «біометричні персональні дані», варто приділити увагу визначенню систематизації біометричних персональних даних зокрема.

У контексті систематизації біометричних персональних даних, слід визначити поняття «база даних», адже біометричні персональні дані відповідно зберігаються загалом у базах даних, тому вважаємо за необхідне розглянути наразі визначення відповідного поняття.

Частина перша ст. 1 Закону України «Про Національну програму інформатизації» визначає поняття «база даних» як іменовану сукупність даних, що відображає стан об'єктів та їх відношень у визначеній предметній області [94].

Також українське законодавство поняття «база даних» дублює з поняттям «державний інформаційний ресурс», яке у ч. 2 ст. 1 Закону України «Про Державну службу спеціального зв'язку та захисту інформації України» визначає як систематизовану інформацію, що є доступною за допомогою інформаційних технологій, право на володіння, використання або розпорядження якою належить державним органам, військовим формуванням, утвореним відповідно до законів України, державним підприємствам, установам та організаціям, а також інформацію, створення якої передбачено законодавством та яка обробляється фізичними або юридичними особами відповідно до наданих їм повноважень суб'єктами владних повноважень [95].

Наразі вважаємо за необхідне наголосити на тому, що бази даних, які містять біометричні персональні дані є відкритими та закритими, і у своєму

дисертаційному дослідженні Ільницький М. П. визначив 148 сайтів в Україні, які містять біометричні персональні дані, тобто відповідні сайти-бази даних [48, с. 289-292].

Навіть, якщо лише розглянути бази даних Міністерства юстиції України, дані інформаційні ресурси містять велику кількість біометричних персональних даних, до яких особи мають доступ через мережу Інтернет тощо [48, с. 289-292].

Загалом захист персональних даних зокрема, та інформації загалом регламентується Правилами забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах, затверджених Постановою Кабінету Міністрів України від 29 березня 2006 року (далі - Правила) [96].

Таким чином, правилами у системі має бути захищеною:

1) відкрита інформація, яка належить до державних інформаційних ресурсів, а також відкрита інформація про діяльність суб'єктів владних повноважень, військових формувань, яка оприлюднюється в Інтернеті, інших глобальних інформаційних мережах і системах або передається телекомунікаційними мережами;

2) конфіденційна інформація, яка перебуває у володінні розпорядників інформації, визначених ч. 1 ст. 13 Закону України «Про доступ до публічної інформації»;

3) службова інформація; інформація, яка становить державну або іншу передбачену законом таємницю;

4) інформація, вимога щодо захисту якої встановлена законом [96].

Сучасний стан дослідження використання, обігу та захисту біометричних персональних даних став передумовою розвитку у науці таких явищ як «інтернет речей» та «хмарні технології», адже на побутовому рівні з використанням мережі інтернет та інформаційних технологій на побутовому рівні біометричні персональні дані використовуються частіше ніж

державними органами офіційно, а зберігаються, у свою чергу, більше у хмарних базах даних, ніж у офіційних державницьких базах даних.

У своїй науковій роботі, у контексті дослідження проблем правового забезпечення правомірної обробки біометричних персональних даних, Заярний О. А. віддає перевагу використанню при цьому інтернету речей, адже наразі саме використання інтернету речей для біометричних персональних даних є ризиком порушення конфіденційності персональних даних [40, с. 93-96].

Інтернет речей складається з мільйонів датчиків і різних пристроїв, що генерують безперервні потоки даних, які можна використовувати для поліпшення як життя взагалі, так і для підвищення ефективності бізнесу зокрема [116, с. 6].

Ми погоджуємось із думкою Заярного О. А. щодо необхідності нормативного врегулювання технічного захисту біометричних персональних даних при проектуванні, використанні та знищенні Інтернету речей, необхідність розробки порядку обробки та технічного захисту біометричних персональних даних власників та споживачів інтернету речей є актуальним сьогодні питанням для законодавця [40, с. 93-96].

Брижко В. М. у своїй науковій роботі аналізує та розкриває тему хмарних обчислень, зазначаючи, що вони використовуються компаніями для обчислення великої кількості даних [14].

Зокрема, ми пропонуємо розглядати ще також і поняття «хмарні бази даних», адже так звані «хмари» з використанням мережі інтернет дійсно зберігають досить велику кількість як публічних баз даних, так і приватних баз даних.

Та, пропонуємо визначати поняття «хмарні бази даних» як сукупність даних, що відображають стан об'єктів та їх відношень у визначеній предметній області, використовуються із застосуванням Інтернету речей.

Визначивши поняття «біометричні персональні дані», ми дійшли проміжного висновку, що порядок у понятійно-категоріальному апараті є

передумовою ефективного подальшого дослідження визначеної теми дисертаційної роботи.

Перевагами вважаємо інформатизацію суспільства та розвиток інформаційних технологій, виникнення та дію в Україні Інтернету речей, розвиток хмарних технологій, але недоліком вважаємо нормативно неврегульованість всього вищезазначеного, адже останнє несе ризик наявності перешкод у захисті біометричних персональних даних.

## 1.2. Межі та способи правомірного обігу персональних даних за законодавством України і Європейського Союзу

Межі та способи правомірного обігу персональних даних у світі активно досліджуються з огляду на специфіку біометричних даних, які все частіше зазнають несанкціоноваго використання. Спеціальні категорії персональних даних, зокрема біометричні персональні дані на сучасному етапі розвитку інформаційних технологій все частіше стають об’єктом зловживань з боку діяльності суб’єктів, що впливають на їх обробку. Запобігти чи попередити порушення права особина приватне життя, перешкодити незаконному обігу та обробці біометричних персональних даних, на нашу думку, можна двома шляхами: маючи ефективне національне та міжнародне законодавство, яке регулює обіг і захист біометричних персональних даних, а також судову практику та практику Уповноваженого Верховної Ради України щодо недопущення порушень та недопущення уникнення відповідальності за порушення законодавства у сфері обігу, обробки та захисту біометричних персональних даних.

Біометричні персональні дані мають особливу ознаку, яка вирізняє їх серед всіх інших персональних даних, а саме - нерозривний зв'язок з їх носієм – людиною, тому біометричні персональні дані є найбільш вразливими, та

найбільш чутливими у разі порушення законодавства щодо їх обігу, обробки чи захисту.

Наступною особливою ознакою біометричних персональних даних є складність зміни, адже особі сьогодні, навіть в епоху розвитку медицини та комп'ютерних технологій, значно складно змінити ДНК, відбитки пальців чи сітківку ока, що ще більше ускладнює специфіку адміністративно-правового забезпечення ефективного регулювання відповідної сфери.

Біометрія - це термін, що відноситься до «використання відмітних біологічних або поведінкових характеристик для ідентифікації людей» за допомогою автоматизованих засобів. Однак ці характеристики можна досліджувати і для інших цілей, а не лише для того, щоб відрізнити одну людину від іншої.

Біологічні та поведінкові характеристики широко використовуються також для оцінки ідентичності та особистісних аспектів (таких як вік, стать, етнічна приналежність, соціальний статус, здібності тощо), для оцінки миттєвого стану людини (виявлення емоцій чи надчуттєвих почуттів), або для медичної діагностики аномалій та захворювань.

Зібрані за допомогою автоматизованих засобів та збережені у цифровому вигляді біологічні або поведінкові характеристики можуть бути проаналізовані за допомогою систем розпізнавання образів та методів машинного навчання для отримання будь-якої необхідної інформації за умови, що встановлений зв'язок між даними, доступними з біометричних датчиків.

Деяка інформація має дуже конфіденційний характер і може вплинути на конфіденційність членів сім'ї (генетичні захворювання). Відбитки пальців можуть бути проаналізовані для визначення статі чи походження людини. За своєю температурою відбитки пальців можуть свідчити про стан розслабленості чи занепокоєння людини і навіть показувати інтенсивність гострого стресу. Крім цього, температура відбитків пальців може прогнозувати ефективність людини у завданнях чи вказувати на симпатичні реакції.

Особливості гребенів на відбитках пальців (дерматогліфіка) також можуть сприяти діагностиці деяких захворювань, оскільки деякі можуть бути пов'язані з генетичними аномаліями. За допомогою камери можна виміряти частоту серцевих скорочень відбитка пальця і виявити потенційне порушення роботи серця.

Обличчя - це багате джерело різноманітної інформації. Природно, зображення обличчя можуть аналізуватись, щоб визначити вік, стать, расове, етнічне чи культурне походження, емоції, або навіть привабливість обличчя. За допомогою алгоритмів машинного зору можуть бути ідентифіковані захворювання.

Зображення райдужної оболонки ока виявляють інформацію про аномалії або захворювання, такі як гостра катаракта, глаукома, задні та передні синехії, відшарування сітківки, рубеоз райдужної оболонки, васкуляризація рогівки, виразки рогівки, помутніння або помутніння, трансплантація рогівки або пошкодження та атрофія райдужної оболонки.

Голос можна аналізувати, наприклад, за статтю, віком, емоційним станом (гнів, радість, страх аб надзвичайний страх, смуток, нудьга, щастя, страждання) або стан здоров’я. Наприклад, такі хвороби, як хвороба Паркінсона, передеменція та хвороба Альцгеймера, можна виявити за голосом.

З одного боку накопичення біометричних персональних даних та систематизація їх у бази даних є ефективним засобом виявлення і запобігання злочинів, ідентифікації людини на користь держави, але так само є ризиком до незаконного обігу та обробки відповідних персональних даних, що може нашкодити людині.

Німецький експерт із захисту даних Йоганнес Каспар зазначає, що краще не використовувати сканер відбитків пальців, якими оснащені моделі смартфону від Apple iPhone. На думку експерта, біометричні дані важко видалити, вони супроводжують людину упродовж усього життя, а відбитки пальців не повинні використовуватися для повсякденної авторизації, особливо коли вони зберігаються у файлі.

Представник Apple з апаратної безпеки Ден Річчіо у відеоролику на сайті компанії розповів, що дактилоскопічні дані зберігаються в зашифрованому вигляді у спеціальній безпечній частині процесора A7 і можуть бути доступні тільки датчику Touch ID. За словами Річчіо, ця інформація не може бути зчитана будь-якими іншими програмами і ніколи не потрапить ні на сервери Apple, ні в хмару зберігання iCloud.

Проте ці аргументи не переконали Йоганнеса Каспара. Він стверджує, що «звичайний користувач не може сьогодні контролювати, що роблять його телефонні додатки, які дані з пристрою вони копіюють і яку інформацію зчитують». У Der Spiegel зазначають, що такі дані довіряти техніці було ризиковано і до викриття американської шпигунської програми PRISM, про яку розповів світові Едвард Сноуден. Але тепер ризики зростають [39].

А відповідне збільшення використання подібних пристроїв, та і загалом інформаційних засобів обміну і розвитку сучасних технологій, ставить питання про правове регулювання отримання, передачі, зберігання і використання біометричних персональних даних, яке очевидно на сьогодні не є достатньо ефективним.

Очевидно, що біометричні технології, які зараз щоденно використовуються великою кількістю людей завдяки своїй зручності та комфорту, вже зараз розкривають значний обсяг додаткової інформації. Ця інформація доступна в цифровому вигляді, може і має призвести до масової переробки для різних цілей. Така практика стимулює ще більш глибокі дослідження кореляцій різних біологічних і поведінкових характеристик.

Деякі з цих досліджень будуть проведені для внутрішніх цілей компаній і, можливо, ніколи не стануть доступними для громадськості.

Усі описані вище можливості збільшують вразливість людей не лише на розкриття інформації про них іншим суб’єктам, а також на розкриття неправильної інформації.

Біометрія як така не є повністю надійною. Те ж саме стосується виявлення розширеної інформативності даних. Інформація може бути отримана лише в

різному ступені ймовірності. Однак навіть ця інформація може бути цінною для деяких суб’єктів, які можуть спробувати використати її потенціал.

Основною наукою, що займається дослідженням обігу, обробки та використання біометричних даних є біометрика, передумовою виокремлення даної міждисциплінарної науки став науково-технічний прогрес, який потребував глибокого дослідження проблем, які неможливо вирішити в рамках одного напряму досліджень. Одні науковці визначають поняття «біометрика» як біологічна дисципліна, що користується математичними прийомами для кількісного аналізу біологічних явищ - мінливості і інше [10].

Інші науковці визначають поняття «біометрика» як процес збору, обробки та зберігання даних про фізичні характеристики людини з метою її ідентифікації [11].

Науковці наразі приділяють багато уваги такому специфічному виду персональних даних як біометричні персональні дані, адже даний вид персональних даних потребує найбільшого правового захисту. Зокрема, Бачило І. Л. вказує, що на сьогоднішній день гостро стоїть проблема правового режиму такого класу інформації, як біоінформація: відбитки пальців, зіниць очей людини, її ДНК і інші елементи індивіда, широко використовувані в практиці ідентифікації суб'єкта в найрізноманітніших сферах його життя і стосунків з іншими суб'єктами, та мають потребу у встановленні їх правового режиму, порядку використання і захисту» [12, с. 138].

Дослідження меж правомірного обігу біометричних персональних даних передбачає дослідження також правового статусу третьї особи як суб`єкта доступу до біометричних персональних даних, адже саме їй надається право доступу до біометричних персональних даних у відповідності до закону, за згодою володільця чи у відповідності до договору.

Стаття 4 Закону України «Про захист персональних даних» до суб’єктів відносин, пов’язаних із персональними даними, відносить: суб'єкта персональних даних, володільця персональних даних, розпорядника

персональних даних, третю особу та Уповноваженого Верховної Ради України з прав людини [88].

Директива Європейського парламенту та Ради «Про захист фізичних осіб при обробці персональних даних і про вільне переміщення таких даних» № 95/46/ЄС від 24 жовтня 1995 року хоч і втратила чинність, однак можлива для використання у якості порівняння, адже визначає поняття «третя особа» як будь-яка фізична чи юридична особа, державний орган, агентство чи будь-який інший орган, інший, ніж суб'єкт даних, контролер, оператор обробки даних і особи, що, будучи безпосередньо підпорядкованими контролеру чи оператору обробки даних, уповноважена обробляти дані [33].

Конституція України законодавчо закріпила право на свободу та особисту недоторканність, у статті 29, і неприпустимість збирання, зберігання, використання та поширення інформації про особу без її згоди, у статті 32, крім випадків, визначених законом, і тільки в інтересах національної безпеки, економічного добробуту та прав людини. Відповідно кожен має право вільно збирати, зберігати, використовувати і поширювати інформацію усно, письмово або в інший спосіб – на свій вибір.

Не викликає жодних заперечень, що невід'ємними характеристиками сучасного суспільства є прогрес інтеграції інформаційних технологій, а також інтенсифікація процесів у галузі інформатизації.

Ці фактори, які безпосередньо обумовлюють поглиблення процесів обміну інформацією, як невід'ємна характеристика глобалізації та побудови інформаційного суспільства водночас породжують низку проблем, пов'язаних із необхідністю захисту особистих прав та свобод людини, зокрема, в аспекті обігу та обробки персональних даних.

Нормативне закріплення особистих прав та свобод людини у міжнародному праві відображено ще у Загальній декларації прав людини 1948 року, відповідно до ст. 12 якої «ніхто не може зазнавати безпідставного втручання у його особисте і сімейне життя, безпідставного посягання на недоторканність його житла, тайну його кореспонденції або на його честь і

репутацію. Кожна людина має право на захист закону від такого втручання або таких посягань» [45].

Положення аналогічного змісту містить чстина перша статті 8 Європейської Конвенції про захист прав людини і основоположних свобод 1950 р., а саме: «Кожен має право на повагу до свого приватного і сімейного життя, до свого житла і кореспонденції» [51].

На думку Пазюка А. В. у контексті обігу персональних даних, правила збору й обробки персональних даних особи охоплюються поняттям «інформаційна приватність», яка в комплексі з тілесною (фізичною), комунікаційною та територіальною приватністю уособлюють у собі складові елементи права особи на приватність [85, с. 10].

У контексті дослідження законодавчого регулювання обігу біометричних персональних даних, українське законодавство дещо відрізняється від європейського, зокрема Україна на законодавчому рівні не надає можливості чи механізму контролю суб'єктом використання чи наявності його персональних даних, виправлення останніх.

Таким чином, власник персональних даних не може обмежити обсяг чи межі використання державою своїх біометричних персональних даних, обмежити цільове призначення використання біометричних персональних даних тощо.

А також в Україні відсутній посилений режим захисту тих біометричних персональних даних особи, які визначають національну приналежність чи погляди із переконаннями, чи здоров'я тощо [97, с. 102].

Базовим документом у сфері захисту біометричних персональних даних США є Закон «Про свободу інформації» (The Freedom of Information Act) 1966 року [140] та Закон «Про надання кредитної інформації про покупця» (The Fair Credit Reporting Act) [141] та Закон США «Про конфіденційність» (The Privacy Act) 1974 року, що зазначає необхідні механізми запобігання випадків протиправних дій з боку держави у випадках використання біометричних даних особи [142].

Так звана концепція США у сфері захисту інформації вказує на те, що інформація має захищатись незалежно від носія такої інформації, таким чином її захист реалізується закріпленням відповідних принципів, які використовуються під час правовідносин із захисту біометричних персональних даних та персональних даних загалом.

Дещо схожі норми, але досить недостатні щодо збору, використання, обробки, поширення чи зберігання інформації про особу, чи її персональних даних містяться у ст.ст. 6, 7 та 11 Закону України «Про захист персональних даних».

Статтею 8 законопроекту пропонується особлива обробка даних. Зокрема, обробка персональних даних, пов’язаних з притягненням осіб до кримінальної відповідальності, правопорушень, кримінальних проваджень та судимості, а також пов'язаних із цим заходів безпеки, може здійснюватись у випадках, передбачених законом, який містить належні гарантії для захисту прав і свобод суб’єкта персональних даних згідно з Конституцією та міжнародними договорами, згода на обов’язковість яких надана Верховною Радою України. Контроль за обробкою персональних даних, пов’язаних з притягненням осіб до кримінальної відповідальності, правопорушень, кримінальних проваджень та судимості, а також пов'язаних із цим заходів безпеки, здійснюється контролюючим органом у затвердженому ним порядку [88].

Європейський Союз гарантує всім фізичним особам право на захист персональних даних людини як фундаментальної свободи. Нещодавно ЄС реформував своє законодавство щодо захисту даних для встановлення єдиних правил і мінімізації відхилень у національних законах.

Оригінальна Директива про захист даних вимагала, щоб національні закони забороняли обробку спеціальних категорій даних, які розкривають «расове або етнічне походження, політичні погляди, релігійні чи філософські переконання, членство в профспілках і обробка даних щодо здоров’я чи

статевого життя», оскільки за своєю природою вони здатні порушувати основні свободи чи конфіденційність.

Біометрія як така є широким терміном, що включає інформацію про аспекти конституції, функціонування або поведінки біологічного організму.

Профілювання визначається як будь-яка форма автоматизованої обробки персональних даних, що полягає у використанні персональних даних для оцінки певних особистих аспектів, що стосуються фізичної особи, зокрема для аналізу або прогнозування аспектів, що стосуються продуктивності цієї фізичної особи на роботі, економічного становища, здоров'я, особистих уподобань, інтересів, надійності тощо.

Профілювання часто пов'язане з повторним використанням інформації та обробкою з метою, відмінною від початково визначеної. Посилається на ризик, пов'язаний із таким повторним використанням інформації як «розповзання функцій», оскільки це стосується використання технології для інших цілей, ніж це було спочатку призначено. Таке використання «може призвести до непередбаченого використання персональних даних контролером або третіми сторонами та у разі втрати контролю суб'єктом даних».

У GDPR профілювання тісно пов'язане з автоматизованим прийняттям рішень. Суб'єктам даних гарантується право не підпадати під автоматизоване прийняття рішень в тому числі профілювання. Однак профілювання можна здійснити навіть без прийняття будь-яких рішень. Якщо виконуються інші вимоги GDPR (принципи та законність обробки), суб'єкт даних не може заперечувати проти профілювання. Важливість прийняття рішень полягає в тому, що прийняття рішень може здійснюватися на шкоду суб'єкту даних, тоді як отримання додаткової інформації, яка не вплине на поведінку контролера щодо суб'єкта даних, вважається відносно нешкідливим.

Слід звернути особливу увагу на можливість профілювання, виконане інакше, ніж автоматизованими засобами.

Що стосується зарубіжного регулювання відповідного питання, федеральний Закон «Про захист онлайнових персональних даних дітей»

(COPPA), регулює в США відносини щодо використання персональної інформації в Інтернеті [143].

Даний нормативно-правовий акт містить заборону збирати та використовувати персональні дані про дітей віком до 13 років без згоди на це їх батьків, а, отже, регулює відносини щодо збирання та використання інформації про малолітніх.

Також даний законодавчий акт закріплює обов'язкові правила для інтернет-ресурсів, які збирають персональну інформацію про дітей. На сьогодні, в Україні, відповідне питання потребує сучасного законодавчого регулювання, як і конкретизація принципів зберігання, збирання, поширення, обробки чи використання біометричних персональних даних, на відміну від США.

Характеризуючи досвід Німеччини, як провідної країни Європейського Союзу, яка характеризується достатньо високою ефективністю правового захисту та загалом регулювання зберігання, обробки, використання та захисту персональних даних, ще з минулого століття, а саме з 1970 року у Німеччині було прийнято законодавчий акт у сфері захисту персональних даних, а саме Закон ФРН «Про захист даних у галузі адміністративного управління».

Даний нормативно-правовий акт забезпечував превентивні дії щодо захисту персональних даних, а також не допускав змін до Конституції ФРН у частині розподілу повноважень державних органів перед парламентом з виникненням «інформаційних переваг». З 1977 року даний нормативний акт запрацював на всій території федерації.

А також Німеччина характеризується у відповідній сфері тим, що громадяни мають право обирати спеціального Уповноваженого із захисту персональних даних, який контролює, чи не порушуються права німців у контексті поширення їх персональних даних тощо [120].

З 1991 року у ФРН діє Закон «Про захист персональних даних», за яким зовнішній контроль за персональними даними осіб вже не здійснюється, а мова про захист персональних даних йде лише тоді, коли вони застосовуються

у приватному житті й виконують певну громадську чи економічну функцію життєдіяльності [120].

Також у жовтні 1997 р. у Німеччині був прийнятий Акт захисту інформації в телекомунікаціях (Teleservices Data Protection Act), адже останній є частиною прийнятих положень федерального законодавства Німеччини щодо регулювання умов інформації та комунікаційних послуг [144].

Що стосується законодавства Франції, на відміну від Німеччини, Франція має інститут Уповноваженого із питань захисту персональних («номінативних») даних, який закріплений Законом Франції «Про інформатику, картотеки та свободи» та діє від 6 листопада 1978 р.

Останній містить механізми автоматизованого збирання, обробки, зберігання і поширення персональних біометричних даних, передбачає створення Національної комісії з інформатики, що займається контролем близько 120 тисяч електронних баз даних.

Закон у контексті відповідальності за порушення норм має відсилочну норму до Декрету від 23 грудня 1981 р. № 81- 1142 у контексті адміністративної відповідальності за правопорушення щодо персональних даних, а також щодо та кримінальної відповідальності за такі порушення.

Вітчизняною правовою доктриною приділяється вкрай мало уваги дослідженню міжнародного співробітництва, пов’язаного з передачею персональних даних іноземним третім особам, у контексті останніх законодавчих змін та тенденцій розвитку автоматизованих алгоритмів аналізу персональних даних.

В Україні процес впровадження біометричних документів було розпочато наприкінці 2012 року. Закон України «Про Єдиний державний демографічний реєстр та документи, що підтверджують громадянство України, посвідчують особу чи її спеціальний статус», що набрав чинності 6 грудня 2012 року передбачає створення Єдиного демографічного реєстру та впровадження документів, що міститимуть безконтактний електронний носій із біометричними даними власника документу.

Серед них – паспорт громадянина України та паспорт громадянина України для виїзду за кордон.

Підсумовуючи співвідношення українського законодавства та законодавства ЄС у контексті обігу та захисту біометричних персональних даних вважаємо за необхідне зазначити наступне.

Основними законодавчими актами, які регулюють в Україні питання захисту біометричних даних, а в тому числі безпосередньо і меж правомірного обігу біометричних персональних даних є Закон України «Про захист персональних даних», Закон України «Про Єдиний державний демографічний реєстр та документи, що підтверджують громадянство України, посвідчують особу чи її спеціальний статус», відповідні законодавчі акти є відносно новими, тож потребують подільшого дослідження. Межі правомірного обігу персональних даних визначені як національним, так і міжнародним законодавством, але межі правомірного обігу біометричних персональних даних не врегульовані безпосередньо національним законодавством.

## 1.3. Право на захист біометричних персональних даних, як складова адміністративно-правового статусу фізичної особи

Право на захист біометричних персональних даних за аналогією вважають складовою частиною конституційного права на недоторканість особистого життя людини.

Стаття 29 Конституції України передбачає право кожного на свободу та особисту недоторканість. На нашу думку, саме особиста недоторканість передбачає конституційне право на захист біометричних персональних даних, тож відповідне право є конституційним.

Розглядаючи відповідне конституційне право людини на захист біометричних персональних даних як складову адміністративно-правового

статусу фізичної особи, слід визначити зміст адміністративно-правового статусу фізичної особи.

Загалом правовий статус є своєрідним зв'язком особи з державою через певні юридичні форми, які відповідно фіксують такий зв'язок, зокрема Оніщенко Н. М. зазначає, що правовим статусом є система законодавчо встановлених та гарантованих державою прав, свобод, законних інтересів та обов'язків суб'єкта суспільних відносин., які характеризуються ознакою універсальності (стосується всіх суб'єктів); індивідуальності (містить індивідуальні особливості людини та фактичний стан у суспільних відносинах); ознакою взаємного зв'язку із іншими складовими та ознакою системності [17, с. 21-25].

Пропонуємо класифікувати правовий статус за декількома підставами, а саме за суб'єктним складом та за характером правового статусу (загальний, галузевий, спеціальний, індивідуальний) та суб'єктом [119, с. 366].

На думку О. Ф. Скакун правовий статус слід визначати як систему закріплених у нормативно-правових актах і гарантованих державою прав, свобод, обов'язків, відповідальності, відповідно до яких індивід як суб'єкт права координує свою поведінку в суспільстві [112, с. 59].

На думку Малька О. В. правовим статусом є комплексна інтеграційна категорія, що відображає взаємовідносини суб'єктів суспільних відносин, особи і суспільства, громадянина і держави, індивіда та колективу, а також інші соціальні зв'язки [121, с. 397].

Ляхович І. визначає правовий статус як комплексну правову категорію, за допомогою якої визначається правове становище у суспільстві та державі будьяких учасників правовідносин, забезпечується реалізація та захист їх прав, свобод та законних інтересів [61].

Розглядаючи структуру правового статусу, ми погоджуємось із думкою Колодія А. М., який зазначає, що складовими частинами правового статусу є статусні правові норми і правові відносини; суб'єктивні права, свободи і

юридичні обов'язки; громадянство; правові принципи і юридичні гарантії; законні інтереси; правосуб'єктність; юридична відповідальність.

Деякі автори у якості елементів правового статусу розглядають правове зобов'язання, законність, правопорядок, правосвідомість, гуманізм, справедливість.

Панчишин А. В., у свою чергу до структурних елементів правового статусу включає правові норми, що визначають статус; основні права, свободи, законні інтереми та обов'язки; правосуб'єктність; правові принципи; громадянство; гарантії прав і свобод; юридична відповідальність; правовідносини загального типу [86, с. 95-98].

Визначивши поняття та структуру правового статусу, вважаємо за необхідне приділити увагу саме визначенню поняття та наданню характеристики адміністративно-правовому статусу особи, зокрема більшість науковців поняття адміністративно-правового статусу визначає через характеристику його структурних елементів.

Битяк Ю. П. зазначає, що адміністративно-правовий статус громадянина є складовою частиною його загального статусу, і відповідно встановлюється обсягом і характером його адміністративної правосуб'єктності, яку становлять адміністративна правоздатність і адміністративна дієздатність [1, с. 58-59].

На думку Голосніченка І. П. до зміст адміністративно-правового статусу особи містить комплекс її прав і обов'язків, закріплених нормами адміністративного права, реалізація яких забезпечується певними гарантіями, основою чого розглядається адміністративна правоздатність, відповідно як можливість мати адміністративно-правові права і обов'язки [1, с. 198].

В свою чергу Вітрук М. В. адміністративно-правовий статус особи розглядає як сукупність прав, обов'язків та законних інтересів відповідної особи [20, с. 147].

А Новосьолов В. І. розглядаючи адміністративно-правовий статус через його структуру, виділяє адміністративну правосуб'єктність, права, обов'язки та право-обов'язки осіб [67, с. 87].

Так от Горшеньов В. М. складовими частинами адміністративно-правового статусу вважає права, свободи, юридичні обов'язки та юридичну відповідальність [21, с. 54-58], а Зуй В. В. складовими частинами адміністративно-правового статусу вважає обов'язки, права, гарантії діяльності і юридичну відповідальність [41, с. 107-108].

Ознаками адміністративно-правового режиму персональних даних є такі як:

1) сукупність визначених норм, правих поведінки у відповідній сфері;

2) вищезазначені правила виступають регулятором відносин між суб'єктами, володільцями, розпорядниками персональних даних та третіми особами у інформаційній сфері;

3) передбачають порядок обробки та умови доступу до персональних даних, зокрема порядок збирання, зберігання, передачі, використання, а також реєстрацію та накопичення, блокування, поширення чи поновлення, або ж зміну чи знищення таких персональних даних;

4) адміністративно-правовий режим персональних даних передбачає грунтування на принципах, таких як добровільності передання персональних даних та цільового характеру використання, принципі законності та верховенства права; принципах згоди письмової форми на передачу персональних даних та охорони від випадкового або несанкціонованого руйнування, втрати, несанкціонованого доступу, зміни, блокування або передачу персональних даних; принципах достовірності, а також визначення строку цільового збереження персональних даних; [21, с. 196-201].

6) за порушення таких правил передбачені дисциплінарна чи адміністративна відповідальність;

7) ознакою також є наявність правового імперативно-диспозитивного методу щодо впливу на поведінку учасників відносин щодо обробки персональних даних;

8) відбувається шляхом використання спеціальних засобів;

9) мета адміністративно-правового режиму персональних даних передбачає реалізацію норми, передбаченої статтею 32 Конституції України щодо забезпечення права на приватність [133, с. 176].

У контексті захисту саме біометричних персональних даних, слід зазначити, що фактичний захист біометричних персональних даних або є високим, або відсутній як захист взагалі.

Наприклад, ми вважаємо високим ступенем захисту біометричний паспорт особи, адже останні мають високу захищеність від підроблення. Новий паспорт містить електронний безконтактний чіп, який неможливо змінити або скопіювати.

Нові паспорти, на відміну від попередніх «книжечок» видаються на основі електронної бази даних – Єдиного державного демографічного реєстру, отже кожній особі лише один раз доводиться пройти процедуру ідентифікації, надалі інформація про неї буде міститися в реєстрі. Але є бази даних, особливо ті, які відкриті в мережі інтернет, тож ми їх вважаємо майже не захищеними.

Розглядаючи захист біометричних персональних даних, важливо зазначити, що 27 квітня 2016 року Європарламент прийняв General Data Protection Regulation (далі - GDPR). А 25 травня цього року Загальний регламент Європейського Союзу про захист даних (далі - Регламент) набув чинності. І навідміну від українського національного законодавства, даний міжнародний нормативно-правовий акт містить норми у контексті забезпечення захисту біометричних персональних даних.

Загальний регламент захисту даних, який безпосередньо застосовується в усьому ЄС держави-члени з 25 травня 2018 року прийняли подібний підхід і в принципі забороняють обробку спеціальних категорій даних, включаючи біометричні дані. У порівнянні з Директивою про захист даних Регламент визначає, що обробка цих категорій даних «може створити серйозні ризики для основних прав і свобод. Ці категорії даних можуть оброблятися лише у виняткових випадках, зазначених у статті 9 Загального регламенту захисту даних.

Загальний регламент захисту даних чітко визначає біометричні дані як «особисті дані, отримані в результаті певної технічної обробки, що стосується фізичних, фізіологічних або поведінкових характеристик фізичної особи, які дозволяють або підтверджують унікальну ідентифікацію цієї фізичної особи, такі як зображення обличчя або дактилоскопічні дані» і встановлює їх як особливу категорію персональних даних. Однак слід зазначити, що Регламент використовує вузьке розуміння біометрія.

Поняття «персональні дані», у контексті міжнародного акту, охоплює будь-яку інформацію, яка стосується фізичних осіб. Відповідно, такі дані можуть включати ім'я, фотографії, електронну адресу, відомості про банківські рахунки, IP-адресу і навіть публікації в соціальних мережах.

А, досліджувані нами біометричні дані є так званими чутливими даними, так звані «sensitive personal data», які включають біометричні дані, расову, релігійну, етнічну приналежність, філософські погляди, участь у некомерційних організаціях, дані про здоров'я.

З метою охорони таких даних встановлюються більш суворі правила збору і обробки інформації, які Україні слід з досвідом переймати та запозичувати у національне законодавство.

У національному законодавстві право на захист біометричних персональних даних є структурним елементом конституційного права на недоторканість особистого життя, яке означає виключення можливості здійснення будь-яких операцій чи дій з біометричними персональними даними за відсутності згоди суб`єкта відповідних даних. Вищезазначеними діями є закріплені статтею 32 Конституції України, зберігання, збір, використання та поширення тощо, і закріплені Законом України «Про захист персональних даних» - збирання, систематизація, накопичення, зберігання, уточнення, оновлення чи зміна, використання, розповсюдження, передача, знеособлення, блокування, знищення (а загалом - обробка біометричних персональних даних).

Важливо зазначити, що суспільні відносини, що стосуються права захисту біометричних персональних даних, хоч і є в основному інформаційними, але мають у своїй структурі ще конституційні правовідносини та адміністративно-правові, адже до адміністративно-правових відносин саме і належить правовий статус фізичної особи – суб`єкта біометричних персональних даних.

Таким чином, аналізуючі правові відносини, що реалізують право на захист біометричних персональних даних, правовідносини складають адміністративно-правовий, інформаційний та конституційний елементи суспільних відносин.

На нашу думку, саме зарубіжний досвід дає змогу оцінити стан реалізації права на захит біометричних персональних даних в Україні та запозичити, за необхідності, позитивний зарубіжний досвід.

На нашу думку, Україні не вистачає законодавчо закріпленого обов`язку обліку операторів, що здійснюють обробку біометричних персональних даних. Українським законодавством визначено перелік операторів, що здійснюють обробку біометричних персональних даних на державному рівні, але, на привеликий жаль, не визначено обов`язку реєструватись іншим операторам біометричних персональних даних у приватному праві, і самі ці оператори становлять ризик для суб`єкта персональних даних порушення їх відповідного права.

Що стосується вразливості людей, два фактори мають велике значення в біометричних системах: датчики моніторингу та алгоритми, які обробляють зібрану інформацію від цих датчиків.

Датчики в біометрії відрізняються залежно від використовуваної біометричної технології. Біометричні датчики – це перетворювачі, які перетворюють інформацію про біометричне лікування людини в електричний сигнал. Вони вимірюють різні види енергії, такі як тиск, температура, світло, швидкість тощо.

Обличчя можна розпізнати за допомогою камер або інфрачервоних датчиків, голос з використанням мікрофонів, відбитків пальців за допомогою оптичних, кремнієвих або ультразвукових датчиків. Датчики мають важливе значення, особливо щодо обсягу та точності даних, які вони можуть зібрати з фізичної особи. Чим більша сума і точніші дані, збільшуються шанси в отриманні додаткової інформації з біометричного зразка, такої як особливості біологічного функціонування особи, симптоми її захворювань, інформація про неї, поточний стан або її особистість. Таку інформацію можна отримати за допомогою спеціальних алгоритмів.

Біометричні алгоритми фактично є системами розпізнавання образів. Як уже було зазначено вище, розпізнавання образів також використовується для виявлення аномалій і діагностики захворювань. Незважаючи на певний рівень технічної стандартизації, кожен алгоритм оригінально обробляє інформацію. Крім того, величезна кількість алгоритмів для обробки зібраних біометричних даних є запатентованим і, отже, секретним за своєю природою.

Для користувачів біометричних систем практично неможливо визначити, яка інформація збирається про них і про те, як вони далі обробляються. Вони повинні покладатися на гарантії надається їм суб'єктом, який керує біометричною системою. При цьому інтереси суб'єктів, які користуються біометричною системою, та фізичних осіб, зареєстрованих у цій системі, не обов'язково збігаються. Ці інтереси можуть бути навіть суперечливими.

Такі країни як Польща, Угорщина, Німеччина, Швеція, Франція мають закріплений законодавчо обов`язок всіх операторів, всіх форм власності, що здійснюють обробку як персональних даних, так і біометричних персональних даних, реєструватись, відповідно у даних європейських країнах є облік операторів, що здійснюють обробку біометричних персональних даних, що є відмінним і дуже ефективним засобом захисту біометричних персональних даних осіб.

Важливо зазначити, що у Франції та Швеції, окрім обов`язку реєструвати та вести облік операторів, що здійснюють обробку біометричних персональних даних, законодавчо закріплено обов`язок ліцензувати відповідних операторів обробки біометричних персональних даних, що унеможливлює порушення права на захист біометричних персональних даних з боку такого оператора.

Закон України «Про захист біометричних персональних даних» хоч і передбачає у статті 9 обов`язок реєстрації баз персональних даних, дану норму виконують в основному підприємства, установи та організації державної форми власності, а приватні, на жаль, ні, і відповідно належних контроль за такими операторами баз даних відсутній.

На нашу думку право на захист біометричних персональних даних - це сукупність організаційно-правових та інформаційно-технічних заходів, що унеможливлюють неправомірні дії з біометричними персональними даними, зберігають їх конфіденційність, передбачають доступ до них лише за згодою суб’єкта даних та під контролем суб`єкта даних.

## Висновки до розділу 1

У першому розділі дисертаційної роботи було визначено поняття «біометричні дані» як особисті дані, отримані внаслідок специфічної технічної обробки, що стосуються фізичних, фізіологічних та поведінкових характеристик фізичної особи, які дозволяють або підтверджують унікальну ідентифікацію цієї фізичної особи, такі як зображення обличчя особи чи дактилоскопічні (відбитки пальців) дані, а поняття «персональні дані» як окремі відомості про фізичну особу чи сукупність таких відомостей про фізичну особу, які вже є ідентифікованими або можуть бути ідентифікованими.

Біометричні дані визначаються у технічній сфері як параметри - відцифровані відбитки пальців рук, відцифроване зображення обличчя. Ми переконані, що біометричними даними є значно ширший перелік даних, однак зважаючи на вузькі межі регулювання відносин визначеного положення, відображаються лише ті дані, які є можливість технічно ідентифікувати у того чи іншого органу влади.

Разом із тим, фіксацією біометричних даних як параметрів є процес збору біометричних даних (параметрів) громадянина України, іноземця та особи без громадянства (далі - особа), внесення їх та зберігання у відомчих інформаційних системах суб'єктів національної системи. У свою чергу біометричною ідентифікацією вважається здійснення пошуку за принципом «один до багатьох» шляхом розпізнавання і зіставлення одного або двох біометричних даних (параметрів) особи з біометричними даними (параметрами) осіб у відомчих інформаційних системах суб'єктів національної системи, а біометричною варифікацією є здійснення пошуку за принципом «один до одного» між біометричними даними (параметрами), отриманими від особи в даний момент, і біометричними даними (параметрами), наявними у відомчих інформаційних системах суб'єктів національної системи.

Генетичні дані визначені як персональні дані щодо вроджених або набутих генетичних ознак фізичної особи, які надають унікальну інформацію про фізіологію чи здоров'я такої фізичної особи та такі, що отримані, зокрема, в результаті аналізу біологічного зразка, взятого у відповідної фізичної особи.

Визначено, що біометричні персональні дані зберігаються у базах даних, та визначено поняття «база даних» як іменована сукупність даних, що відображає стан об'єктів та їх відношень у визначеній предметній області. Бази біометричних даних є закритими та відкритими.

Наведено ще один різновид носія біометричних персональних даних, а саме «хмарні бази даних», та дане поняття є похідним від поняття «хмарні технології». Хмарні бази даних зберігають біометричні персональні дані через застосування інтернету речей, є законодавчо неврегульованими в Україні та потребують врегулювання, зокрема порядку використання та обробки біометричних даних задля подальшого їх ефективного захисту.

У контексті дослідження питання меж і способів правомірного обігу персональних даних за законодавством України та Європейського Союзу було визначено суб`єктів доступу до персональних даних та основні характеристики правомірних меж їх обігу.

Дослідження питання законодавства України та Європейського Союзу, яке закріплює межі правомірного обігу персональних даних показало наявність закріплених законодавчо меж правомірного обігу персональних даних як з точки зору національного, так і з точки зору європейського законодавства.

Але у проміжному підсумку дослідження визначеного питання було зазначено, що закріплених у національному законодавстві меж правомірного обігу біометричних персональних даних нема, що і є передумовою необхідності зміни профільного законодавства у частині передбачення як визначення поняття «біометричні дані», так і визначення порядку їх використання, обробки, обігу та захисту.

Ми запропонували наступне визначення права на захист біометричних персональних даних, а саме як сукупність організаційно-правових та інформаційно-технічних заходів, що унеможливлюють неправомірні дії з біометричними персональними даними, зберігають їх конфіденційність, передбачають доступ до них лише за згодою суб`єкта даних та під контролем суб`єкта даних.

Запропоновано визначати поняття «хмарні бази даних» як сукупність даних, що відображають стан об'єктів та їх відношень у визначеній предметній області, використовуються із застосуванням Інтернету речей.

Також було запропоновано використати ефективний зарубіжних досвід у сфері захисту біометричних персональних даних, а саме аналізувався досвід країн Франції та Швеції у контексті необхідності ліцензування операторів баз біометричних персональних даних та персональних даних загалом.

На нашу думку, оператори саме баз біометричних персональних даних, як найбільш сутливих персональних даних, мають бути не лише обов’язково зареєстровані, щоб відповідні державні органи могли вести їх облік, а і обов’язково ліцензовані, щоб уникнути ризику здійснення неправомірних дій з біометричними персональними даними.

Визначено, що адміністративно-правовий статус громадянина є складовою частиною його загального статусу, і відповідно встановлюється обсягом і характером його адміністративної правосуб’єктності, яку становлять адміністративна правоздатність і адміністративна дієздатність. У національному законодавстві право на захист біометричних персональних даних є структурним елементом конституційного права на недоторканість особистого життя, яке означає виключення можливості здійснення будь-яких операцій чи дій з біометричними персональними даними за відсутності згоди субєкта відповідних даних.

Вищезазначеними діями є закріплені статтею 32 Конституції України, зберігання, збір, використання та поширення тощо, і закріплені Законом України «Про захист персональних даних» - збирання, систематизація,

накопичення, зберігання, уточнення, оновлення чи зміна, використання, розповсюдження, передача, знеособлення, блокування, знищення (а загалом - обробка біометричних персональних даних).

# РОЗДІЛ ІІ. МЕХАНІЗМ АДМІНІСТРАТИВНО-ПРАВОВОГО ЗАБЕЗПЕЧЕННЯ ОБІГУ ТА ЗАХИСТУ БІОМЕТРИЧНИХ ПЕРСОНАЛЬНИХ ДАНИХ ЗА ЗАКОНОДАВСТВОМ УКРАЇНИ

## 2.1. Нормативні засади адміністративно-правового забезпечення обігу та захисту біометричних персональних даних за законодавством України та Європейського Союзу

Законодавче врегулювання адміністративно-правового забезпечення обігу та захисту біометричних персональних даних є інструментом уникнення та попередження порушень у сфері інтелектуальної власності, є поштовхом наближення України до рівня європейських країн у різних сферах життя та механізмом подолання корупції в Україні.

Відповідно до ст. 2 Закону України «Про захист персональних даних» персональні дані - відомості чи сукупність відомостей про фізичну особу, яка ідентифікована або може бути конкретно ідентифікована. Разом з тим, законодавство України не завжди узгоджується із нормами Закону «Про захист персональних даних».

Закон України «Про захист персональних даних в Україні» не закріплює визначення поняття «біометричні персональні дані», однак наразі у Верховній Раді України зареєстровано проект Закону України «Про захист персональних даних» (реєстраційний № 5628 від 07.06.2021), який має на меті ліквідувати визначену прогалину [89].

Роз’яснення Уповноваженого Верховної Ради України з прав людини від 08.01.2014 р. «Роз’яснення основних положень Порядку повідомлення Уповноваженого щодо визначення обробки персональних даних, яка становить особливий ризик для прав і свобод суб’єктів персональних даних» біометричними даними визначає сукупність даних про особу, зібраних на основі фіксації її характеристик, що мають достатню стабільність та істотно відрізняються від аналогічних параметрів інших осіб (наприклад

відцифрований підпис особи, відцифрований образ обличчя особи, відцифровані відбитки пальців рук, відцифрований малюнок сітківки ока тощо).

Загальним регламентом захисту даних поняття «біометричні персональні дані» визначено як особисті дані, отримані внаслідок специфічної технічної обробки, що стосуються фізичних, фізіологічних та поведінкових характеристик фізичної особи, які дозволяють або підтверджують унікальну ідентифікацію цієї фізичної особи, такі як зображення обличчя особи чи дактилоскопічні (відбитки пальців) дані.

Визначення біометричних даних (параметрів) закріплене також Положенням про національну систему біометричної верифікації та ідентифікації громадян України, іноземців та осіб без громадянства, звтвердженим постановою Кабінету Міністрів України від 27 грудня 2017 року № 1073, зокрема біометричними даними (параметрами) - відцифровані відбитки пальців рук, відцифроване зображення обличчя.

Ми переконані, що біометричними даними є значно ширший перелік даних, однак зважаючи на вузькі межі регулювання відносин визначеного положення, відображаються лише ті дані, які є можливість технічно ідентифікувати у того чи іншого органу влади.

Разом із тим, положенням пропонується також визначити поняття "фіксація біометричних даних (параметрів) особи", "біометрична ідентифікація", "біометрична верифікація". Зокрема, фіксацією біометричних даних як параметрів є процес збору біометричних даних (параметрів) громадянина України, іноземця та особи без громадянства (далі - особа), внесення їх та зберігання у відомчих інформаційних системах суб’єктів національної системи. У свою чергу біометричною ідентифікацією вважається здійснення пошуку за принципом “один до багатьох” шляхом розпізнавання і зіставлення одного або двох біометричних даних (параметрів) особи з біометричними даними (параметрами) осіб у відомчих інформаційних системах суб’єктів національної системи, а біометричною варифікацією є

здійснення пошуку за принципом “один до одного” між біометричними даними (параметрами), отриманими від особи в даний момент, і біометричними даними (параметрами), наявними у відомчих інформаційних системах суб’єктів національної системи.

Наразі, у Верховній Раді України зареєстровано проект Закону України «Про захист персональних даних» (реєстраційний № 5628 від 07.06.2021) (далі - законопроект), поданий народними депутатами України Чернєвим Є.В., Тарасенком Т. П. та іншими народними депутатами України. Відповідний проект Закону є важливим кроком у зміні правового регулювання як персональних даних, так і біометричних персональних даних, адже окрім визначення необхідних понять у проекті закону також пропонується визначити таким, що втратив чинність Закон України "Про захист персональних даних в Україні".

Законопроектом пропонується визначити біометричні дані як персональні дані, які стосуються фізичних, фізіологічних чи поведінкових характеристик фізичної особи, які в результаті спеціальної технічної обробки надають можливість ідентифікувати або верифікувати фізичну особу. Також законопроектом пропонується визначити такі поняття як витік персональних даних, генетичні дані та інші.

Генетичні дані визначаються як персональні дані щодо вроджених або набутих генетичних ознак фізичної особи, які надають унікальну інформацію про фізіологію чи здоров’я такої фізичної особи та такі, що отримані, зокрема, в результаті аналізу біологічного зразка, взятого у відповідної фізичної особи.

Разом із тим, вважаємо, що визначений законопроет є суттєвим кроком до сучасного законодавчого регулювання в Україні сфери захисту персональних даних, зокрема біометричних персональних даних, а також виступає своєрідною імплементацією положень GDRP.

Міжнародний нормативно-правовий акт Директива 95/46/ЄС Європейського парламенту і Ради від 24 жовтня 1995 року «Про захист фізичних осіб при обробці персональних даних і про вільне переміщення таких

даних» визначає персональні дані як будь-яку інформацію, що стосується встановленої фізичної особи чи фізичної особи, яку можна встановити «суб'єкт даних» (втратила чинність).

Таким чином, суб'єкт даних - особа, яку можна встановити, прямо чи непрямо, зокрема за допомогою ідентифікаційного коду або одного чи більше факторів, притаманних фізичним, фізіологічним, розумовим, економічним, культурним чи соціальним захистам її особистості.

Вищезазначений міжнародний нормативно-правовий акт згадку про біометричні дані не містить, жодним чином не закріплює та не розкриває дане поняття.

У контексті дослідження нормативних засад адміністративно-правового забезпечення обігу та захисту біометричних персональних даних, останні регламентуються наступними міжнародними документами:

Конвенція № 108 Ради Європи про захист осіб у зв'язку з автоматизованою обробкою їх персональних даних;

Додатковий протокол до Конвенції щодо наглядового органу та транскордонних потоків даних;

Рекомендації КМ РЄ (наприклад, № R (87) 15 щодо використання персональних даних у сфері діяльності правоохоронних органів, Рекомендація № R (97) 5 щодо захисту медичних даних);

Директива 95/46/ЄС Європейського парламенту та Ради про захист осіб у зв'язку з обробкою персональних даних і про вільний рух таких даних. Конвенція про захист прав і основоположних свобод людини (стаття 8 «Право особи на повагу до її приватного, сімейного життя, житла та кореспонденції» тощо).

Важливо визначити зміст адміністративно-правового режиму загалом, та згодом розглядати його у контексті забезпечення захисту біометричних персональних даних.

Таким чином, звертаючи увагу на дослідження науковців, зокрема Алексєєв С. С. пропонує правовий режим розглядати як «свого роду об'ємний

блок в спільному арсеналі правового інструментарію, певний комплекс правових засобів, який з'єднує в єдину конструкцію». Останнє ще раз підкреслює, що використання правових засобів при вирішенні тих чи інших спеціальних завдань в значній мірі полягає в тому, щоб вибрати оптимальний для вирішення відповідного завдання правовий режим, майстерно відпрацювати його відповідно до специфіки цього завдання і змісту регульованих суспільних відносин [5, с. 243].

На думку Л.В. Томаша правовий режим має власну структуру, яка складає норми права, юридичні факти, правовідносини, акти реалізації прав і обов'язків, правозастосування, суб'єкти права, їх правові статуси, об'єкти права, методи взаємозв'язку конкретних видів суб'єктів з об'єктами, систему гарантій (насамперед юридичну відповідальність за порушення режиму) [123, с. 25].

У свою чергу, Б. Я. Бляхман виділяє такі складові правового режиму як норми права, нормативно-правові акти, юридичні факти, правові відносини, акти реалізації, тлумачення і застосування норм права, правову культуру тощо [15, с. 21].

На думку Матузова М.І. правовим режимом є особливий порядок правового регулювання, що виражається в певному поєднанні юридичних засобів і, який створює соціальний стан і конкретну ступінь благополуччя або неблагополуччя для задоволення інтересів суб'єктів права [64, с. 17].

Адміністративно-правове забезпечення розглядається як один із видів правового забезпечення, але єдиного визначеного поняття, з яким би погодилась більшість науковців нема. Цвік М. В. визначає адміністративно-правове забезпечення як цілеспрямована дія на поведінку людей і суспільні відносини за допомогою правових (юридичних) засобів [127, с. 327].

На думку Колесникова Є.Є. адміністративно-правовим забезпеченням є здійснюване державою за допомогою спеціального механізму упорядкування суспільних відносин, їх юридичне закріплення, охорона, реалізація та розвиток, на думку науковця адміністративно-правове забезпечення захисту

відповідних прав особи, зокрема права на захист персональних даних, є впливом держави на суспільні відносини з метою впорядкування, захисту та охорони відносин між органами влади, споживачами та суб'єктами господарювання, що здійснюється за допомогою норм права та через спеціальний механізм [52, с. 432-438].

На думку Римарчук Г. С. адміністративно-правовим забезпеченням є здійснення державою за допомогою правових норм, приписів і сукупності засобів упорядкування суспільних відносин, їх юридичне закріплення, охорона, реалізація та розвиток [99].

Гумін А. П. пропонує адміністративно-правове забезпечення розглядати як упорядкування суспільних відносин уповноваженими на те державою органами, їх юридичне закріплення за допомогою правових норм, охорона, реалізація і розвиток [25, с. 46-50].

Насамперед, у контексті дослідження засад адміністративно-правового забезпечення обігу та захисту біометричних персональних даних, вважаємо за необхідне визначити, яким чином здійснюється адміністративно-правове регулювання біометричних персональних даних міжнародними документами.

Регламент Європейського парламенту і Ради Європи «Про захист фізичних осіб у зв'язку з опрацюванням персональних даних і про вільний рух таких даних, та про скасування Директиви 95/46/ЄС (Загальний регламент про захист даних)» від 27 квітня 2016 року (далі - Загальний регламент про захист даних) у пункті 51 Передмови зазначається, що особливо чутливі персональні дані, у контексті фундаментальних прав і свобод потребують особливого захисту, адже їх опрацювання може створити істотні ризики для фундаментальних прав і свобод. Ми презумуємо, що визначеними особливо чутливими персональними даними і є біометричні персональні дані.

Пунктом 53 Передмови Загального регламенту про захист даних передбачено необхідність державами-членами забезпечити умови та обмеження у контексті роботи з біометричними даними, адже саме

біометричні персональні дані є спеціальною категорією персональних даних [93, с. 34].

Що стосується обробки будь-яких типів персональних даних, Загальний регламент захисту даних вимагає від обробки бути максимально прозорою. Зобов'язання щодо прозорої обробки викладено в загальному вигляді в статті 5, а про принципи обробки персональних даних та зазначені у статті 12.

Прозорість призначена для усунення негативних наслідків внутрішньої непрозорості обробки персональних даних, що часто призводить до відсутності або значного зменшення контролю над власними персональними даними. Люди, чиї персональні дані обробляються (суб’єкти даних), мають право і на прозору інформацію, а також на прозору комунікацію. Це передбачає вимоги до використовуваної мови, яка має бути чіткою та простою. Водночас інформація має бути короткою, зрозумілою та легкодоступною.

Тільки ті, хто справді розуміє, що передбачає обробка їхніх особистих даних, мають можливість вирішити, як та за яких умов вони готові дати згоду на таку обробку особі, яка має обробляти дані (контролер).

Однак було доведено, що з таким зростаючим обсягом обробки даних, суб’єкти даних не можуть прочитати та зрозуміти політику конфіденційності, пам’ятати про всі надані згоди. Крім того, у разі диверсійного використання біометрії з самого початку контролери можуть уникати інформування суб'єкта даних за проектом, розраховувати ризик ймовірності того, що така практика коли-небудь буде розкрита.

На жаль, вислів «від дискримінації не захистишся, якщо ви не знаєте про те, що вас дискримінують» можна також застосувати до подання документів, які насправді часто тісно пов'язані з дискримінацією. Суб’єкти даних можуть не мати найменшого уявлення про те, що їх використовують як джерело інформації про їхню фізичну форму або психологічний стан.

Прозорість також пов'язана з правом на пояснення суб'єкта даних, щодо якого контролери зобов’язані обробляти персональні дані законно. Їхню діяльність міг би розслідувати національний наглядовий орган. Цей захід має

допомогти гарантувати відповідність обробки. На жаль, враховуючи кількість контролерів, можливі інциденти не можуть бути врегульовані своєчасно. Крім того, деякі контролери порушують свій обов'язок реєструвати і невідомі владі. Оскільки біометричні дані можуть бути отримані та оброблені як віддалено, так і таємно, правоохоронні органи можуть не захистити суб'єктів даних.

Щоб мінімізувати порушення законів, Загальний регламент запровадив новий правовий інститут – спеціаліст із захисту даних.

Спеціаліст із захисту даних має право на доступ до всієї інформації, пов'язаної з обробкою особистих даних. Це означає, що вона також повинна мати доступ до вихідного коду, щоб перевірити його реальні функції. Роль уповноваженого із захисту даних полягає у забезпеченні постійної інформації, огляду діяльності під час обробки персональних даних. Оскільки суб'єкти даних обмежені, засіб перевірки реальних дій контролера, уповноваженої особи із захисту даних є гарантією законних способів обробки. На жаль, незважаючи на те, що призначення уповноваженого із захисту даних є розумним рішенням проблем із непрозорістю обробки даних, в результаті ця установа може не виконувати своїх функцій з різних причин. Головною причиною може бути те, що організація не призначає уповноваженого із захисту даних і після збирання достатньої кількості біометричних даних буде ліквідованою.

Важливим є те, що міжнародний документ має певні вимоги щодо того, що створивши умови та обмеження по роботі з біометричними персональними даними держави-члени не мають права перешкоджати вільному потоку персональних даних в межах Союзу тоді, коли такі умови застосовують до транскордонного опрацювання таких даних; а також держави-члени мають зберегти професійну таємницю, для певних цілей, пов'язаних із здоров'ям у роботі з біометричними персональними даними [100].

Пункт 14 статті 4 Загального регламенту про захист даних надає визначення поняттю «біометричні дані», та визначає останні як персональні дані, отримані в результаті спеціального технічного опрацювання, що

стосується фізичних, фізіологічних чи поведінкових ознак фізичної особи, таких як, зображення обличчя чи дактилоскопічні дані, що дозволяють однозначно ідентифікувати або підтверджують однозначну ідентифікацію фізичної особи [100].

Відповідно до ч. 1 ст. 9 Загального регламенту про захист даних заборонено опрацювання персональних даних, що розкривають расову чи етнічну приналежність, політичні переконання, релігійні чи філософські вірування, чи членство в професійних спілках, і опрацювання генетичних даних, біометричних даних для цілі єдиної ідентифікації фізичної особи, даних стосовно стану здоров'я чи даних про статеве життя фізичної особи чи її сексуальної орієнтації [100].

А ч. 4 ст. 9 Загального регламенту про захист даних (далі - Регламент) надає можливість державам-членам мати або вводити деталізовані умови, в тому числі, обмеження, у зв'язку з опрацюванням генетичних даних, біометричних даних або даних стосовно стану здоров'я [100].

Вищезазначений Регламент було прийнято 14 квітня 2016 року, набрав чинності він 24 травня 2016 року (на 20-й день після офіційного опублікування в «Офіційному віснику Європейського Союзу») і після дворічного перехідного періоду почав застосовуватися відповідно 25 травня 2018 року [42].

Важливо зазначити, що за правовою процедурою Регламент не є директивою, яку необхідно вводити в дію на національному рівні шляхом прийняття відповідного закону, Регламент фактично діє і на території України з 25 травня 2018 року.

Тобто вже більше трьох років Регламент діє і в Україні, але запропоновані Регламентом норми щодо біометричних персональних даних у профільному Законі України «Про захист персональних даних» сьогодні відсутні.

Хоча в деяких країнах пострадянського простору нормативно-правові акти у сфері врегулювання питання обігу персональних даних містять навіть окремі статті, присвячені біометричним персональним даним.

В свою чергу, Конвенція № 108 Ради Європи про захист осіб у зв'язку з автоматизованою обробкою їх персональних даних № 994_326 ратифікована Україною 06.07.2010 року також закріплює норми, що відповідно складають засади адміністративно-правового забезпечення обігу та захисту персональних даних. Зокрема преамбула відповідного документу передбачає мету Конвенції як забезпечення на території кожної Сторони для кожної особи, незалежно від її громадянства або місця проживання, дотримання її прав й основоположних свобод, зокрема її права на недоторканість приватного життя, у зв'язку з автоматизованою обробкою персональних даних, що її стосуються [53].

Вважаємо за необхідне зазначити, що відповідний міжнародний документ не приділяє уваги біометричним персональним даним, а регулює у загальному вигляді відносини щодо персональних даних, так само, як і Додатковий протокол до Конвенції про захист осіб у зв'язку з автоматизованою обробкою персональних даних щодо органів нагляду та транскордонних потоків даних, Рекомендації КМ РЄ (наприклад, № R (87) 15 щодо використання персональних даних у сфері діяльності правоохоронних органів тощо.

Закон України «Про захист персональний даних» не регулює індивідуально сферу відносин щодо біометричних персональних даних, а виключно містить згадку про біометричні дані у контексті особливих вимог до обробки персональних даних. Частиною 1 статті 7 Закону забороняється обробка персональних даних про расове або етнічне походження, політичні, релігійні або світоглядні переконання, членство в політичних партіях та професійних спілках, засудження до кримінального покарання, а також даних, що стосуються здоров’я, статевого життя, біометричних або генетичних даних.

Статтею 7 законопроекту запропоновано наступним чином врегульовувати питання надання/отримання згода суб’єкта персональних даних на обробку його персональних даних, тож остання може бути надана у

письмовій чи електронній формі через веб-сайт, електронну інформаційну систему, у разі заповнення інтерфейсу або шляхом проставлення у відповідному полі відмітки (позначки).

Згода також може бути надана шляхом обрання відповідних технічних налаштувань в інтерфейсі веб-сайта, операційній системі, програмному забезпеченні, чи мобільному додатку, які передбачають обробку персональних даних чи через іншу ствердну дію чи поведінку, яка однозначно вказує на те, що суб’єкт персональних даних в конкретному випадку згоден на подальшу обробку його персональних даних.

Відповідно законопроектом визначено, що не може бути згодою, зокрема дії суб’єкта персональних даних, які не передбачають волевиявлення; встановлені за замовчуванням налаштування веб-сайту, операційної системи, програмного забезпечення, мобільного додатку, в тому числі автоматичне заповнення передбаченої інтерфейсом форми або попереднє проставлення у відповідному полі відмітки (позначки) без безпосередньої участі конкретного суб’єкта персональних даних або ж бездіяльність такого суб’єкта.

Також, у розімінні законопроекту згода не буде вважатися вільною якщо суб'єкт персональних даних знаходиться у залежному чи підпорядкованому становищі відносно контролера, якому надається згода; у суб’єкта персональних даних немає вільного вибору або немає можливості відмовити в наданні згоди або немає можливості відкликати раніше надану згоду, без настання негативних наслідків для себе; у суб’єкта персональних даних відсутні альтернативні шляхи доступу до певних товарів, послуг, соціальних благ тощо, без надання ним згоди на обробку своїх персональних даних або вона не передбачає окремого дозволу суб’єкта персональних даних на окремі види обробки персональних даних, незважаючи на те, що такий дозвіл є необхідним за індивідуальних обставин.

Законопроектом визначено, що не допускається відмова від надання суб’єкту персональних даних товарів, робіт чи послуг на підставі відмови суб’єкта від надання згоди.

А відповідно згода суб’єкта персональних даних на обробку його персональних даних вважається інформованою, якщо до її надання або на момент її надання суб'єкт персональних даних був проінформований про підставу, мету, вид обробки його персональних даних; персональні дані, які підлягають обробці; контактні дані контролера : постійне місце розташування та засоби зв'язку з ними у обсязі, який дозволяє суб'єкту персональних даних ідентифікувати такого контролера та оператора та безперешкодно зв'язатися з ними; права, передбачені законодавством у сфері захисту персональних даних, та способи їх реалізації.

Згода на обробку персональних надається контролеру незалежно від форм та способів її надання, а також згода не може бути підставою для обробки персональних даних суб’єктами владних повноважень, суб’єктами природних монополій, а також підприємствами, установами або організаціями, якщо вони виконують делеговані повноваження суб'єктів владних повноважень згідно із законом чи договором.

Обробка персональних даних здійснюється на підставі згоди суб'єкта персональних даних, відповідний суб’єкт має право відкликати згоду в будь-який час, та згоду на обробку персональних даних малолітньої особи надає її законний представник.

Контролер, у свою чергу відповідно до законопроекту, зобов’язаний вжити всіх розумних заходів для перевірки того, що згода надана суб’єктом персональних даних, який досяг 14 років, а у разі якщо суб’єкт є малолітньою особою, що згода надана від її імені законним представником.

Таким чином, надана згода вважається недійсною з моменту її надання у разі недотримання вимог цієї статті. А обов’язок доведення факту надання суб’єктом персональних даних згоди на обробку його даних з дотриманням вимог, передбачених цією статтею, покладається на контролера [89].

Відповідно до частини 2 статті 7 Закону обробка біометричних персональних даних дозволяється у визначених Законом випадках, а саме:

- у разі надання суб’єктом біометричних персональних даних однозначної згоди на обробку його даних;

- у разі, коли обробка необхідна для здійснення прав та виконання обов'язків володільця у сфері трудових правовідносин відповідно до закону із забезпеченням відповідного захисту;

- у разі, коли обробка необхідна для захисту життєво важливих інтересів суб'єкта персональних даних або іншої особи у разі недієздатності або обмеження цивільної дієздатності суб'єкта персональних даних;

- у разі, коли обробка здійснюється із забезпеченням відповідного захисту релігійною організацією, громадською організацією світоглядної спрямованості, політичною партією або професійною спілкою, що створені відповідно до закону, за умови, що обробка стосується виключно персональних даних членів цих об'єднань або осіб, які підтримують постійні контакти з ними у зв'язку з характером їх діяльності, та персональні дані не передаються третій особі без згоди суб'єктів персональних даних;

- коли необхідна для обґрунтування, задоволення або захисту правової вимоги;

- коли необхідна в цілях охорони здоров’я, встановлення медичного діагнозу, для забезпечення піклування чи лікування або надання медичних послуг, функціонування електронної системи охорони здоров’я за умови, що такі дані обробляються медичним працівником або іншою особою закладу охорони здоров’я чи фізичною особою - підприємцем, яка одержала ліцензію на провадження господарської діяльності з медичної практики, та її працівниками, на яких покладено обов’язки щодо забезпечення захисту персональних даних та на яких поширюється дія законодавства про лікарську таємницю, працівниками центрального органу виконавчої влади, що реалізує державну політику у сфері державних фінансових гарантій медичного обслуговування населення, на яких покладено обов’язки щодо забезпечення захисту персональних даних;

- стосується вироків суду, виконання завдань оперативно-розшукової чи контррозвідувальної діяльності, боротьби з тероризмом та здійснюється державним органом в межах його повноважень, визначених законом;стосується даних, які були явно оприлюднені суб'єктом персональних даних [88].

На нашу думку, відповідного законодавчого регулювання обігу, обробки та захисту саме біометричних персональних даних на національному рівні не достатньо. Саме біометричні персональні дані є найбільш вразливими, та щодо них є найбільший ризик порушень.

## 2.2. Особливості правовідносин у сфері адміністративно-правового забезпечення обігу та захисту біометричних персональних даних

Розвиток інформаційних технологій та збільшення використання біометричних персональних даних у світі охоплює різні сфери життя. На шляху євроінтеграції Україна має зводити національне законодавство до міжнародних вимог, але з урахуванням специфіки ментальності та особливостей правовідносин українців у сфері адміністративно-правового забезпечення обігу та захисту біометричних персональних даних. На сьогодні дослідження відповідних правовідносин є актуальним з огляду на відсутність достатнього законодавчого регулювання обігу та захисту саме біометричних персональних даних, і відповідно дослідивши визначену сферу, ми матимемо змогу запропонувати конкретні законодавчі зміни, які б відповідали міжнародним стандартам.

Насамперед, адміністративно-правові відносини характеризують та визначають як у широкому, так і у вузькому розумінні, а єдність щодо визначення у думках науковців відсутня, але найголовнішим є загально-теоретичне визначення змісту адміністративно-правових відносин, та їх структури у контексті обігу та захисту біометричних персональних даних.

Загалом, на думку Стеценка С. Г. правовідносинами слід вважати результатом впливу правових норм на поведінку суб'єктів, внаслідок якого між ними виникають правові зв'язки [115, с. 80].

У свою чергу Олійник А. Ю. правовідносини визначає як специфічні суспільні відносини, які виникають на підставі норм права, учасники яких є носіями суб'єктивних прав та юридичних обов'язків [69, с. 169].

На думку Горбача А. М. зміст адміністративно-правових відносин, з загально-теоретичної точки зору, складається із суб`єктивних адміністративних прав суб`єктів адміністративного правовідношення та їх юридичних обов`язків. В свою чергу, суб`єктивними адміністративними правами суб`єктів адміністративно-правових відносин є передбачена адміністративно-правовим законодавством міра можливої поведінки учасників адміністративно-правових відносин у контексті задоволення їх публічних інтересів та потреб, що забезпечується певними адміністративними обов`язками інших осіб, а також гарантується державним примусом. А відповідно, юридичні обов`язки і є мірою необхідної поведінки, що має нормативно встановлені межі, а їх реалізація забезпечується нормами адміністративного права та державою. Таким чином змістом адміністративно-правових відносин є фактичні суспільні відносини, які через норми адміністративного права мають закріплену адміністративно-правову форму, визначають адміністративні права та юридичні обов`язки суб`єктів відповідних відносин [26, с. 91-96].

Визначивши зміст адміністративно-правових відносин у загально-теоретичному аспекті, слід перейти до дослідження адміністративно-правових відносин саме у контексті біометричних персональних даних. Насамперед, важливо визначити об'єкт правовідносин, зокрема сферу суспільних відносин – біометричні персональні дані як нематеріальне благо щодо якого суб'єкти даних правовідносин виконують свої права та обов'язки.

У відповідності до Закону України «Про захист персональних даних», об'єктом правовідносин в сфері захисту персональних даних є персональні

дані, що підлягають обробці в базах персональних даних. Персональними даними можна вважати будь які відомості чи сукупність відомостей про фізичну особу, яка ідентифікована або може бути конкретно ідентифікована [88].

Якщо розглядати об'єкт правовідносин як конкретно біометричні персональні дані, слід дати їх визначення. На жаль Закон України «Про захист персональних даних» не містить визначення поняття «біометричні дані», але відповідне визначення поняття закріплене у Роз'ясненні Уповноваженого Верховної Ради України з прав людини від 08.01.2014 р. «Роз'яснення основних положень Порядку повідомлення Уповноваженого щодо визначення обробки персональних даних, яка становить особливий ризик для прав і свобод суб'єктів персональних даних».

На думку Гербута В. С. у контексті дослідження адміністративно-правових відносин у сфері забезпечення захисту та обігу персональних даних, всіх суб'єктів правовідносин у вищезазначеній сфері можна поділити на індивідуальних та колективних, адже на думку науковця суб'єкти даних правовідносин загалом можуть бути як індивідуальними, так і колективними, вони можуть бути і фізичними, і юридичними особами [27, с. 146-149].

Але важливо все ж наголосити, що суб'єкт біометричних персональних даних як обов'язковий учасник вищезгадуваних відносин завжди є індивідуальною фізичною особою. Адже сама сутність та характер даних, носієм яких є фізична особа зосереджується у терміні «персональні».

Досліджуючи ґрунтовніше поняття «персона», «персональний» походить від латинського «persona», що в перекладі означає «особа, людина як окрема особистість» [65, с. 41].

Але відповідна фізична чи юридична особа, що може бути суб'єктом адміністративно-правових відносин у сфері обігу та захисту біометричних персональних даних повинна мати правосуб'єктність.

В свою чергу, правосуб'єктність – це політико-юридичний стан визначеної особи та складається з трьох елементів: правоздатності, дієздатності та деліктоздатності. Кожне з цих трьох елементів слід дослідити.

Насамперед, правоздатність розглядається як загальна (абстрактна) можливість, що визнається державою, а відповідно можливість мати визначені нормативно-правовим актом права і обов'язки, здатність бути їх носієм. Але варто зазначити, що це не є фактичним правоволодінням, а лише можливістю або здатністю до цього. Кожен громадянин України є правоздатним, та в однаковій мірі володіє із всіма громадяни без винятку такою правоздатністю. Правоздатність особа набуває з моменту народження, та припиняється у момент смерті особи [27, с. 146-149].

Наступним складовим елементом правосуб'єктності є дієздатність, яку слід визначати як передбачену нормами права здатність індивіда самостійно, своїми усвідомленими діями здійснювати (виконувати) суб'єктивні юридичні права та обов'язки [49].

Третім елементом правосуб'єктності є деліктоздатність, як здатність нести юридичну відповідальність особи за свої дії [49].

Важливо зупинитись на дослідженні суб'єкта правовідносин у сфері обігу та захисту біометричних персональних даних, та наголосити на тому, що не слід плутати суб'єкта правовідносин та суб'єкта біометричних персональних даних.

Адже відповідно до Закону України «Про захист персональних даних» суб'єктом персональних даних може бути будь-яка фізична особа, стосовно якої відповідно до закону здійснюється обробка її персональних даних [88].

Так як Закон не визначає, хто саме може бути суб'єктом біометричних персональних даних, по аналогії від загального до конкретного зазначаємо, що суб'єктом біометричних персональних даних також може бути будь-яка фізична особа, стосовно якої відповідно до закону здійснюється обробка її персональних даних. А суб'єктом правовідносин, відповідно може бути, як

фізична, так і юридична особа, яка і здійснює обробку біометричних персональних даних.

Слід зупинитись на етапі дослідження суб'єкта правовідносин, адже Закон України «Про захист персональних даних» регламентує детальніше суб'єктів правовідносин, пов'язаних з персональними даними.

По-перше, Закон передбачає володільця бази персональних даних, та визначає останнього як фізичну або юридичну особу, якій законом або за згодою суб'єкта персональних даних надано право на обробку цих даних, яка затверджує мету обробки персональних даних у цій базі даних, встановлює склад цих даних та процедури їх обробки, якщо інше не визначено законом [88].

Тако Закон визначає такого суб'єкта правовідносин як розпорядника бази персональних даних, і визначає останнього як фізичну чи юридичну особу, якій володільцем бази персональних даних або законом надано право обробляти ці дані [88].

Третя особа – це будь-яка особа, за винятком суб'єкта персональних даних, володільця чи розпорядника бази персональних даних та уповноваженого державного органу з питань захисту персональних даних, якій володільцем чи розпорядником бази персональних даних здійснюється передача персональних даних відповідно до закону [27, с. 146-149].

Досліджуючи адміністративно-правові відносини у контексті захисту та обробки персональних даних, де об'єктом є саме біометричні персональні дані, варто визначити яким чином використовуються вищенаведені суб`єти адміністративно-правових відносин саме у цій сфері щодо суб'єктів біометричних персональних даних.

Відповідь міститься у Конвенції Ради Європи «Про захист осіб в зв'язку з автоматизованою обробкою персональних даних». Даний міжнародний документ містить визначення поняття «контролер файлу», та визначає його як фізичну або юридичну особу, державний орган, установу чи будь-який інший орган, що уповноважений відповідно до національного законодавства

вирішувати, яким повинно бути призначення файлу даних для автоматизованої обробки, які категорії персональних даних повинні зберігатися та які операції повинні здійснюватися з ними [53].

Тобто, у випадку обробки чи обігу біометричних персональних даних, у кожному органі, підприємстві, установі, саме визначена особа, у визначений законом чи підзаконними нормативно-правовими актами, спосіб має працювати з біометричними даними осіб.

А проводячи паралелі норми Конвенції з Законом України «Про захист персональних даниї», відповідно визначений «контролер файлу» і є закріпленим Законом «володільцем персональних даних».

А також Конвенція Ради Європи «Про захист осіб в зв'язку з автоматизованою обробкою персональних даних» містить визначений Законом термін «треті особи», хоч і дещо інакше його визначає. У відповідності до Конвенції третіми особами є будь-які фізичні чи юридичні особи, державний орган, агентство чи будь-який інший орган, інший ніж суб'єкт даних, контролер, оператор обробки даних і особи, що, будучи безпосередньо підпорядкованими контролеру чи оператору обробки даних, уповноважені обробляти відповідні дані [100].

І варто зазначити, що якщо Закон України «Про захист персональних даних» третіми особами визначає будь-яких осіб, володільця чи розпорядника бази персональних даних та уповноваженого державного органу, якій володільцем чи розпорядником бази персональних даних здійснюється передача персональних даних відповідно до закону, то Конвенція таких осіб називає «одержувачами», як особами, яким безпосередньо здійснюється передача персональних даних використовується [27, с. 146-149].

Ми переконані, що у законодавця під час розробки Закону України «Про захист персональних даних» не було перешкод прописати певні ключові норми Закону у відповідності до міжнародного законодавства.

Зокрема, Конвенція Ради Європи «Про захист осіб в зв'язку з автоматизованою обробкою персональних даних» була прийнята близько

тридцяти років потому, а всі недоліки та прогалини буди заповнені та доопрацьовані в новіших актах (Директива 95/46/ЄС Європейського Парламенту і Ради «Про захист фізичних осіб при обробці персональних даних і про вільне переміщення таких даних», прийнята в 1995 році) [27, с. 146-149].

Тому вважаємо, що слід привести національне законодавство у відповідності до міжнародного, зокрема визначення ключових термінів, які визначають структуру правосуб'єктності осіб, біометричні персональні дані яких обробляються чи захищаються.

Дослідивши суб'єктний склад, слід дещо більше уваги звернути на сутність і зміст адміністративно-правових відносин у контексті обігу та захисту біометричних персональних даних, зокрема детальніше розглянути нормативне забезпечення використання біометричних персональних даних.

Конституція України у статті 32 забороняє втручання в особисте і сімейне життя людини, крім випадків, передбачених Конституцією України. Не допускається збирання, зберігання, використання та поширення конфіденційної інформації про особу без її згоди, крім випадків, визначених законом, і лише в інтересах національної безпеки, економічного добробуту та прав людини [55].

Але, наявні ті суб'єкти правовідносин, які законом визначаються як такі, що беруть участь у захисті та обігу біометричних персональних даних. Зокрема, мова йде про практично всі органи державної влади та місцевого самоврядування, адже законодавчо мають повноваження, що дотичні до захисту, обігу та обробці біометричних персональних даних.

Також мова йде про Президента України, який відповідно до Конституції України є гарантом дотримання прав та свобод людини та громадянина; про Верховну Раду України, яка через власну законодавчу функцію має виступати гарантом забезпечення прав та свобод людини.

А найголовніше мова йде про Уповноваженого Верховної Ради України з прав людини, який здійснює парламентський контроль за дотриманням законодавства про захист, обіг та обробку біометричних персональних даних

відповідно до Регламенту Європейського Союзу про захист даних та Закону України «Про захист персональних даних».

А також мова йде про органи місцевого самоврядування, які відповідно до Конституції України мають забезпечувати дотримання прав та свобод людини та громадянина на місцевому рівні тощо, а також суди, які у відповідності до Закону України «Про захист персональних даних» разом із Уповноваженим Верховної Ради України з прав людини здійснюють контроль за дотриманням законодавства у сфері обігу, обробки та захисту біометричних персональних даних.

Специфіка та вразливість біометричних персональних даних полягає у неможливості їх зміни, адже це специфічні об'єкти. Зокрема, науковець Emilio Mordini зазначає, що найбільш часто ідентифікація людини відбувається на підставі наступних фізіологічних характеристик: відбитків пальців, сітківки і райдужної оболонки ока, відбитків рук, рис обличчя [136].

На думку науковця Franjiehel Khoury, молекулярна будова ДНК і групу крові є також біометричними персональними даними [137].

Варто наголосити, що одні науковці вважають, що поведінкові дані відносяться безпосередньо до фізіологічних персональних даних, а саме до динамічних біометричних характеристик людини, [6] інші науковці виділяють поведінкові дані в окрему самостійну категорію, що не відноситься до фізіологічних [138, с. 23].

Ми наразі не можемо погодитись із вищезазначеними думками науковців, хоча вони мають право на життя. Відсутність будь-якого законодавчого закріплення поведінкових характеристик як біометричних персональних даних не дає можливості предметно коментувати відповідні думки.

Маються на увазі такі поведінкові характеристики людини, якими можна ідентифікувати людину за манерою його ходи, ведення розмови, підпису, способу друку символів на клавіатурі тощо [139, с. 15]. Незважаючи на те, що зазначений тип даних не може зрівнятися в точності ідентифікації з

біологічними або фізіологічними даними, невирішені питання правового регулювання його використання можуть призвести до зловживань недобросовісними суб'єктами.

Науковець Травкін Ю. В. вважає біометричні персональні дані непридатними для ідентифікації конкретної особи, та пропонує їх не вважати персональними даними, наводячи конкретні приклади.

На думку науковця генетичний код людини можливо змоделювати за допомогою комп'ютера, проте ідентифікувати ці дані з генетичним кодом одного із проживаючих на Землі людей представляється практично неможливим [126, с. 246].

На нашу думку така позиція заслуговує на існування, але це спір щодо того, що можна вважати біометричними даними, а що ні, а предметом нашого дисертаційного дослідження є адміністративно-правове забезпечення обігу та захисту біометричних персональних даних загалом.

Адміністративно-правове регулювання обігу та захисту саме біометричних персональних даних на національному рівні є недостатньо врегульованим і з розвитком інформаційних технологій та інформаційного суспільства потребує нагального врегулювання.

## 2.3. Інструменти адміністративно-правового забезпечення правомірного обігу та захисту біометричних персональних даних

Формування та закріплення на законодавчому рівні інструментів адміністративно-правового забезпечення правомірного обігу і захисту біометричних персональних даних є необхідним аспектом забезпечення ефективного захисту персональних даних, зокрема біометричних персональних даних та відповідно забезпечення ефективного регулювання адміністративно-правового забезпечення правомірного обігу біометричних персональних даних.

Разом із тим, дослідження інструментів адміністративно-правового забезпечення правомірного обігу та захисту біометричних персональних даних дає можливість визначити способи, методи та законодавче регулювання визначеного обігу та захисту.

Відповідні дані набувають статусу персональних даних у випадках, коли в них йдеться про встановлену особу чи, принаймні, особу, яку можна встановити - тобто таку особу, додаткову інформацію про яку можна встановити без необґрунтованих зусиль, і яка дозволяє ідентифікувати відповідну особу (підтвердження, що вона має певну ідентичність та має право здійснювати певні види діяльності) [93].

Біометричні персональні дані як чутливі персональні дані визначено у Конвенції 108 та у Директиві про захист персональних даних, адже біометричні дані потребують посиленого захисту а, отже, є предметом особливого правового режиму, а відповідно потребують і спеціальних інструментів роботи.

Насамперед, дослідження інструментів передбачає спочатку визначення у загальному вигляді поняття «персональні дані», зокрема європейський посібник наводить визначення персональних даних як інформації, що пов’язана з ідентифікацією або можливою ідентифікацією фізичної особи, тобто інформацією про особу, ідентичність якої відкрито встановлена або ж може бути встановлена за допомогою отримання додаткової інформації. Особа, персональні дані якої обробляються, визначається як «суб’єкт персональних даних» [93].

Із наведеного вище визначення, яке передбачає розкриття поняття «персональні дані» у загальному вигляді можна дійсно зробити висновок про універсальність такого визначення. Його універсальність полягає у тому, що дане визначення підходить будь-якому із видів персональних даних, у тому числі і біометричним персональним даним, чого не можна сказати про визначення поняття «персональні дані», що міститься в Законі України «Про захист персональних даних».

Біометричні дані можна розділити на три категорії, залежно від стійкості та відмінності: сильні біометричні дані (відбитки пальців, райдужна оболонка ока), слабкі біометричні дані (голос, ходьба) та м'які біометричні дані (стать, вік). Особливим сегментом біометрії є поведінкова біометрія. Для використання в біометричних системах для цілей ідентифікації або верифікації ці біометричні дані повинні мати певні обов'язкові якості. Ці біометричні дані мають бути універсальними (присутніми у всіх людей), стійкими (якість не змінюється з часом) і унікальними або принаймні відмінними. Ці якості є відносними, а не абсолютними – наприклад, деякі біометричні дані можуть бути більш сприйнятливими до змін, ніж інші. Біометрія зосереджена на ідентифікаторах на основі цих біометричних даних. Ідентифікатори на основі цих біометричних даних зазвичай скануються та передаються в електронну форму, що дозволяє їх обробку електронними інформаційними системами.

Біометричні дані можуть використовуватися в біометрії та біометричних системах. Відповідно до стандарту ISO термін біометрія має використовуватися лише як іменник (як «автоматичне розпізнавання осіб на основі їхніх біологічних і поведінкових характеристик», синонім «біометричного розпізнавання») або як прикметник (як «повинен зробити з біометрією»). Глосарій, розміщений на веб-сайті Європейського інспектора із захисту даних («EPDS»), дає визначення біометрії як «методів однозначного розпізнавання людей на основі однієї або кількох внутрішніх фізичних або поведінкових рис», але поміщає цей термін у контекст захисту персональних даних і пояснює, що ці методи можуть викликати міркування щодо захисту даних, оскільки сьогодні машини можуть розпізнавати людей автоматично й точно. Тоді біометричні системи служать основою для цілей біометричного розпізнавання, яке включає як функції біометричної ідентифікації, так і перевірки (автентифікації).

Необхідно описати, як працює біометрична система, щоб правильно обговорити питання, пов'язані із захистом біометричних даних. Першим етапом біометричної системи є отримання необробленого біометричного зразка від

людини, який є «аналоговим або цифровим представленням біометричних характеристик».

Цей необроблений зразок зазвичай обробляється, і з використанням окремих функцій зразка створюється необоротний шаблон. Тому шаблон містить лише зменшені, унікальні ознаки зразка. Потім шаблон (або безпосередньо зразок, залежить від структури зберігання біометричної системи) зберігається для довідки централізованим або децентралізованим способом. Він використовується як еталон для порівняння в процесі ідентифікації/автентифікації, де поданий зразок порівнюється зі збереженим зразком/шаблоном. Результат ґрунтується на ймовірності, оскільки немає двох абсолютно однакових зразків від однієї людини. Розраховується оцінка подібності та приймається рішення щодо ідентифікації/автентифікації.

Біометричні дані, у технічному сенсі, створюються шляхом вимірювання біометричних характеристик. Біометричні характеристики вимірюються, обробляються та отримуються так звані біометричні зразки (наприклад, графічне зображення відбитка пальця або райдужної оболонки ока). Ці зразки зазвичай не зберігаються, оскільки вони становлять високий ризик для суб'єктів даних, про яких вони містять конфіденційну інформацію. Тому зразки зазвичай перетворюються на біометричні шаблони. У типовій біометричній системі використовуються шаблони, які містять лише найбільш відмітні характеристики, які можна використовувати для верифікації та ідентифікації. Шаблон може зберігатися на скануючому пристрої або на пристрої, який має суб'єкт даних (наприклад, картка), або в центральній базі даних, залежно від характеру та призначення конкретної біометричної системи.

Характер і кількість інформації, включеної в шаблон, мають бути достатньо великими, щоб підтримувати достатній рівень безпеки та уникнути помилок точності, але не настільки великими, щоб дозволити можливу реконструкцію необроблених даних. В принципі, процес створення біометричного шаблону з необроблених даних має бути одностороннім і незворотнім. Однак біометричні системи не ідентифікують самих осіб – вони

завжди порівнюють надану інформацію з іншою інформацією. Від характеру порівняння залежить, чи особу аутентифіковано чи ідентифіковано. Розрізнення між системами автентифікації та ідентифікації має вирішальне значення для визначення ризиків для суб'єктів даних, а також може впливати на правовий режим, що регулює обробку біометричних даних.

З огляду на практику Європейського суду з прав людини та загалом європейського законодавства протягом останніх років ЄС напрацювали значну кількість захисних інструментів щодо персональних даних фізичної особи, про що свідчать предметні Рішення Європейського суду з прав людини. Нажаль відповідна судова практика відсутня на національному рівні, тому пропонуємо взяти до уваги та належним чином дослідити саме ті акти, які належним чином регулюють досліджуване питання.

Зважаючи на положення Директиви про захист персональних даних та на судову практику Європейського суду з прав людини, не важлива форма зберігання чи використання біометричних персональних даних, адже форма не має відношення до застосовності законодавства про захист персональних даних.

Письмовий або усний формат передачі даних може містити персональну інформацію та зображення, включаючи дані, записані за допомогою замкнутої системи ТВ-спостереження (CCTV) або звукові дані. Персональними даними може бути інформація як з електронного, так і з паперового носія; навіть зразки клітин тканини людини можуть бути персональними даними, оскільки містять ДНК людини [32].

Відповідно до ст.. 6 Конвенції 108 та ст.. 8 Директиви про захист персональних даних біометричні персональні дані є особливою категорією персональних даних, які за своєю природою можуть становити загрозу для суб'єктів, персональні дані яких обробляються, і потребують посиленого захисту.

Міжнародні документи передбачають необхідність отримання дозвілу на обробку цих особливих категорій даних («чутливих») лише з особливими

гарантіями. Важливо, що такі біометричні персональні дані міжнародні документи, на відміну від національного законодавства, перелічують, а саме мова йде про:

– персональні дані, які розкривають расове чи етнічне походження;

– персональні дані, які розкривають політичні, релігійні чи інші переконання; та

– персональні дані, які стосуються здоров'я або статевого життя [53].

Дослідження обробки особливого виду персональних даних як біометричні дані є актуальним адже, це одне із основних питань у контексті дослідження забезпечення інструментарію адміністративно-правового забезпечення правомірного обігу та захисту біометричних персональних даних.

Сьогодні, у процесі розвитку інформаційних технологій, коли мова йде про обробку персональних даних, загалом мається на увазі автоматизований процес обробки персональних даних. Але практика обробки персональних даних Європейського Союзу передбачає не лише автоматизовану обробку персональних даних, а і ручну, [93] зокрема як і національна практика.

Процес захисту персональних даних відповідно до міжнародного законодавства здійснюється також в основному на процесі автоматизованої обробки персональних даних [93].

Конвенція 108 Ради Європи Про захист осіб у зв'язку з автоматизованою обробкою їх персональних даних врегульовує процес обробки даних, які зберігаються у файлах для автоматизованої обробки [53].

Важливо зазначити, що положення Конвенції передбачають можливість поширення у національному законодавстві процедури захисту на процес ручної обробки, але скориставшись цією можливістю про останнє держави-члени мають повідомляти про це у своїх заявах на ім'я Генерального Секретаря Ради Європи [53].

Також у міжнародному законодавстві наводиться визначення поняття «обробка персональних даних», воно визначається як будь-яка операція, здійснювана з персональними даними, така, як збір, реєстрація, організація, зберігання, адаптація чи зміна, пошук, консультація, використання, розкриття за допомогою передачі, поширення чи іншого надання, упорядкування чи комбінування, блокування, стирання чи знищення» [53].

А в свою чергу, поняття «обробка» визначається як дії, в результаті яких персональні дані виходять з-під відповідальності одного володільця і передаються під відповідальність іншого [93].

У загальному продублюємо суб'єктний склад, який зазначався у попередньому підрозділі дисертаційної роботи, зокрема «володільцем» є той, хто вирішує обробляти персональні дані інших осіб відповідно до Закону України «Про захист персональних даних»; якщо таке рішення приймається декількома особами, вони можуть бути «спільними володільцями» у відповідності до міжнародного законодавства [93].

Особа, яка від імені володільця у порядку визначеному чинним законодавством обробляє персональні дані є «розпорядником».

Розпорядник стає володільцем, якщо він або вона використовують персональні дані у власних цілях і не дотримуються вказівок володільця, і загалом будь-хто, хто отримує дані від володільця, є «розпорядником». В свою чергу, «третя особа» – це фізична або юридична особа, яка не виконує вказівки володільця (і не є суб'єктом персональних даних), а «розпорядник – третя особа» – це фізична або юридична особа, яка юридично відокремлена від володільця, але отримує персональні дані від володільця [93].

У контексті дослідження процедури здійснення обробки біометричних персональних даних, їх обігу чи навіть захисту є необхідним один важливий елемент – згода.

Згода як правова основа для обробки персональних даних має бути вільно вираженою, поінформованою та висловленою окремо. Якщо для звичайних персональних даних форма надання згоди – це прямо надана

особою згода, або шляхом дій, які не залишають сумнівів у тому, що суб'єкт персональних даних погоджується на обробку своїх даних; то для біометричних персональних даних форма згоди – це обов'язково чітко висловлена згода.

У відповідності до ст. 8 Директиви Про захист персональних даних згоду може бути відкликано в будь-який момент, а з наведеного у міжнародному документі визначення поняття «згода» випливає, що остання є «будь-яким вільним, окремим та поінформованим висловленням бажання суб'єктом персональних даних; у більшості випадків є правовою підставою для законної обробки персональних даних» [33].

В Україні законодавчий інструментарій стосовно захисту, обігу та обробки біометричних персональних даних як елемента прав особи відбувається достатньо повільно, зокрема наразі порядок роботи з біометричними персональними даними як із спеціальним видом персональних даних закріплений лише у Роз`ясненнях Уповноваженого Верховної Ради України з прав людини.

Судова практика у контексті розгляду справ з таким елементом як біометричні персональні дані не суттєва на національному рівні, і передбачає використання судової практики Європейського суду з прав людини, а у контексті національної практики ґрунтується на принципі переважного забезпечення прав володільця баз даних.

Разом із тим, варто визначити повноваження Уповноваженого Верховної Ради України з прав людини, які також є своєрідним інструментом адміністративно-правового забезпечення правомірного обігу і захисту біометричних персональних даних, адже пунктом 7 частини першої статті 3 Закону України «Про Уповноваженого Верховної Ради України з прав людини» останній уповноважений здійснювати парламентський контроль за використанням персональних даних та зокрема біометричних персональних даних [73].

Так само, Уповноважений Верховної Ради України гарантує безпеку обігу та оброблення персональних даних, контролює захист біометричних персональних даних тощо.

На нашу думку, сьогодні Уповноважений Верховної Ради України має цілу низку повноважень, які слід визначати як інструменти не тільки захисту персональних даних, а і інструментами адміністративно-правового забезпечення правомірного обігу і захисту біометричних персональних даних, які реалізуються через контроль та перевірки.

Проект Закону України «Про захист персональних даних» (реєстраційний № 5628 від 07.06.2021), про який йшла мова у попередніх підрозділах дисертаційної роботи пропонує велику кількість ефективних новел.

Запропонований законопроект відповідно до частин третьої, четвертої статті 1 визначає, що дія закону не поширюється на обробку персональних даних фізичними особами для особистих чи побутових потреб. Зокрема, визначається щодо яких особистих та побутових потреб, а саме ведення кореспонденції та збереження поштових (електронних) адрес, підтримання соціальних контактів, а також комунікація у мережі Інтернет, яка здійснюється в контексті такої діяльності. Однак, важливо наголосити, що саме через такі побутові використання даних, зокрема шляхом внесення їх до смартфону чи компьютера, особа в мережі Інтернет ризикує надати доступ до незаконного їх використання.

Запропоноване законопроектом визначення поняття біометричних даних не деталізує, який саме перелік даних захищається у розумінні відповідного законопроекту.

Законопроектом пропонується також удосконалити визначення поняття знеособлення персональних даних шляхом заміни звичайного вилучення на комплекс заходів щодо незворотнього вилучення із сукупності даних про фізичну особу та/або щодо незворотного розірвання будь-якого зв`язку між інформацією та фізичною особою, що на нашу думку є ефективним

удосконаленням визначення знеособлення персональних даних, адже визначається також певний алгоритм зазначеного знеособлення.

Також, серед ряду новер, законопроектом запропоновано визначити поняття послуги інформаційного суспільства як оплатного чи безоплатного надання будь-яких товарів, робіт і послуг на вимогу їхнього отримувача на підставі правочину, укладеного за допомогою засобів дистанційного зв'язку або поза торговельними або офісними приміщеннями, в тому числі інформаційними електронними послугами.

Також, законопроектом запропоновано затвердити визначення поняття псевдонімізація, тож псевдонімізація визначається як обробка персональних даних у спосіб, що не дозволяє ідентифікацію суб'єкта персональних даних без використання додаткової інформації, яка повинна зберігатися окремо із вжиттям усіх необхідних технічних та організаційних заходів, які не дають можливості відтворити зв'язок із суб'єктом персональних даних або ідентифікувати його.

Разом із тим, законопроектом запропонована ще одна новела, та визначається поняття широкомасштабна обробка персональних даних як обробка значних обсягів персональних даних на регіональному, національному або міжнародному рівнях, яка може мати вплив на значну кількість суб'єктів персональних даних та яка може призвести до ризиків високого ступеню для їх прав та свобод.

Важливими інструментами адміністративно-правового забезпечення правомірного обігу і захисту біометричних персональних даних, окрім національного законодавства, зокрема міжнародних договорів, декларацій тощо, повноважень контролюючих та перевіряючих органів, зокрема Уповноваженого Верховної Ради України з прав людини мають бути ще і ті інструменти, які продиктовані тими, чиї біометричні персональні дані слід захищати. Особи мають робити усе можливе, щоб їхнє право на захист біометричних персональних даних не було порушене.

Національне законодавство слід удосконалювати та доповнювати, національній правовій системі не вистачає ефективного інструментарію забезпечення обігу, обробки та захисту біометричних персональних даних.

Тому, з огляду на вищезазначене пропонуємо внести зміни до Закону України «Про захист персональних даних» шляхом зазначення загального порядку роботи з особливими видами персональних даних, та окремо щодо кожного, зокрема з біометричними персональними даними.

Вважаємо за необхідне передбачити в Законі України «Про захист персональних даних» які біометричні персональні дані взагалі не підлягають збиранню, вказати їх перелік, адже із значним розвитком інформаційного суспільства важко уявити, які біометричні персональні дані особи збиратимуться через рік, а переліку заборонених до збирання біометричних даних, або дозволених до збирання біометричних персональних даних у Законі України «Про захист персональних даних» нема.

## Висновки до розділу 2

Дослідивши нормативниі засади адміністративно-правового забезпечення обігу та захисту біометричних персональних даних, було визначено, що національне законодавство, у контексті піднятого питання регулює Конституція України, Закон України «Про захист персональних даних» та частково інші нормативно-правові акти.

Було визначено, що адміністративно-правовим забезпеченням є здійснення державою за допомогою правових норм, приписів і сукупності засобів упорядкування суспільних відносин, їх юридичне закріплення, охорона, реалізація та розвиток.

Міжнародне законодавство регламентує забезпечення умов та обмежень у контексті роботи з біометричними даними, адже саме біометричні персональні дані є спеціальною категорією персональних даних.

Міжнародне законодавство містить застереження щодо того, що створивши умови та обмеження по роботі з біометричними персональними даними держави-члени не мають права перешкоджати вільному потоку персональних даних в межах Союзу тоді, коли такі умови застосовують до транскордонного опрацювання таких даних; а також держави-члени мають зберегти професійну таємницю, для певних цілей, пов’язаних із здоров’ям у роботі з біометричними персональними даними.

Обробка біометричних даних має серйозні наслідки для конфіденційності індивідуумів не тільки через їхню здатність бути пов’язаними з індивідуумом, а й тому, що біометричні дані можна аналізувати для отримання додаткової інформації, безпосередньо пов’язаної з їх ідентичністю, психічним і біологічним функціонуванням, а також прогнозом цього функціонування. Законодавці усвідомлюють чутливість і шкідливий потенціал біометрії даних та можуть взагалі заборонити їх обробку, однак ця заборона може бути скасованою за згодою суб’єкта даних, до якого відносяться біометричні дані. Наприклад, користувачі смартфонів часто готові надати свою згоду

контролерам. Це іноді через необізнаність про можливі наслідки збору та обробки цього дані можуть впливати на їх конфіденційність і життя. На жаль, рівень необізнаності зростає.

Автоматизована обробка персональних даних за своєю суттю є непрозорою. Незважаючи на те, що Загальний регламент захисту даних вимагає прозорості обробки персональних даних і вимагає призначення уповноваженого із захисту даних, існує висока ймовірність того, що останній не буде дотримуватись малими компаніями чи фізичними особами, або що законодавство можна буде обійти. На даний момент єдиний істинно ефективний засіб захисту біометричних даних від потенційного аналізу для отримання додаткової інформації знаходяться в руках суб'єктів даних, які повинні або ретельно вибирати надійні компанії або уникати використання біометрії. У деяких випадках, наприклад, з пристроями, які належать даним суб'єкти (тобто смартфони чи ноутбуки), суб'єкти даних можуть використовувати незалежно розроблене програмне забезпечення, яке б перевіряло фактичну роботу програмного забезпечення, яке керує біометричними датчиками.

Ми дійшли проміжного висновку, що законодавчого регулювання обігу, обробки та захисту саме біометричних персональних даних на національному рівні не достатньо, адже біометричні персональні дані є найбільш вразливими, та щодо них є найбільший ризик порушень, про що свідчать і такі думки науковців.

Адміністративно-правове регулювання обігу та захисту саме біометричних персональних даних на національному рівні є недостатньо врегульованим і з розвитком інформаційних технологій та інформаційного суспільства потребує нагального врегулювання.

Зміст адміністративно-правових відносин складається із суб'єктивних адміністративних прав суб'єктів адміністративного правовідношення та їх юридичних обов'язків.

Суб’єктивними адміністративними правами суб’єктів адміністративно-правових відносин є передбачена адміністративно-правовим законодавством міра можливої поведінки учасників адміністративно-правових відносин у контексті задоволення їх публічних інтересів та потреб, що забезпечується певними адміністративними обов’язками інших осіб, а також гарантується державним примусом.

А юридичні обов’язки і є мірою необхідної поведінки, що має нормативно встановлені межі, а їх реалізація забезпечується нормами адміністративного права та державою.

Таким чином змістом адміністративно-правових відносин є фактичні суспільні відносини, які через норми адміністративного права мають закріплену адміністративно-правову форму, визначають адміністративні права та юридичні обов’язки суб’єктів відповідних відносин.

Об`єктом адміністративно-правових відносин у сфері захисту та обігу біометричних персональних даних і є самі біометричні дані - сукупність даних, що були зібрані на основі фіксації характеристик визначеної особи, які відповідно є стабільними та унікальними (відцифрований підпис особи та/або образ обличчя, відбитки пальців, малюнок сітківки ока тощо).

Суб’єктний склад даних правовідносин становлять суб'єкт персональних даних, володілець бази, розпорядник бази даних; третя особа, уповноважений відповідного державного органу, інші державні органі чи органи місцевого самоврядування, які функціонують у відповідній сфері.

Суб’єкт біометричних персональних даних як обов’язковий учасник вищезгадуваних відносин завжди є самеіндивідуальною фізичною особою.

Адже сама сутність та характер даних, носієм яких є фізична особа зосереджується у терміні «персональні», так само «персона», «персональний» походить від латинського «persona», що в перекладі означає «особа, людина як окрема особистість».

Фізична чи юридична особа, що може бути суб’єктом адміністративно-правових відносин у сфері обігу та захисту біометричних персональних даних

повинна мати правосуб'єктність (політико-юридичний стан визначеної особи та складається з трьох елементів: правоздатності, дієздатності та деліктоздатності).

Не слід плутати суб'єкта правовідносин та суб'єкта біометричних персональних даних, адже суб'єктом персональних даних може бути будь яка фізична особа, стосовно якої відповідно до закону здійснюється обробка її персональних даних.

Конституція України у статті 32 забороняє втручання в особисте і сімейне життя людини, крім випадків, передбачених Конституцією України.

Не допускається збирання, зберігання, використання та поширення конфіденційної інформації про особу без її згоди, крім випадків, визначених законом, і лише в інтересах національної безпеки, економічного добробуту та прав людини, але, наявні ті суб'єкти правовідносин, які законом визначаються як такі, що беруть участь у захисті та обігу біометричних персональних даних.

Протягом останніх років ЄС напрацювали значну кількість захисних інструментів щодо персональних даних фізичної особи, про що свідчать предметні Рішення Європейського суду з прав людини. Нажаль відповідна судова практика відсутня на національному рівні, тому пропонуємо взяти до уваги та належним чином дослідити саме ті акти, які належним чином регулюють досліджуване питання.

Відповідно до ст.. 6 Конвенції 108 та ст.. 8 Директиви про захист персональних даних біометричні персональні дані є особливою категорією персональних даних, які за своєю природою можуть становити загрозу для суб'єктів, персональні дані яких обробляються, і потребують посиленого захисту.

Міжнародні документи передбачають необхідність отримання дозвілу на обробку цих особливих категорій даних («чутливих») лише з особливими гарантіями.

Процес захисту персональних даних відповідно до міжнародного законодавства здійснюється також в основному на процесі автоматизованої обробки персональних даних.

Положення Конвенції передбачають можливість поширення у національному законодавстві процедури захисту на процес ручної обробки, але скориставшись цією можливістю про останнє держави-члени мають повідомляти  про це у своїх заявах на ім'я Генерального Секретаря Ради Європи.

У відповідності до міжнародного законодавства поняття «обробка персональних даних» визначається як будь-яка операція, здійснювана з персональними даними, така, як збір, реєстрація, організація, зберігання, адаптація чи зміна, пошук, консультація, використання, розкриття за допомогою передачі, поширення чи іншого надання, упорядкування чи комбінування, блокування, стирання чи знищення.

Поняття «обробка» визначається як дії, в результаті яких персональні дані виходять з-під відповідальності одного володільця і передаються під відповідальність іншого.

Необхідним елементом у контексті дослідження процедури здійснення обробки біометричних персональних даних є згода, вона як правова основа для обробки персональних даних має бути вільно вираженою, поінформованою та висловленою окремо.

Якщо для звичайних персональних даних форма надання згоди – це прямо надана особою згода, або шляхом дій, які не залишають сумнівів у тому, що суб'єкт персональних даних погоджується на обробку своїх даних; то для біометричних персональних даних форма згоди – це обов'язково чітко висловлена згода.

У час пандемії, з 2019 року, припав період найбільшого розвитку інформаційного розвитку державних адміністративно-правових процесів. Відповідний стан речей спровокував ефективніше використання електронних сервісів, а оцифрування державних послуг набуло нових обертів в Україні,

адже особам, які бажали отримати державну послугу саме у час пандемії зручніше було скористатись електронною можливістю подати заяву тощо, ніж виходити на вулицю [28; 66; 128].

Відповідне, на нашу думку є однією із передумов, пришвидшення оцифрування державних сервісів та ефективним сприйняттям відповідного населенням, про що стверджують і інші науковці у сфері інформаційного права в Україні [134, с. 135-141].

Мобільний додаток «Дія», який курує Міністерство цифрової трансформації та державне підприємство «Дія», наразі надає близько ста послуг, які колись фізичні особи мали отримувати шляхом фактичного подання документів нарочно чи поштою до державних органів влади чи органів місцевого самоврядування. Саме з 2019 року розпочався розвиток відповідного мобільного додатку [36; 37].

Судова практика у контексті розгляду справ з таким елементом як біометричні персональні дані майже відсутня на національному рівні, і передбачає використання судової практики Європейського суду з прав людини.

Національне законодавство слід удосконалювати та доповнювати, адже Роз`яснення Уповноваженого Верховної Ради України з прав людини не достатньо для забезпечення ефективного порядку обробки, обігу та захисту біометричних персональних даних, як особливого виду персональних даних.

Тому, з огляду на вищезазначене пропонуємо внести зміни до Закону України «Про захист персональних даних» шляхом зазначення загального порядку роботи з особливими видами персональних даних, та окремо щодо кожного, зокрема з біометричними персональними даними.

Також важливо в Законі України «Про захист персональних даних» як в профільному нормативно-правовому акті передбачити загалом, які біометричні персональні дані взагалі не підлягають збиранню, вказати їх перелік, адже із значним розвитком інформаційного суспільства важко уявити, які біометричні персональні дані особи збиратимуться через рік, а переліку

заборонених до збирання біометричних даних, або дозволених до збирання біометричних персональних даних у Законі України «Про захист персональних даних» нема.

# РОЗДІЛ ІІІ. ОСОБЛИВОСТІ АДМІНІСТРАТИВНО-ПРАВОВОГО ЗАБЕЗПЕЧЕННЯ ОБІГУ ТА ЗАХИСТУ БІОМЕТРИЧНИХ ПЕРСОНАЛЬНИХ ДАНИХ ОКРЕМИМИ СУБ`ЄКТАМИ ПРАВОЗАСТОСОВЧОЇ ДІЯЛЬНОСТІ

## 3.1. Адміністративно-правове забезпечення правомірного обігу та захисту права на конфіденційність біометричних персональних даних Уповноваженим Верховної Ради України з прав людини: процедури, засоби та умови реалізації

Процедура, засоби та умови реалізації адміністративно-правового забезпечення обігу та захисту біометричних персональних даних з боку Уповноваженого Верховної Ради України є надзвичайно важливим та актуальним питанням у контексті дослідження інституту біометричних персональних даних.

У контексті обробки та захисту біометричних персональних даних слід звернути увагу на Конвенцію про захист осіб у зв’язку з автоматизованим обробленням персональних даних та додатковий протокол до неї, яка була ратифікована Верховною Радою України у 2010 році, адже даний міжнародний документ регулює відносини у зв’язку з автоматизованим обробленням персональних даних [51].

Відповідно до ст. 32 Конституції України ніхто не може зазнавати втручання в його особисте і сімейне життя, крім випадків, передбачених Конституцією України [55].

Не допускається збирання, зберігання, використання та поширення конфіденційної інформації про особу без її згоди, крім випадків, визначених законом, і лише в інтересах національної безпеки, економічного добробуту та прав людини.

Кожний громадянин має право знайомитися в органах державної влади, органах місцевого самоврядування, установах і організаціях з відомостями про себе, які не є державною або іншою захищеною законом таємницею.

Кожному гарантується судовий захист права спростовувати недостовірну інформацію про себе і членів своєї сім'ї та права вимагати вилучення будь-якої інформації, а також право на відшкодування матеріальної і моральної шкоди, завданої збиранням, зберіганням, використанням та поширенням такої недостовірної інформації.

Лише п. 7 ч. 1 статті 3 Закону України «Про Уповноваженого Верховної Ради України з прав людини» закріплює за Омбудсменом як складову парламентського контролю сприяння правовій інформованості населення та захист конфіденційної інформації про особу [73].

Закон не містить визначення поняття «персональні дані» або поняття «біометричні персональні дані», виокремлюючи останні лише видом даних.

Уповноважений Верховної Ради України є гарантом безпеки обігу та оброблення персональних даних та має низку повноважень у сфері контролю за захистом персональних даних, у тому числі і біометричних персональних даних.

Згідно із статтею 23 Закону України «Про захист персональних даних» Уповноважений Верховної Ради України у сфері захисту персональних даних має, зокрема, наступні повноваження:

– отримує звернення на предмет порушення особами права на захист персональних даних, розглядає такі звернення, та приймає рішення його врегулювання проблемних питань у межах своїх повноважень, визначених чинним законодавством України;

– затверджує нормативно-правові акти у сфері захисту персональних даних у випадках, передбачених Законом України «Про захист персональних даних»;

– видає обов’язкові до виконання приписи, вимоги, за підсумками перевірки, що мають на меті усунути порушення законодавства про захист

персональних даних. За результатами таких приписів персональні дані можуть бути змінені, видалені або знищені, а їх обробка може бути припинена або зупинена, а доступ до них може бути обмежений;

– взаємодіє із структурними підрозділами або відповідальними особами, що мають відношення до обробки чи захисту персональних даних;

– звертається із пропозиціями до Верховної Ради України, Президента України, Кабінету Міністрів України, інших державних органів, місцевого самоврядування, їх посадових осіб щодо прийняття або внесення змін до нормативно-правових актів з питань захисту персональних даних;

– інформує про актуальні питання, зміни, чинне законодавство у сфері захисту персональних даних, проблеми його практичного застосування, права і обов'язки суб'єктів відносин;

– здійснює моніторинг нових практик, тенденцій, технологій захисту персональних даних;

– організовує та забезпечує взаємодію з іноземними суб'єктами відносин, пов'язаних із персональними даними, у тому числі у зв'язку з виконанням Конвенції про захист осіб у зв'язку з автоматизованою обробкою персональних даних та Додаткового протоколу до неї, інших міжнародних договорів України у сфері захисту персональних даних;

– бере участь у роботі міжнародних організацій з питань захисту персональних даних [88].

Під час здійснення своєї щорічної доповіді Уповноважений Верховної Ради України з прав людини доповідає про стан додержання та захисту прав і свобод людини і громадянина в Україні, зокрема про стан додержання законодавства у сфері захисту персональних даних.

Різак М. В. у своїй науковій статті, присвяченій саме дослідженню діяльності Уповноваженого Верховної Ради України у сфері захисту персональних даних пропонує класифікувати функції Уповноваженого Верховної Ради України на наступні:

– розпорядчі (видача приписів за результатами розгляду звернень у контексті захисту персональних даних);

– рекомендаційні (надання рекомендацій у контексті організації роботи щодо обігу, обробки чи захисту персональних даних);

– контрольні (розгляд скарг та пропозицій; проведення перевірок; отримання доступу до необхідної інформації; складення протоколів про притягнення до відповідальності);

– представницькі (взаємодія із структурними підрозділами або відповідальними особами; міжнародне співробітництво);

– погоджувальні (надання висновків щодо проектів кодексів поведінки у сфері захисту персональних даних, обігу та їх оброблення, за зверненням заінтересованих осіб);

– нормотворчі (затвердження нормативно-правових актів у сфері безпеки обігу та обробки персональних даних у відповідності до чинного законодавства України);

– інформаційні (інформування про зміни в законодавстві, здійснення моніторингу нових практик, тенденцій, технологій у відповідній сфері) [102].

На нашу думку, автор виділив занадто багато підстав до класифікації повноважень Уповноваженого Верховної Ради України у контексті обігу, обробки та захисту персональних даних, адже деякі підстави до класифікації містили лише одне повноваження, передбачене ст. 23 Закону України «Про захист персональних даних».

У контексті обробки, обігу та захисту саме біометричних персональних даних, стаття 23 Закону не передбачає конкретних повноважень Уповноваженого Верховної Ради України з прав людини, адже можна вищезазначені повноваження використовувати лише по аналогії від загального - персональних даних.

Враховуючи специфіку біометричних персональних даних, було б доцільним Уповноваженого Верховної Ради України з прав людини наділити ще таким повноваженням як надання висновків щодо можливості

застосування тих чи інших біометричних технологій до людини, перед тим, як вони будуть введені в законодавчий та практичний обіг, адже повноваження у сфері контролю за використанням за захистом біометричних персональних даних для Уповноваженого Верховної Ради України з прав людини мають певну специфіку.

Велика кількість технологій, що застосовуються для ідентифікації людини, зокрема біометричні персональні дані, можуть шкодити здоров'ю людини, або встановлювати тотальний контроль, що порушуватиме право людини на приватне життя, гарантоване Конституцією України.

Таким чином висновок Уповноваженого Верховної Ради України з прав людини має бути врахований на предмет того, чи можна вводити ту чи іншу технологію ідентифікації людини перед її введенням в практичний обіг.

А також у випадку звернень чи скарг щодо порушення права людини у контексті обробки, тощо біометричних персональних даних, для перевірки відповідної інформації Уповноважений Верховної Ради України з прав людини просто зобов'язаний залучати експерта у подібних перевірках, адже не може мати достатньо знань щоб об'єктивно і фахово перевірити чи наявні порушення у сфері обігу, обробки чи захисту біометричних персональних даних [132, с. 194–199].

У контексті дослідження ролі Уповноваженого Верховної Ради України з прав людини у захисті біометричних персональних даних, слід виділити саме контролюючі повноваження.

Згідно ст. 22 Закону України «Про захист персональних даних» контроль за дотриманням законодавства у сфері обігу, обробки та захисту персональних даних, окрім Уповноваженого Верховної Ради України з прав людини здійснюють також суди [88].

Але слід зазначити, що саме суди здійснюють контроль лише через реалізацію свого правосуддя, тоді, коли Омбудсмен напряму за заявою особи, або з власної волі, має право реалізовувати контрольні, наглядові, розпорядчі, тощо, повноваження.

Уповноважений Верховної Ради України з прав людини також має власний секретаріат, який складається з відповідних структурних підрозділів, що виконують поставлені перед ними завдання.

Департамент з питань захисту персональних даних, що знаходиться в секретаріаті Уповноваженого Верховної Ради України з прав людини і є тим структурним підрозділом, який проводить перевірки, складає проекти нормативно-правових актів, проекти постанов, проекти рекомендацій, і займається моніторингом нових тенденцій, технологій, тощо [71].

Відповідно до Роз'яснення до Порядку здійснення Уповноваженим контролю за додержанням законодавства про захист персональних даних № 0002715-14, в редакції від 08.01.2014 Уповноважений Верховної Ради України з прав людини (далі - Уповноважений), окрім інших функцій, здійснює контроль за додержанням законодавства про захист персональних даних.

З цією метою Уповноваженим за скаргами юридичних та фізичних осіб, а також за власною ініціативою проводяться перевірки додержання законодавства про захист персональних даних [103].

Відповідно до цього порядку, скарга особи, яка звертається до Уповноваженого також має відповідати певним вимогам, зокрема має бути обґрунтованою, повинна містити інформацію щодо історії виникнення проблемного питання, фактів, що свідчать про порушення прав, сутність вчиненого порушення, а також інформацію щодо заходів, вжитих з метою виправлення порушення, зокрема скарг, направлених до інших органів [103].

А також найголовнішим є те, що викладені у скарзі обставини мають бути підкріпленими реальними доказами, які прикріплюються до скарги додатками, як копії тих чи інших документів, чи як роздруківка електронного джерела, сайту, сторінки тощо.

Як звернення, так і скарги слід подавати Уповноваженому у письмовій формі, що на нашу думку є неефективним, адже коли мова йде про порушення обігу, обробки чи захисту персональних даних, великий відсоток який на жаль здійснюється саме через мережу інтернет, на офіційній веб-сторінці

Уповноваженого має бути електронний розділ, куди людина може надіслати, або залишити на сторінці свою скаргу чи звернення, залишивши свої контактні дані для зворотного зв'язку.

Уповноважений ВРУ з прав людини, як контролюючий орган у сфері обігу, обробки та захисту персональних даних особи, зокрема біометричних персональних даних, має вживати заходів щодо швидкого оповіщення особи про порушення щодо неї, адже має секретаріат, який може взяти на себе функцію моніторингу звернень і скарг на офіційній веб-сторінці.

Тому, відповідно ми вважаємо, що запровадження електронної форми звернень і скарг на офіційній сторінці Уповноваженого Верховної Ради України з прав людини є необхідним елементом забезпечення ефективного контролю та нагляду за дотриманням законодавства у сфері обігу, обробки та захисту персональних даних, а найголовніше біометричних персональних даних особи.

Законодавство України не позбавляє особу права одночасно подати заяву чи скаргу до Уповноваженого, та до суду.

Але, вищезазначений Порядок, який регулює дії Уповноваженого, процедурно надає можливість Уповноваженому зупиняти провадження по справі, коли останньому стає відомо про наявність відкритого судового провадження у цій самій справі [103].

На нашу думку, це є неприпустимим, адже Порядок здійснення Уповноваженим контролю за додержанням законодавства про захист персональних даних № 0002715-14, в редакції від 08.01.2014 не має вищої юридичної сили ніж закони України, і якщо чинне законодавство прямо не забороняє особі звертатись із заявою одночасно і до суду, і до Уповноваженого, то Уповноважений не має законних підстав зупиняти провадження у справі, дізнавшись про відкрите судове провадження у відповідній справі. На нашу думку, слід прописати в Законі України «Про Уповноваженого Верховної Ради України» норму, яка б прямо забороняла

Уповноваженому зупиняти провадження у зв’язку із розглядом відповідної справи у суді.

У контексті дослідження повноважень Уповноваженого Верховної Ради України з прав людини у сфері контролю за дотриманням законодавства щодо обігу, обробки та захисту персональних даних пропонуємо звернути увагу на Лист Уповноваженого Верховної Ради України з прав людини «Щодо захисту персональних даних» від 03.03.2014 року № 2/9-227067.14-1/НД-129 (далі - Лист), у якому надаються рекомендації щодо механізму контролю судів за додержанням законодавства про захист персональних даних у межах повноважень, передбачених законом; щодо необхідності отримувати згоду на обробку персональних даних; щодо визначення «особливого ризику для прав і свобод суб'єктів персональних даних»; щодо здійснення захисту персональних даних, про обробку яких повідомляти Уповноваженого не потрібно тощо [60].

Проаналізувавши даний Лист, ми зробили для себе висновок, що він фактично є дублюванням норм Закону України «Про захист персональних даних» та відповідно Кодексу України про адміністративні правопорушення тощо.

А регулювання питання захисту, обігу та обробки біометричних персональних даних у даному документі зводиться виключно до зазначення поняття «біометричні дані» у переліку персональних даних, що несуть особливий ризик для прав і свобод суб’єктів персональних даних.

На нашу думку, підзаконні нормативно-правові акти, зокрема як процитований Лист, навпаки мають не стільки дублювати положення закону, як глибше та детальніше регулювати особливі питання законодавчих актів, які недостатньо висвітлені, зокрема питання біометричних персональних даних, як сучасного ідентифікатора особи, який несе загрозу порушення конституційного права людини - зокрема права на приватне життя.

На думку Лутковської В. громадяни достатньо часто не переймаються можливими ризиками, пов’язаними з безпекою обробки та обігу

своїх персональних даних, загалом через відсутність інформації про наявні законодавчі стандарти та вимоги у цій сфері, відсутність обізнаності громадян у відповідній сфері є найголовнішою проблемою, адже будучи обізнаними - вони б рідше допускали порушення процедури обігу та обробки персональних даних щодо себе [43, с. 4-5].

За останні роки, незважаючи на недостатньо ефективне законодавче регулювання захисту саме біометричних персональних даних, Омбудсмен все ж звертав увагу на можливі порушення законодавства у сфері захисту біометричних персональних даних, та звертався до Конституційного Суду України та до Верховної Ради України щодо недопущення порушень законодавства та зміни законодавства у сфері захисту біометричних персональних даних.

Зокрема, у 2017 році Омбудсмен звернувся до Конституційного Суду щодо заборони правоохоронцям створювати ДНК-базу громадян. Адже у відповідності до п. 7 ч. 1 ст. 26 Закону України «Про Національну поліцію», національна поліція має право наповнювати та підтримувати в актуальному стані бази даних «осіб, затриманих за підозрою у вчиненні правопорушень» [72].

А також ч. 2 ст. 26 Закону України «Про Національну поліцію» для формування вищезазначених баз даних національна поліція має право збирати та накопичувати дактилокартки та зразки ДНК, що є біометричними даними осіб [72].

Відповідно, Омбудсмен В. Лутковська, вважаючи, що зберігання зразків ДНК осіб суперечить Конституції України, а саме статті 32, у відповідності до якої не допускається збирання, зберігання, використання та поширення конфіденційної інформації про особу без її згоди, крім випадків, визначених законом, і лише в інтересах національної безпеки, економічного добробуту та прав людини», звернулась до Конституційного Суду України щодо застосування диференційованого підходу, який зараз відсутній, до випадків

збирання зразків ДНК залежно від тяжкості та характеру правопорушення [75].

Ми погоджуємось із думкою Уповноваженого, що зберігання зразків ДНК осіб суперечить Конституції України, але лише у контексті відсутності диференційованого підходу до зберігання біометричних даних, адже загалом зберігання біометричних даних, зазначених у ст. 26 Закону України «Про Національну поліцію» дозволений як національним, так і міжнародним законодавством.

Зокрема, пункт 8 рекомендацій Комітету міністрів Ради Європи R(92)1 про використання аналізу дезоксирибонуклеїнової кислоти (ДНК) в рамках провадження за кримінальними справами зазначає, що у разі, коли йдеться про державну безпеку, зберігання зразків, результатів аналізу ДНК особи дозволяється, і навіть у випадках, коли їй не було висунуто звинувачення, а також не було винесено обвинувального вироку суду, але відповідний збір даних має регламентуватися законодавством і доступний лише тоді, коли сама процедура зберігання та збирання зразків буде законною [117].

Також, слід зазначити, що у 2012 році Омбудсмен В. Лутковська закликала Президента України ветувати закон, який передбачає запровадження біометричних паспортів, та повернути його на доопрацювання, як такий, що суперечить Конституції України [70].

Л. Денісова також зверталась у 2018 році до Конституційного Суду України щодо конституційності частини другої статті 26 закону «Про Національну поліцію», відповідно до якої поліцейські накопичують у бази даних біометричні дані затриманих [59].

Відповідно до статті 17 законопроекту, пропонується ще одна новела, яка стосується відстеження дій суб'єктів персональних даних, яке може здійснюватись за допомогою програмного забезпечення наприклад, або ж за допомогою інших технологій чи сервісів забороняється крім випадків, визначених Законом.

Тож, обробка, відповідно до частини першої статті, є правомірною, за умови дотримання принципів обробки персональних даних, що законопроектом встановлені [89].

Дослідивши законодавче регулювання контролю Уповноваженого Верховної Ради України з прав людини щодо обігу, обробки та захисту біометричних персональних даних, практичного контролю та нагляду з боку Омбудсмена, ми дійшли проміжного висновку, що у процесі євроінтеграції та підведення національного законодавства до міжнародного все ж національне законодавство України відповідає основним нормам захисту біометричних персональних даних міжнародного законодавства, але наявні і недоліки, зокрема відсутність диференційованого підходу у використанні біометричних даних національною поліцією, та відсутність конкретного регулювання захисту, обігу та обробки біометричних персональних даних з боку Омбудсмена.

### 3.2. Захист права на конфіденційність біометричних персональних даних адміністративними судами України

У разі порушення права особи на конфіденційність біометричних персональних даних Законом визначено право звернутись з метою захисту порушеного права до Уповноваженого Верховної Ради України з прав людини та до суду.

Гарантоване особі право на конфіденційність національним і міжнародним законодавством, все частіше зазнає порушень, про що свідчать численні статті у засобах масової інформації та судова практика як національних судів, так і Європейського суду з прав людини.

Законом України «Про захист персональних даних» визначено, що контроль за дотриманням законодавства у сфері захисту персональних даних здійснюють Уповноважений Верховної Ради України з прав людини та суди.

Вивчивши звіти Уповноваженого Верховної Ради України з прав людини ми отримали інформацію про наявність численних порушень інформаційних прав людини.

В Україні правами людей нехтують, зокрема правом на конфіденційність біометричних персональних даних, адже все частіше наявне втручання в приватне життя особи та поширення конфіденційної інформації щодо особи тощо [131, с. 70].

Часто українці звертаються до Європейського суду з прав людини, який ухвалюючи рішення проти України констатує грубі порушення Конвенції прав людини і основоположних свобод, наголошуючи на тому, що вони є неприпустимими в демократичному суспільстві [104].

Частиною першою ст. 55 Конституції України закріплена гарантія, що права і свободи людини і громадянина захищаються судом, а відповідно ч. 1 ст. 16 Цивільного кодексу України визначає, що кожна особа має право звернутися за захистом свого особистого немайнового або майнового права та інтересу до суду.

Таким чином, судовий захист займає чільне місце серед юрисдикційних форм захисту прав людини та має універсальний характер, адже дозволяє захистити будь-яке порушене право або законний інтерес. Звідси слідує, що саме суд є тим органом, котрий здійснює захист прав, свобод та законних інтересів у сфері приватноправових та публічно-правових відносин.

Пунктом 8 частини другої статті 8 Закону України «Про захист персональних даних» надано право суб'єкту персональних даних звертатися із скаргами на обробку своїх персональних даних до Уповноваженого Верховної Ради України з прав людини або до суду. У попередньому підрозділі даної дисертаційної роботи було наведено дослідження контролю та нагляду Уповноваженого Верховної Ради України з прав людини за дотриманням законодавства України у контексті обробки, обігу та захисту біометричних персональних даних. Другим суб'єктом захисту особи є суд. Саме до суду

особа має право звернутись із заявою про порушене право, що відповідно і зазначає ст. 8 Закону України «Про захист персональних даних».

Якщо розглядати у загальному провадження адміністративних судів щодо порушення захисту персональних даних переважають спори громадян до засобів масової інформації про захист честі, гідності та ділової репутації. Таких за рік судами першої інстанції розглядається в середньому від 200 до 300 справ, з них у 77 справах позовні вимоги задоволено, у 102 справах відмовлено у задоволенні позову, у 18 справах закрито провадження, 82 позовні заяви залишено без розгляду, 10 справ передано в інші суди [81, с. 24].

Оскільки законодавство не передбачає порядку підтвердження поширення недостовірної інформації про особу в мережі Інтернет, відповідно розгляд справ судами з даного предмету спору є складним, люди стикаються з неможливістю доведення необхідності захисту своєї честі, гідності та ділової репутації, внаслідок поширення щодо неї недостовірної інформації.

У подібних судових справах суди присуджують порушника права до примусового вибачення, що помилково трактується деякими суддями як належний в даному випадку спосіб судового захисту.

Щодо цього Саприкіна І. В. зазначає, що примусове вибачення не можна розглядати, як спеціальний спосіб захисту честі, гідності та ділової репутації особи, оскільки воно не передбачене нормативними актами і служить лише додатковим підтвердженням добросовісної помилки поширювача, сприяючи при цьому моральному задоволенню потерпілого. Окрім того, слушним зауваженням з її боку є те, що примусове вибачення глибоко суперечить праву особи на власну думку та вільне вираження поглядів, і є порушенням особистих немайнових прав порушника, що також неприпустимо [111, с. 17-18].

Подібне закріплюється Постановою Пленума Верховного Суду України у № 1 від 27 лютого 2009 р., а саме абзац 2 пункту 27 зазначає, суд не має повноважень зобов’язувати відповідача перед позивачем певним чином

вибачитись, адже відповідне може бути розцінене як порушення гідності, честі чи ділової репутації за поширення недостовірної інформації [103].

Пропонуємо звернути увагу на судову практику національних судів. Зокрема, відповідно до Рішення Святошинського районного суду м. Києва від 25 грудня 2013 р. у справі № 2608/18606/1214, відповідно до якого на телевізійний канал СТБ судом було покладено обов'язок опублікувати на офіційному веб-сайті особисте вибачення перед позивачем про те, що відповідачами поширена недостовірна інформація, яка не відповідає дійсності та порушує права та свободи позивача, а також ганьблять його честь, гідність та ділову репутацію [105].

Однак, все ж суди враховують на наявність біометричних даних особи, і деколи у своїх Рішеннях розрізняють види персональних даних. Зокрема, у справі за позовом громадян до Укрзалізниці, яка розглядалася Печерським районним судом м. Києва, були наявні скарги з боку громадян на протиправні дії Укрзалізниці щодо зберігання їх персональних даних, отриманих внаслідок оформлення квитків із зазначенням прізвища та імені у Єдиній автоматизованій системі керування пасажирськими перевезеннями Укрзалізниці, просили їх знищити та компенсувати завдану такими діями моральну шкоду.

У своєму рішенні від 14 березня 2014 р. у справі №757/24796/13-ц20 Печерський районний суд м. Києва не знайшов підстав для задоволення позову, зазначивши, що виключно прізвище та ім'я особи не є персональними даними, оскільки за ними не можна конкретно ідентифікувати особу. Для цього необхідно додаткові дані про особу, такі як: партійність, релігійність, національність, стать, професія, будь-які біометричні, соціальні дані, адреса проживання тощо. З цих підстав суд визнав, що прізвище та ім'я пасажирів обробляються у відповідності з чинним законодавством України [106].

Однак, необхідно зазначити, що судових рішень щодо визнання факту порушення захисту біометричних персональних даних з боку національних адміністративних судів дуже мало. Досить проблемним, як для країни, яка

стоїть на шляху євроінтеграції і має підвищувати рівень правової обізнаності населення, право на захист біометричних персональних даних яких очевидно що порушується.

У відповідності до Рішення Житомирського окружного адміністративного суду від 01 березня 2018 року у справі № 806/3744/17 вимоги позивача щодо порушення його права на захист біометричних персональних даних не були задоволені. Вважаючи, що відповідач порушує його права та інтереси, відмовляючи в оформленні закордонного паспорта без встановлення біометричного чіпа та сканування відбитків пальців рук, позивач звернувся до суду з даним адміністративним позовом [107].

Відповідно до пунктів 6, 7 частини першої статті 3 Закону України «Про Єдиний державний демографічний реєстр та документи, що підтверджують громадянство України, посвідчують особу чи її спеціальний статус» для цілей вищезазначеного закону ідентифікацією особи визначається її встановлення способом порівняння наданих даних, зокрема біометричних, з наявною інформацією про особу в картотеках, базах даних чи певних реєстрах; ім'я особи - прізвище, ім'я та по батькові фізичної особи [107].

Також, суд проаналізувавши зміст чинного законодавства щодо зобов'язання відповідача видати ОСОБА_1 закордонний паспорт без електронних носіїв старого зразку, дійшов висновку, що в даний час оформлення паспорта громадянина України для виїзду за кордон може здійснюватися лише з безконтактним електронним носієм, а тому позовні вимоги ОСОБА_1 є необґрунтованими та такими, що не підлягають задоволенню [107].

У контексті розгляду тенденцій сучасної практики судового розгляду справ щодо порушення законодавства про захист персональних даних, після прийняття Закону України «Про захист персональних даних» спостерігається активізація судової практики, адже Україна отримала спеціальний нормативно-правовий акт, який чітко визначає права й обов’язки суб’єктів

відносин у сфері захисту персональних даних, що в свою чергу надає підстави для звернення до суду щодо захисту порушених прав.

Загалом, варто зазначити, що судова практика є відображенням довільності застосування норм чинного законодавства у сфері захисту персональних даних, оскільки багато судових рішень мають здебільшого роз'яснювальний характер.

Нами було проаналізовано велику кількість Рішень адміністративних судів у контексті порушення певних прав на захист біометричних персональних даних, та ми дійшли висновку, що всі ці судові справи стосуються або закордонного паспорту, або ID-картки (нового українського паспорту), адже процедури видачі даних паспортів передбачають обробку та обіг біометричних персональних даних, інших Рішень адміністративних судів щодо порушення права на захист біометричних персональних даних нами не було знайдено.

Але ж із засобів масової інформації суспільству відомо про велику кількість випадків порушення права на захист біометричних персональних даних, постає питання, чому особи не звертаються до суду за захистом своїх прав.

Маються на увазі такі порушення, зокрема, як: несанкціонований доступ до інформації персонального характеру, використання біометричних персональних даних з метою, яка не відповідає меті створення бази персональних даних, порушення умов надання доступу до персональних даних відповідної третьої особи тощо.

Однак позитивним є той факт, що сьогодні судочинство залишається основним засобом захисту прав учасників правовідносин, пов'язаних з персональними даними, що вказує на довіру до цієї гілки влади, але відсутність обізнаності людей про можливість захисту у суді своїх порушених прав на захист біометричних персональних даних і дає таку малу судову статистику щодо профільних рішень адміністративних судів.

Відповідно до статей 18, 19 законопроекту закріплюється право на інформацію та право на доступ до персональних даних. Крім того, якщо персональні дані будуть зібрані за допомогою суб'єкта даних, особа, що збирає дані як контролер під час або перед отриманням персональних даних зобов'язана повідомити відповідного суб'єкта, надавши таку інформацію, зокрема:

1) інформацію про контролера - його контактні дані чи контактні дані його представника за наявності;

2)інформацію про дані оператора, якщо такий наявний;

3) інформацію про особу, що відповідає за захист контролером відповідних персональних даних;

4) інформацію про цілі, способи та мету обробки;

5) інформацію про самі дії, які будуть здійснюватись з перснальними даними;

6) інормацію про те, які саме дані відповідно оброблятимуться;

7) інформацію про наявність законних підстав на таку обробку;

8) інформацію про одержувачів чи інформацію про категорію одержувачів відповілних персональних даних;

9) інформацію про те, кому відповідні дані передаватимуться, зокрема про міжнародні організації чи держави, з приміткою про наявність у останніх необхідного рівня захист персональних даних;

10) інформацію про строки зберігання таких даних та інформацію про підстави неможливості визначення строків збору;

11) інформацію про можливість подати скаргу щодо порушення захисту даних;

12) інформацію про можливість та алгоритм відкликання згоди на обробку персональних даних, якщо відповідна згода на обробку таких даних надавалась попередньо;

13) інформацію про перелік прав суб'єкта даних, визначиних чинним законодавством України;

14) інформацію про наслідки у разі надання чи ненадання відповідних персональних даних;

15) інформацію про механізм автоматизованого прийняття рішень (профілювання, інформацію про алгоритм роботи механізму, наслідки обробки для суб`єкта даних);

16) інформацію про реалізацію обробки персональних даних для цілей прямого маркетингу, можливості відмовитися від такої обробки.

Законопроектом зазначається, що вищезазначена інормація не є обовязковою тоді, коли суб'єкт персональних даних інформацію таку має.

Інформація, вказана в цій статті законопроекту, надається суб'єктам персональних даних у спосіб, що є зрозумілим та доступним, а інформація в результаті є зрозумілою для суб'єктів персональних даних.

Щодо права суб'єкта персональних даних на доступ до персональних даних, останній має право отримати від контролера інформацію про обробку чи її відсутність щодо його персональних даних, а коли здійснюється обробка - право на доступ та на отримання інформації щодо персональних даних, зокрема інформація наступна:

1) інформація про ціль такої обробки;

2) інформація про склад персональних даних, які відповідно готуються до обробки;

3) інформація про одержувачів даних чи категорії одерржувачів таких відповідних даних;

4) інформація про строк зберігання персональних даних та про критерії визначення строку у випадках, коли в момент збору персональних даних таких строк видається неможливим визначити;

5) інформація щодо права виправлення, забуття, обмеження, заперечення щодо такої обробки;

6) інформація про право оскарження та інормація про орган, до якого можна оскаржити;

7) інформація про джерело збору даних у разі, коли не від суб'єкта персональних даних;

8) інформація про механізм автоматизованого прийняття рішень;

9) інформація про гарантії захисту даних у разі наявності міжнародної організації чи іноземної крати у контексті обробки чи використання таких даних.

Законопроектом наголошується, суб'єкт персональних даних отримує від контролера, що обробляє дані право на отримання копії своїх оброблюваних даних, а в свою чергу контролер зобов'язаний зберігати інформацію про джерело даних, що підлягали обробці.

Суб'єкту персональних даних може бути обмежено право на доступ вищезазначених даних відповідно до Закону та у разі, якщо таке обмеження є пропорційним та з легітимною метою.

Крім того, законопроектом зазначено, що інформація, викладена у статті, можу бути надана суб'єктам персональних даних у спосіб, що є доступним та зрозумілим для останнього [89].

Наприкінці дослідження предмету даного підрозділу дисертаційної роботи, вважаємо за необхідне зазначити про Хартію основних прав Європейського Союзу, адже у перших договорах Європейських співтовариств немає посилань на права людини або їх захист. З огляду на те, що до тодішнього Суду першої інстанції Європейських співтовариств надходили заяви про порушення прав людини у сферах дії права ЄС, він розробив новий підхід [118].

Для забезпечення захисту фізичних осіб він включив основоположні права до так званих загальних принципів європейського права, якими сьогодні користуються і суди України. Але нам не вистачає інструкцій, порядків, на кшталт колишніх Постанов Пленуму ВСУ, в яких би систематизовувалась судова практика у справах про біометричні персональні дані, та роз'яснювався порядок розгляду відповідних справ.

Питання відповідальності є дуже важливим, адже відповідальність за порушення права на захист персональних даних має бути такою, що зупинить або попередить настання шкоди персональним даним особи. Таким чином, сьогодні відповідно до статті 188-39 Кодексу України про адміністративні правопорушення за порушення у сфері поводження з персональними даними передбачено штраф, максимальний розмір якого є дещо більшим ніж 30 тисяч гривень. У свою чергу, незаконне збирання, зберігання, використання, знищення, поширення конфіденційної інформації про особу або незаконна зміна такої інформації передбачає настання кримінальної відповідальності відповідно до статті 182 Кримінального кодексу України.

Слід наголосити, що кримінальна відповідальність може бути застосована виключно до юридичних осіб, а фізичні особи у разі незаконного збирання, зберігання, використання, знищення чи поширення конфіденційної інформації про особу лише нестимуть адміністративну відповідальність, що була визначена вище.

Доказовість відповідних правопорушень є дуже складним процесом, і на сьогодні в Україні за останні роки достатньо мало кримінальних проваджень, де предметом є незаконне збирання, зберігання, використання, знищення, поширення біометричних персональних даних.

Таким чином, видається необхідним перегляд відповідальності, визначеної законодавством за порушення у сфері поводження з персональними даними, шляхом збільшення розміру передбаченого штрафу або передбачення інших більш суттєвих санкцій, а за незаконне збирання, зберігання, використання, знищення, поширення конфіденційної інформації про особу передбачення можливості несли кримінальну відповідальність не тільки юридичними, а і фізичними особами.

### 3.3. Захист біометричних даних в практиці Європейського Суду з прав людини та основні напрями її імплементації у правозастосовну діяльність органів судової влади України

Досліджуючи практику Європейського Суду у контексті захисту біометричних даних осіб, варто, насамперед, зазначити, що дійсно Європейський Суд з прав людини досить часто стикається з необхідністю вирішувати подібні справи, а українці також є тими, хто подає подібні позови проти України та виносяться рішення проти зарубіжних країн

Якщо досліджувати це питання глибше, законодавство європейських країн у сфері захисту персональних даних починає формуватися з 80-х рр. минулого століття.

У 1983 році Федеральний Конституційний суд Федеративної Республіки Німеччина надав підстави до необхідності створення нормативно-правових актів у сфері захисту біометричних даних, адже, на думку суду, користувач має право знати інформацію про себе, а також про те, яким чином його персональні дані використовуються та розкриваються.

Згодом, у 1990 році було розроблено та прийнято Закон «Про захист даних» [46]. Дійсно, варто зазначити, що Німеччина була далеко не першою європейською країною, яка прийняла закон, що врегульовував право на захист персональних даних, але даний закон сьогодні є одним із найкращих у даній сфері серед країн Європи.

Якщо Німеччина прийняла профільний нормативно-правовий акт у 1990 році, то Нідерланди прийняли Декрет про вразливі дані у 1993 році, Фінляндія прийняла Закон «Про реєстрацію громадян» у 1987 року, Франція - Закон «Про інформатику, картотеку та свободи» у 1978 року, в свою чергу Великобританія - «Закон про захист персональних даних» у 1984 році, а Угорщина - Закон «Про захист інформації про особу і доступ до інформації, що становить суспільний інтерес» у 1992 року.

Гонконг, як азійська країна, прийняв відповідний профільний закон у 1995 році і на його основі закони «Про практику стосовно номерів посвідчення особи» та «Про дані стосовно кредитоспроможності споживачів» [82, с. 513 – 219; 46].

Європейська спільнота у той час активно почала займатись врегулюванням питання захисту персональних даних осіб на міжнародному рівні, про що свідчить ще 28 січня 1981 року Радою Європи Конвенції № 108 «Про захист осіб у зв'язку з автоматизованою обробкою персональних даних» [50].

Відповідний міжнародний документ став першою спробою створення єдиного міжнародного законодавчого акта, який би ставив за мету захист персональних даних. Цей документ спрямований на об'єднання країн світу для визначення основних вимог до передачі індивідуальної інформації про людину у всесвітньому електронному просторі, тобто створення низки правил, які стають обов'язковими при обробці персональних даних.

До вищезазначеної Конвенції першими приєднались такі країни, як Іспанія, Німеччина, Норвегія, Франція та Швеція. А з 2000 року до Конвенції приєдналось більше 20 країн [50].

15 грудня 1997 року Європейський Парламент прийняв Директиву 97/66/ЄС «Стосовно обробки персональних даних і захисту права на невтручання в особисте життя в телекомунікаційному секторі» [31].

Ця Директива встановлює вимоги для впровадження у національне законодавство гарантій щодо захисту персональних даних. З цією метою при Раді Європи утворюється особливий орган, так звана «Робоча група 29-ої статті».

Задача його полягає в нагляді за державами, що увійшли до Конвенції № 108, та дотримання ними вимог Директиви 97/66/ЄС у захисті персональних даних при обробці інформації в автоматизованих базах даних. З часом з метою адаптування попереднього законодавства у цій сфері до змін на ринку та у технологіях надання послуг електронного зв'язку її замінила Директива №

2002/58/ЄС Європейського Парламенту і Ради ЄС стосовно обробки персональних даних та захисту права на недоторканість особистого життя в сфері електронних засобів зв'язку (Директива про право на недоторканність особистого життя та електронні засоби зв'язку), прийнята 12 липня 2002 року, яка мала забезпечити уніфікований рівень захисту персональних даних та інформації про приватне життя користувачів загальнодоступних послуг електронного зв'язку незалежно від технологій, що використовуються.

Слід також навести такі міжнародні документи як Директива 2002/20/ЄС Європейського Парламенту і Ради від 7 березня 2002 року про дозвіл для мереж і послуг електронних засобів зв'язку (Директива про дозвіл), Директива 2002/22/ЄС Європейського Парламенту і Ради від 7 березня 2002 року про універсальну послугу і права користувачів стосовно мереж і послуг електронного зв'язку (Директива про універсальну послугу) та Директива 2009/136/ЄС Європейського Парламенту і Ради від 25 листопада 2009 року, що вносила зміни до ряду раніше ухвалених документів, які регулюють діяльність у сфері захисту персональних даних, і очевидно що стають своєрідним інструментарієм захисту персональних даних [57].

Варто зазначити, що подібні активні рухи зі сторони Ради Європи щодо ефективного врегулювання правового статусу персональних даних, їх обігу та обробки та їх захисту направлений на майбутнє створення європейської зони вільного руху інформації. Така мета була поставлена і загалом перед ЄС, і перед країнами-членами та претендентами у Союз ще на початку 21 століття, хоч і Україна не надто поспішала створювати необхідні нормативно-правові акти у сіерф захисту персональних даних, про що свідчить Закону України «Про захист персональних даних» лише у 2010 році [88].

На даному етапі дослідження дисертаційної роботи, пропонуємо розглянути європейські принципи захисту персональних даних, на яких відповідно і будується все європейське законодавство у сфері захисту персональних даних, і зокрема біометричних персональних даниз. Тож, виділяються наступні принципи:

– принцип персоноцентризму (автоматизація обробки персональних даних осіб, відповідно через автоматизовані системи). Такі системи закріплені і Конвенцією 108 і національним законодавством України, зокрема окрім автоматизованих систем все ж і європейське і українське законодавство передбачає ручну обробку шляхом створення картотек із персональними даними.

– принцип екстериторіальності (необхідність поваги до основних прав та свобод людини незважаючи на місцезнаходження баз даних). Обмеження за територіальними ознаками неприпустимі в сфері захисту персональних даних, у відповідності до основних положень Загальної декларації прав людини ООН від 10 грудня 1948 року; [44]

– зв'язок захисту персональних даних та права на приватність життя людини;

– рівність усіх щодо захисту персональних даних у будь-якому місті, територіальна незалежність [46, с. 149-157]. Мається на увазі, що країни – учасники Конвенції гарантують належний захист індивідуальної інформації, всі майбутні країни-члени, які побажають приєднатися до цієї Конвенції, повинні надати гарантії виконання основних прописаних у ній вимог;

– принцип субсидіарності (будь-яка обробка індивідуальної інформації про фізичну особу повинна відбуватися на основі законодавства країни-члена, повноважень створеного нею контролера, рівень можливих ризиків втрати або витоку інформації базуються на національних законодавчих базах);

– зближення законодавств в сфері захисту персональних даних не повинно бути причиною зниження рівня безпеки, а навпаки – служити підвищенню якості послуг захисту персональної інформації;

– принципи захисту персональних даних повинні бути однаковими як для автоматизованих баз, так і для інших форм ведення баз даних;

– збір та обробка персональних даних повинні проводитися на основі чітко визначених та законних цілей;

– дозвіл використання персональних даних у разі захисту життєво важливих для суб'єкта інтересів;

– дозвіл на використання персональних даних у разі виправдання їх обробки суспільними цілями в сфері охорони здоров'я, соціального захисту, в науковій сфері та в державних статистичних дослідженнях;

– держави-члени можуть у своєму законодавстві встановлювати спеціалізацію за сферами для отримання індивідуальної інформації. Медична інформація видається медичним працівником, інформація соціального захисту – соціальним агентом тощо;

– контрольний орган держави-члена може наділятися правами з метою захисту інтересів національної безпеки, забезпечення основних прав громадян, захисту економічних та фінансових інтересів держави.

Кожна з держав – членів Конвенції № 108 бере на себе зобов'язання приводити своє законодавство у сфері захисту персональних даних у відповідність до викладених вище принципів [34].

Для України виконання цих вимог є однією з обов'язкових умов на шляху до євроінтеграції. Крім європейського досвіду у сфері захисту персональних даних, слід звернути увагу і на специфіку вирішення цієї проблеми в США. Точкою відліку постановки проблеми захисту індивідуальної інформації в США став випадок у Бостоні у 1890 році, коли на шпальтах однієї з газет були опубліковані деякі подробиці одного весілля.

Процес проти газети почав батько нареченої, відомий в той час адвокат та юрист Самуель Воррен. У результаті у зазначеній статті, присвяченій захисту інформації особистого характеру, вперше визначається поняття «захист персональних даних» як синонім «бути залишеним у спокої» [85].

Саме подальший розвиток цієї концепції і призвів до появи у Загальній Декларації прав людини ООН від 10 грудня 1948 року статті 12, якою прямо передбачено, що жодна людина не може зазнавати втручання у приватне життя, тим більше безпідставного, а також відповідно посягання на недоторканність житла, крім того на таємницю кореспонденції людини, а

також на честь та гідність людини, адже кожен має бути захищеним від відповідних втручань відповідно до закону [44].

Досвід європейських країн у сфері захисту даних сприяв початку дослідження цієї проблеми Організацією Економічної Співпраці та Розвитку (ОЕСР), яка розпочала активну діяльність у цьому напрямку у 1969 році. Саме тоді виникають спроби вивчення комп'ютеризації та автоматизації обробки даних. У 1978 році ОЕСР створює групу експертів, основною спеціалізацією якої стають випадки транскордонної передачі інформації та захист відповідних даних. Керівником цієї групи стає представник Австралійського Комітету з правової реформи [85].

23 вересня 1980 року ОЕСР ухвалила Керівні принципи про захист права на приватність та транскордонні потоки інформації [85]. Ці принципи не покладають на держав-членів особливих зобов'язань, але обмежують деякі виключення з установлених ними правил.

До того ж Керівні принципи поширюються не тільки на автоматизовані бази даних, а й на «змішані» системи, в яких методи обробки здійснюються не за допомогою комп'ютерних засобів. У 1998 році в Канаді на засіданні ОЕСР, на якому були присутні представники 29 країн-членів, була прийнята Декларація про захист інформації в глобальних мережах, у тому числі й мережі Інтернет.

Для Декларації важливим аспектом є попередження користувача мереж про можливі проблеми приватності, навчання користувачів основним правилам захисту персональних даних, їх правам та обов'язкам [44].

Отже, роблячи попередні висновки, стає можливим визначити основні орієнтири в сфері національної регуляції захисту персональних даних та міжнародний досвід у вирішенні цієї проблеми. Зусилля держав – членів Конвенції № 108 та ОЕСР сприяли приведення законодавств багатьох країн до стандартизації захисту прав споживачів щодо захисту та обробки персональних даних не тільки в мережі Інтернет, а й взагалі в усіх мережевих системах [85].

Виконання вимог Директиви 97/66/ЄС значно підвищило рівень безпеки при транскордонних потоках передачі персональних даних та їх надійного збереження в країнах, що взяли на себе відповідальність за виконання вказівок Директиви. При цьому різниця в підходах національних законодавств нівелюється досягненням основної мети – забезпечення основних прав людини.

Що стосується судової практики ЄСПЛ, варто наголосити, що останній визнає втручання законним у разі наявності законодавчо передбаченої можливості втручатись у певних випадках, з забезпеченням необхідних визначених законодавством процедур і правил такого втручання. ЄСПЛ визначена необхідність національних нормативно-правових актів бути «доступними для зацікавлених осіб і передбачуваними щодо наслідків їх дії» [108].

У розумінні ЄСПЛ «передбачуваність» норми – це її закріплене законодавчо сформулювання настільки чітко, що дає змогу кожному, хто її використовуватиме, вивіряти свою поведінку. «Ступінь чіткості, що вимагається від закону» у зв'язку з цим залежатиме від конкретного питання.» [109].

Загалом імплементація у правозастосовну діяльність органів судової влади України міжнародної практика є актуальним питанням, адже і сьогодні, українські суди вивчають рішення ЄСПЛ у контексті певних складних справ, хоча судового прецеденту в Україні нема. Українські суди використовують практику ЄСПЛ, як у свій час використовували Постанови Пленуму ВСУ. Ми вбачаємо необхідним, не стільки імплементацію судової практики ЄСПЛ в Україну, скільки приведення національного законодавства до міжнародних вимог, шляхом приділення значної уваги в Законі України «Про захист персональних даних» уваги саме біометричним персональним даних, зазначення порядку їх обігу, обробки і захисту, в кінці кінців - перелічити їх, зазначити, що можна конкретно вважати біометричними персональними даними, а також приведення у порядок підзаконних нормативно-правових

актів, які також мають врегульовувати питання обігу, обробки та захисту біометричних персональних даних в Україні.

**Висновки до розділу 3**

Пункт 7 частини 1 статті 3 Закону України «Про Уповноваженого Верховної Ради України з прав людини» закріплює за Омбудсменом як складову парламентського контролю сприяння правовій інформованості населення та захист конфіденційної інформації про особу , Закон жодного разу не використовує поняття «персональні дані» або «біометричні персональні дані», таким чином конкретно не врегульовує питання обігу, обробки чи захисту біометричних персональних даних особи.

Уповноважений Верховної Ради України є гарантом безпеки обігу та оброблення персональних даних та має низку повноважень у сфері контролю за захистом персональних даних, у тому числі і біометричних персональних даних.

Повноваження Омбудсмена у сфера контролю за дотриманням законодавства з захисту персональних даних слід на поточні та індивідуальні; на обов'язкові та декларативні; на нормотворчі, розпорядчі, контрольні та організаційні.

На нашу думку, враховуючи специфіку біометричних персональних даних, повноваження Уповноваженого Верховної Ради України з прав людини слід доповнити наступними повноваженнями:

– надання висновків щодо можливості застосування тих чи інших біометричних технологій до людини, перед тим, як вони будуть введені в законодавчий та практичний обіг;

– залучення експертів у контексті проведення перевірок щодо порушення законодавстві України у сфері захисту біометричних персональних даних.

Ми переконані, що Уповноважений Верховної Ради України з прав людини має спочатку надавати висновок на предмет того, чи можна вводити ту чи іншу технологію ідентифікації людини тощо, а потім вже вводити її як в законодавчий, так і в практичний обіг.

Департамент з питань захисту персональних даних, що знаходиться в секретаріаті Уповноваженого Верховної Ради України з прав людини і є тим структурним підрозділом, який проводить перевірки, складає проекти нормативно-правових актів, проекти постанов, проекти рекомендацій, і займається моніторингом нових тенденцій, технологій, тощо.

Відповідно до Роз'яснення до Порядку здійснення Уповноваженим контролю за додержанням законодавства про захист персональних даних № 0002715-14, в редакції від 08.01.2014 (далі - Порядок) Уповноважений Верховної Ради України з прав людини (далі - Уповноважений), окрім інших функцій, здійснює контроль за додержанням законодавства про захист персональних даних.

З цією метою Уповноваженим за скаргами юридичних та фізичних осіб, а також за власною ініціативою проводяться перевірки додержання законодавства про захист персональних даних.

Відповідно до цього порядку, скарга особи, яка звертається до Уповноваженого також має відповідати певним вимогам, зокрема має бути обґрунтованою, повинна містити інформацію щодо історії виникнення проблемного питання, фактів, що свідчать про порушення прав, сутність вчиненого порушення, а також інформацію щодо заходів, вжитих з метою виправлення порушення, зокрема скарг, направлених до інших органів.

А також найголовнішим є те, що викладені у скарзі обставини мають бути підкріпленими реальними доказами, які прикріплюються до скарги додатками, як копії тих чи інших документів, чи як роздруківка електронного джерела, сайту, сторінки тощо.

Як звернення, так і скарги слід подавати Уповноваженому у письмовій формі, що на нашу думку є неефективним, адже коли мова йде про порушення обігу, обробки чи захисту персональних даних, великий відсоток який на жаль здійснюється саме через мережу інтернет, на офіційній веб-сторінці Уповноваженого має бути електронний розділ, куди людина може надіслати,

або залишити на сторінці свою скаргу чи звернення, залишивши свої контактні дані для зворотного зв'язку.

Якщо Уповноважений є контролюючим органом за обігом, обробкою та захистом персональних даних особи, зокрема біометричних персональних даних, відповідний Уповноважений має надати всі необхідні можливості задля швидкого оповіщення його про можливі порушення, та і загалом має бути ближче до людини.

Тим більше, що має секретаріат, який може взяти на себе функцію моніторингу звернень і скарг на офіційній веб-сторінці. Тому, ми вважаємо, що запровадження електронної форми звернень і скарг на офіційній сторінці Уповноваженого Верховної Ради України з прав людини є необхідним елементом забезпечення ефективного контролю та нагляду за дотриманням законодавства у сфері обігу, обробки та захисту персональних даних, а найголовніше біометричних персональних даних особи.

Законодавство України не позбавляє особу права одночасно подати заяву чи скаргу до Уповноваженого, та до суду. Але, вищезазначений Порядок, який регулює дії Уповноваженого, процедурно надає можливість Уповноваженому зупиняти провадження по справі, коли останньому стає відомо про наявність відкритого судового провадження у цій самій справі.

На нашу думку, це є неприпустимим, адже Порядок здійснення Уповноваженим контролю за додержанням законодавства про захист персональних даних № 0002715-14, в редакції від 08.01.2014 не має вищої юридичної сили ніж закони України, і якщо чинне законодавство прямо не забороняє особі звертатись із заявою одночасно і до суду, і до Уповноваженого, то Уповноважений не має законних підстав зупиняти провадження у справі, дізнавшись про відкрите судове провадження у відповідній справі. На нашу думку, слід прописати в Законі України «Про Уповноваженого Верховної Ради України» норму, яка б прямо забороняла Уповноваженому зупиняти провадження у зв'язку із розглядом відповідної справи у суді.

За останні роки, незважаючи на недостатньо ефективне законодавче регулювання захисту саме біометричних персональних даних, Омбудсмен все ж звертав увагу на можливі порушення законодавства у сфері захисту біометричних персональних даних, та звертався до Конституційного Суду України та до Верховної Ради України щодо недопущення порушень законодавства та зміни законодавства у сфері захисту біометричних персональних даних.

Законом України «Про захист персональних даних» визначено, що контроль за дотриманням законодавства у сфері захисту персональних даних здійснюють Уповноважений Верховної Ради України з прав людини та суди. Вивчивши звіти Уповноваженого Верховної Ради України з прав людини ми отримали інформацію про наявність численних порушень інформаційних прав людини. Суди в Україні не часто мають справу з біометричними персональними даними.

Ч. 1 ст. 55 Конституції України закріплена гарантія, що права і свободи людини і громадянина захищаються судом, а відповідно ч. 1 ст. 16 Цивільного кодексу України визначає, що кожна особа має право звернутися за захистом свого особистого немайнового або майнового права та інтересу до суду.

Ми визначити, що конфіденційна інформація є підвидом інформації про особу і не вичерпується персональними даними.

Поняття конфіденційної інформації визначено Законами України «Про інформацію» та «Про доступ до публічної інформації» , а також багато інших законів прямо визначають інформацію про особу, що є конфіденційною.

Відсутність в Україні порядку підтвердження поширення недостовірної інформації про особу в мережі Інтернет, відповідно розгляд справ судами з даного предмету спору є складним, люди стикаються з неможливістю доведення необхідності захисту своєї честі, гідності та ділової репутації, внаслідок поширення щодо неї недостовірної інформації.

Нами було проаналізовано велику кількість Рішень адміністративних судів у контексті порушення певних прав на захист біометричних

персональних даних, та ми дійшли висновку, що всі ці судові справи стосуються або закордонного паспорту, або ID-картки (нового українського паспорту), адже процедури видачі даних паспортів передбачають обробку та обіг біометричних персональних даних.

На шляху євроінтеграції Україна намагається підлаштовувати національне законодавство під міжнародні норми, але у контексті регламентації права на захист біометричних персональних даних, обіг і їх обробку, а також у контексті наявності належного інструментарію здійснення законної обробки, обігу та захисту біометричних персональних даних, Україна має запозичити європейський досвід та внести відповідні зміни в Закон України «Про захист персональних даних» задля деталізації та максимального урегулювання питання обігу, обробки та захисту біометричних персональних даних.

# ВИСНОВКИ

Дослідивши питання адміністративно-правового забезпечення обігу та захисту біометричних персональних даних у рамках даного дисертаційного дослідження, у якому розкривались питання визначення поняття біометричних персональних даних, меж та способів правомірного обігу персональних даних за законодавством України і Європейського Союзу, характеристика права на захист біометричних персональних даних, як складової адміністративно-правового статусу фізичної особи, нормативні засади адміністративно-правового забезпечення обігу та захисту біометричних персональних даних за законодавством України та Європейського Союзу, особливості правовідносин у сфері адміністративно-правового забезпечення обігу та захисту біометричних персональних даних, визначення інструментів адміністративно-правового забезпечення правомірного обігу та захисту біометричних персональних даних та адміністративно-правового забезпечення правомірного обігу та захисту права на конфіденційність біометричних персональних даних Уповноваженим Верховної Ради України з прав людини: процедури, засоби та умови реалізації, а також захист права на конфіденційність біометричних персональних даних адміністративним судами України та в практиці Європейського Суду з прав людини, і відповідно основні напрями її імплементації у правозастосовчу діяльність органів судової влади України ми дійшли таких висновків.

1. Україна як держава-член Загального регламенту про захист даних взяла на себе зобов`язання відповідно до пункту 53 передмови забезпечити умови та обмеження у контексті роботи з біометричними даними, адже саме біометричні персональні дані є спеціальною категорією персональних даних. Міжнародний документ має певні вимоги щодо того, що створивши умови та обмеження по роботі з біометричними персональними даними держави-члени не мають права перешкоджати вільному потоку персональних даних в межах Союзу тоді, коли такі умови застосовують до транскордонного опрацювання

таких даних; а також держави-члени мають зберегти професійну таємницю, для певних цілей, пов'язаних із здоров'ям у роботі з біометричними персональними даними.

2. В результаті аналізу сучасного аналізу предмету дослідження було визначено, що сучасний стан дослідження використання, обігу та захисту біометричних персональних даних став передумовою розвитку у науці таких явищ як «інтернет речей» та «хмарні технології», адже на побутовому рівні з використанням мережі інтернет та інформаційних технологій на побутовому рівні біометричні персональні дані використовуються частіше ніж державними органами офіційно, а зберігаються, у свою чергу, більше у хмарних базах даних, ніж у офіційних державницьких базах даних.

Інтернетом речей є перелік датчиків та відповідних пристроїв, що шляхом генерації потоку даних, поліпшують життя людей, підвищують ефективність бізнесу, передбачають розвиток інформаційного суспільства загалом.

Тож, вважаємо за необхідне наголосити на потребі нормативного врегулювання технічного захисту біометричних персональних даних при проектуванні, використанні та знищенні Інтернету речей, необхідності розробки порядку обробки та технічного захисту біометричних персональних даних власників та споживачів інтернету речей.

3. Біометричними персональними даними є дані, що були отримані за результатами спеціального технічного опрацювання фізичних, фізіологічних чи поведінкових ознак особи, якими можуть бути зображення обличчя чи дактилоскопічні дані тощо, які надають можливість однозначно ідентифікувати або підтверджують однозначну ідентифікацію фізичної особи.

Відповідно до статтей 6 Конвенції 108 та статті 8 Директиви про захист персональних даних біометричні персональні дані є особливою категорією персональних даних, які за своєю природою можуть становити загрозу для суб'єктів, персональні дані яких обробляються, і потребують посиленого захисту. Міжнародні документи передбачають необхідність отримання дозволу на обробку цих особливих категорій даних («чутливих»)

лише з особливими гарантіями. Важливо, що такі біометричні персональні дані міжнародні документи, на відміну від національного законодавства, перелічують, а саме мова йде про персональні дані, що містять інформацію про расове чи етнічне походження, або ж персональні дані, що інформують про політичні, релігійні чи інші переконання, а також відповідно персональні дані, які стосуються здоров'я або статевого життя особи.

Генетичні дані визначені як персональні дані щодо вроджених або набутих генетичних ознак фізичної особи, що надають індивідуальнізовану інформацію щодо фізіології чи здоров'я такої фізичної особи та/або ж такі, які відповідно отримані, наприклад, в результаті аналізу біологічного зразка, взятого у відповідної фізичної особи.

Визначено, що біометричні персональні дані зберігаються у базах даних, та визначено поняття «база даних» як іменована сукупність даних, що відображає стан об'єктів та їх відношень у визначеній предметній області. Бази біометричних даних є закритими та відкритими.

Наведено ще один різновид носія біометричних персональних даних, а саме «хмарні бази даних», та дане поняття є похідним від поняття «хмарні технології». Хмарні бази даних зберігають біометричні персональні дані через застосування інтернету речей, є законодавчо неврегулюваними в Україні та потребують врегулювання, зокрема порядку використання та обробки біометричних даних задля подальшого їх ефективного захисту.

У дисертації запропоновано визначати поняття «хмарні бази даних» як сукупність даних, що відображають стан об'єктів та їх відношень у визначеній предметній області, використовуються із застосуванням Інтернету речей.

4. Специфіка та вразливість біометричних персональних даних полягає у неможливості їх зміни, адже це специфічні об'єкти. Ми погоджуємось із думками науковців, проаналізованих у дисертації, що найбільш часто ідентифікація людини відбувається на підставі наступних фізіологічних характеристик: відбитків пальців, сітківки і райдужної оболонки ока, відбитків рук, рис обличчя. Молекулярна будова ДНК і групу крові є також

біометричними персональними даними. Однак, дієвих алгоритмів збирання, зберігання та використання відповідних даних нема, тож адміністративно-правове регулювання обігу та захисту саме біометричних персональних даних на національному рівні є недостатньо врегульованим і з розвитком інформаційних технологій та інформаційного суспільства потребує нагального врегулювання.

5. Обробка біометричних персональних даних є можливою лише у разі надання суб'єктом біометричних персональних даних однозначної згоди на обробку його даних. Також у випадках необхідності обробки для реалізації прав та виконання обов'язків володільця, наприклад у сфері трудових відносин разом з забезпеченням відповідного захисту, у разі необхідності обробки для захисту життєво важливих інтересів суб'єкта персональних даних або іншої особи у разі недієздатності або обмеження цивільної дієздатності суб'єкта персональних даних та відповідно коли обробка здійснюється із забезпеченням відповідного захисту певними громадськими чи політичними організаціями, якщо обробляються дані членів цих громадських об'єднань або пов`язаних осіб. Крім того, третім особам персональні дані не передаються без згоди суб'єктів персональних даних, або ж у разі коли необхідне обґрунтування передання чи задоволення/захисту правової вимоги. Передаються дані у сфері охорони здоров'я, у разі коли мова йде про встановлення медичного діагнозу, під час піклування чи лікування або надання медичних послуг, або ж функціонування електронної системи охорони здоров'я за умови, що відповідні дані оброблятимуться медичним працівником або працівником закладу охорони здоров'я чи суб`єктом підприємницької діяльності, який має ліцензію щодо відповідної діяльності з медичної практики, його працівники, що мають відповідні обов'язки забезпечити захист персональних даних, посадові особи, які зобов`язані зберігати лікарську таємницю, Міністерство охорони здоров`я України та його територіальні підрозділи. Також дані не надаються у сферах виконавчих проваджень, вироків суду, під час контррозвідувальної чи оперативно-

розшукової, під час боротьби з тероризмом, винятки ставлять використання даних державними органами в межах визначених чинним законодавством повноважень, та стосовно даних, що були оприлюднені самим суб'єктом таких даних.

6. Поняття «обробка» визначається як дії, в результаті яких персональні дані стають такими, що вийшли за межі відповідальності одного володільця та перейшли під відповідальність іншого. У контексті дослідження процедури здійснення обробки біометричних персональних даних, їх обігу чи навіть захисту є необхідним один важливий елемент - згода. Згода у вигляді законної підстави для обробки персональних даних має бути вільно вираженою, поінформованою та висловленою окремо. Якщо для звичайних персональних даних форма надання згоди – це прямо надана особою згода, або особа своїми діями прямо показала, що погоджується; то для біометричних персональних даних форма згоди має бути обов`язково висловленою.

7. Дослідивши порядок використання та межі використання і обігу біометричних персональних даних в Україні та зарубіжних країнах, ми дійшли висновку, що такі країни як Польща, Угорщина, Німеччина, Швеція, Франція мають закріплений законодавчо обов`язок всіх операторів, всіх форм власності, що здійснюють обробку як персональних даних, так і біометричних персональних даних, реєструватись, відповідно у даних європейських країнах є облік операторів, що здійснюють обробку біометричних персональних даних, що є відмінним і дуже ефективним засобом захисту біометричних персональних даних осіб. У Франції та Швеції, окрім обов`язку реєструвати та вести облік операторів, що здійснюють обробку біометричних персональних даних, законодавчо закріплено обовязок ліцензувати відповідних операторів обробки біометричних персональних даних, що унеможливлює порушення права на захист біометричних персональних даних з боку такого оператора. Ми визначили, що Україні не вистачає законодавчо закріпленого обов`язку обліку операторів, що здійснюють обробку біометричних персональних даних. Українським законодавством визначено перелік операторів, що здійснюють

обробку біометричних персональних даних на державному рівні, але, на привеликий жаль, не визначено обов`язку реєструватись іншим операторам біометричних персональних даних у приватному праві, і самі ці оператори становлять ризик для субєкта персональних даних порушення їх відповідного права.

8. Зміст адміністративно-правових відносин складається із суб`єктивних адміністративних прав суб`єктів адміністративного правовідношення та їх юридичних обов`язків. В свою чергу, суб`єктивними адміністративними правами суб`єктів адміністративно-правових відносин є передбачена адміністративно-правовим законодавством міра можливої поведінки учасників адміністративно-правових відносин у контексті задоволення їх публічних інтересів та потреб, що забезпечується певними адміністративними обов`язками інших осіб, а також гарантується державним примусом. А відповідно, юридичні обов`язки і є мірою необхідної поведінки, що має нормативно встановлені межі, а їх реалізація забезпечується нормами адміністративного права та державою. Таким чином змістом адміністративно-правових відносин є фактичні суспільні відносини, які через норми адміністративного права мають закріплену адміністративно-правову форму, визначають адміністративні права та юридичні обов`язки суб`єктів відповідних відносин.

Об’єктом правовідносин в сфері захисту персональних даних вважаються відповідні персональні дані, що обробляються у визначених базах даних, зокрема базах персональних даних. Таким чином, персональні дані – це відомості про особу, за якими остання може бути ідентифікованою.

Об’єкт адміністративно-правових відносин – це відповідні біометричні дані, що становлять  сукупність даних про особу, які відповідно були зібрані шляхом фіксації її характеристик, стабільних та таких, що істотно відрізняються від відомостей про іншу особу (мається на увазі відцифрований підпис чи образ обличчя, відбитки пальців чи сітківки ока тощо).

Суб'єктами відносин, що пов`язані з персональними даними є суб'єкт даних, володілець та розпорядник бази персональних даних, третя особа, державні органи та посадові особи, що уповноважені у сфері захисту персональних даних. Суб’єкт біометричних персональних даних як обов’язковий учасник вищезгадуваних відносин завжди є індивідуальною фізичною особою. Адже сама сутність та характер даних, носієм яких є фізична особа зосереджується у терміні «персональні».

Фізична чи юридична особа, що може бути суб’єктом адміністративно-правових відносин у сфері обігу та захисту біометричних персональних даних повинна мати правосуб’єктність як політико-юридичний стан визначеної особи та складається з трьох елементів: правоздатності, дієздатності та деліктоздатності. Кожне з цих трьох елементів слід дослідити.

Не є ідентичними чи схожими поняття суб’єкта правовідносин та суб’єкта біометричних персональних даних, адже останні співвідносяться наступним чином. Відповідно до Закону України «Про захист персональних даних» суб’єктом персональних даних може бути будь яка фізична особа, персональні дані якої відповідно до Закону підлягають обробці.

9. У дисертації визначено, що адміністративно-правовий статус особи як відповідна частина загального статусу особи може визначатись обсягом і характером адміністративної правосуб’єктності такої особи, тобто сукупністю адміністративної дієздатності та відповідно адміністративної правоздатності. У національному законодавстві право на захист біометричних персональних даних є структурним елементом конституційного права на недоторканість особистого життя, яке означає виключення можливості здійснення будь-яких операцій чи дій з біометричними персональними даними за відсутності згоди субєкта відповідних даних. Вищезазначеними діями є закріплені статтею 32 Конституції України, зберігання, збір, використання та поширення тощо, і закріплені Законом України «Про захист персональних даних» - збирання, систематизація, накопичення, зберігання, уточнення, оновлення чи зміна, використання, розповсюдження, передача, знеособлення, блокування,

знищення (а загалом - обробка біометричних персональних даних). Суспільні відносини, що стосуються права захисту біометричних персональних даних, хоч і є в основному інформаційними, але мають у своїй структурі ще конституційні правовідносини та адміністративно-правові, адже до адміністративно-правових відносин саме і належить правовий статус фізичної особи – суб`єкта біометричних персональних даних.

10. Забороняється втручання в особисте і сімейне життя людини, крім випадків, передбачених Конституцією України відповідно до статті 32 останньої. Таим чином, збирання, а також використання інформації чи її зберігання, у тому числі поширення конфіденційної інформації про особу без її згоди не допускається, однак наявні випадки здійснення вищезазначених дій з конфіденційною інформацією в інтересах економічного добробуту та прав людини, а також національної безпеки.

Суб'єкти правовідносин, які законом визначаються як такі, що беруть участь у захисті та обігу біометричних персональних даних мають відповідну можливість, практично всі органи державної влади та місцевого самоврядування є такими суб'єктами, адже законодавчо мають повноваження, що дотичні до захисту, обігу та обробці біометричних персональних даних. Президент України, який відповідно до Конституції України має гарантувати додержання прав та свобод людей тощо, Верховна Рада України, яка через власну законодавчу функцію має виступати гарантом забезпечення прав та свобод людини та відповідно Уповноважений Верховної Ради України з прав людини, основним завданням якого є парламентський контроль, зокрема, у контексті дотримання законодавства щодо захисту, обігу та обробки біометричних персональних даних відповідно до Регламенту Європейського Союзу про захист даних та Закону України «Про захист персональних даних». Так само органи місцевого самоврядування, які відповідно до Конституції України мають забезпечувати дотримання на місцевому рівні прав людей тощо, а також суди, які у відповідності до Закону України «Про захист персональних даних» разом із Уповноваженим Верховної Ради України з прав

людини здійснюють контроль за дотриманням законодавства у сфері обігу, обробки та захисту біометричних персональних даних.

11. Практика Європейського суду з прав людини та загалом європейського законодавства протягом останніх років ЄС має значну кількість захисних інструментів щодо персональних даних фізичної особи, про що свідчать предметні Рішення Європейського суду з прав людини. Нажаль відповідна судова практика відсутня на національному рівні.

Процес захисту персональних даних відповідно до міжнародного законодавства здійснюється також шляхом обробки персональних даних через автоматизовані системи. Процес обробки даних, які зберігаються у файлах для автоматизованої обробки здійснюється відповідно до профільної Конвенції Ради Європи у контексті захисту осіб під час автоматизованої обробки їх даних.

Положення вищезазначеного нормативно-правового акту надають можливість закріпити у національному законодавстві процедуру захисту щодо ручної обробки, але скориставшись цією можливістю про останнє держави-члени мають повідомляти про це у своїх заявах на ім'я Генерального Секретаря Ради Європи. Також у міжнародному законодавстві, як в Конвенції, так і в Директиві, наводиться визначення поняття «обробка персональних даних», воно визначається як будь-яка операція, здійснювана з персональними даними, зокрема реєстрація, організація чи збір, адаптація, зміна чи зберігання, а також консультація та пошук, разом з тим використання, розкриття за допомогою передачі, чи відповідно поширення, інше надання, упорядкування, а також комбінування, знищення, стирання чи блокування.

Судова практика у контексті розгляду справ з таким елементом як біометричні персональні дані не суттєва на національному рівні, і передбачає використання судової практики Європейського суду з прав людини, а у контексті національної практики ґрунтується на принципі переважного забезпечення прав володільця баз даних.

12. В Україні законодавчий інструментарій стосовно захисту, обігу та обробки біометричних персональних даних як елемента прав особи відбувається достатньо повільно, зокрема наразі порядок роботи з біометричними персональними даними як із спеціальним видом персональних даних закріплений лише у Роз`ясненнях Уповноваженого Верховної Ради України з прав людини. Національне законодавство слід удосконалювати та доповнювати, адже Роз`яснення Уповноваженого Верховної Ради України з прав людини не достатньо для забезпечення ефективного порядку обробки, обігу та захисту біометричних персональних даних, як особливого виду персональних даних. Також загалом національній правовій системі не вистачає ефективного інструментацію забезпечення обігу, обробки та захисту біометричних персональних даних.

Тому, з огляду на вищезазначене пропонуємо внести зміни до Закону України «Про захист персональних даних» шляхом зазначення загального порядку роботи з особливими видами персональних даних, та окремо щодо кожного, зокрема з біометричними персональними даними.

13. Законі України «Про захист персональних даних» як в профільному нормативно-правовому акті передбачити загалом, які біометричні персональні дані взагалі не підлягають збиранню, вказати їх перелік, адже із значним розвитком інформаційного суспільства важко уявити, які біометричні персональні дані особи збиратимуться через рік, а переліку заборонених до збирання біометричних даних, або дозволених до збирання біометричних персональних даних у Законі України «Про захист персональних даних» нема.

14. Обіг біометричних персональних даних є вразливим на сьогодні в Україні, незахищеним через відсутність дієвих, законодавчо прописаних, інструментів захисту незаконного використання біометричних персональних даних. Окрім підзаконних нормативно-правових актів в Україні відсутні нормативні документи, які визначають механізм чи алгоритм роботи з персональними даними, а отже – унеможливлюють контроль за порядком використання та обігу білометричних персональних даних. Центральні органи

у сфері формування державної політики у визначеній галузі мають ініціювати розроблення на законодавчому рівні дієвого прописаного алгоритму роботи в Україні з біометричними персональними даними.

15. Опрацювавши текст проекту Закону України «Про захист персональних даних» (реєстраційний № 5628 від 07.06.2021) було виявлено ряд новел, які ефективно впливатимуть на врегулювання використання та обробки біометричних персональних даних та персональних даних загалом. Зокрема законопроектом запропоновано визначити поняття послуги інформаційного суспільства як надання оплатних чи безоплатних послуг або ж товарів у результаті наявності вимоги отримувача шляхом укладення правочину засобами дистанційного зв'язку, інформаційними електронними послугами.

16. У результаті дослідження питання відповідальності за незаконне використання та обіг біометричних персональних даних зазначаємо, що відповідальність за порушення права на захист персональних даних має бути такою, що зупинить або попередить настання шкоди персональним даним особи. Таким чином, сьогодні відповідно до статті 188-39 Кодексу України про адміністративні правопорушення за порушення у сфері поводження з персональними даними передбачено штраф, максимальний розмір якого є дещо більшим ніж 30 тисяч гривень. У свою чергу, зберігання, незаконне збирання, знищення або використання, а також поширення конфіденційної інформації про особу, крім того незаконна зміна такої інформації несе за собою притягнення до кримінальної відповідальності згідно із статтею 182 Кримінального кодексу України. Слід наголосити, що кримінальна відповідальність може бути застосована виключно до юридичних осіб, а фізичні особи у разі незаконного збирання, зберігання, використання, знищення чи поширення конфіденційної інформації про особу лише нестимуть адміністративну відповідальність, що була визначена вище.

17. Ми переконані у необхідності врегулювання меж обігу біометричних персональних даних, визначенні поняття біометричних даних на

законодавчому рівні, співвіднесення біометричних та генетичних даних та урегулювання захисту біометричних персональних даних, що є можливим шляхом зміни Закону України «Про захист персональних даних» або шляхом прийняття Верховною Радою Уаїни проекту Закону України «Про захист персональних даних» (реєстраційний № 5628 від 07.06.2021).

# СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ


1. Адміністративне право України: підручник / Ю. П. Битяк, В. М. Гаращук, О. В. Дьяченко та ін.; за ред. Ю. П. Битяка. К.: Юрінком Інтер, 2006. 544 с.
2. Адміністративне право України. Академічний курс: підручник: у 2-х томах: Том 1. Загальна частина / ред. колегія: В. Б. Авер'янов. К.: Юридична думка, 2004. – 584 с.
3. Административное право Российской Федерации: учеб. пособие / А. П. Алехин, Ю. М. Козлов, А. А. Кармолицкий. М.: Зерцало, 2009. Ч.1. 528 с.
4. Алексеев С. С. Общая теория права: в 2-х т. / С. С. Алексеев. – М.: Юрид. лит., 1981. Т. 1. 360 с.
5. Алексеев С.С. Общие дозволениям и общие запреты в советском праве. – М., 1989. С. 243.
6. Амелин Р. В., Волков Ю. В., Марченко Ю. А. Комментарий к Федеральному закону от 27.06.2006 № 152-ФЗ «О персональных данных» (постатейный). СПС КонсультантПлюс, 2013.
7. Ануфриев Е. А. Социальный статус и активность личности. Личность как объект и субъект социальных отношений / А. Е. Ануфриев. М.: Изд-во МГУ, 1984. 288 с.
8. Адміністративне право України: основні категорії та поняття : [навч. посібник] / [В.І. Загуменник, В.В. Мусієнко, В.В. Проценко] ; за заг. ред. О.Х. Юлдашева. К. : Поліграфіст, 2010. 512 с.
9. Арістова І. В. Державна інформаційна політика: організаційноправові аспекти : монографія / Арістова І. В. ; за загальною редакцією дра юрид. наук, проф. Бандурки О. М. Харків : Видво унту внутр. справ, 2000. 368 с.
10. Биометрика. URL: http://dic.academic.ru/dic.nsf/dic_fwords/49896/
11. Биометрия // Юридический словарь. URL: http://dic.academic.ru/

12. И. Л. Информационное право. Учебник для магистров. Гриф МО РФ. 3-е изд. М: Юрайт, 2013. 576 с.

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

14. Брижко В. М. Приватність даних у хмарних технологіях. URL: http://ippi.org.ua/brizhko-vm-privatnist-danikh-u-khmarnikh-tekhnologiyakh-stor-47-59

15. Бляхман Б. Я. Правовой режим в системе регулирования социальных отношений / Б. Я. Бляхман. Кемерово, 1999. С. 21.

16. Богатир В. Щодо контролю Уповноваженим ВРУ з прав людини за дотриманням порядку внесення відомостей, які містять персональні дані до Єдиного Реєстру Досудових Розслідувань. URL: https:.dostup.pravda.com.ua/request/shchodo_kontroliu_upovnovazhieni (дата звернення: 12.05.2022).

17. Бояринцева М. Адміністративно-правовий статус громадян: до питання про склад елементів. Право України. 2002. № 8. С. 21-25.

18. Бурило Ю.П. Організаційно-правові питання державного управління в інформаційній сфері.: Дис. канд. наук: 12.00.07 2008. URL: http:.adminpravo.com.ua/index.php/20100413140513/14520100928132730/194222.html (дата звернення: 10.05.2022).

19. В.М. Брижко, О.М. Гальченко, В.С. Цимбалюк, О.А. Орєхов, А.М. Чорнобров. Інформаційне суспільство. Дефініції: людина. Її права, інформація, інформатика, інформатизація, телекомунікації, інтелектуальна власність, ліцензування, сертифікація, економіка, ринок, юриспруденція/За ред. Доктора юридичних наук, професора, Р.А. Калюжного, доктора економічних наук М.Я. Швеця.-К.: «Інтеграл», 2002. С. 145.

20. Витрук Н. В. Основы теории правового положения личности в социалистическом обществе / Н. В. Витрук. М., 1979. 229 с.

21. Вакарюк Л. Основні підходи до розуміння поняття «правовий режим». Підприємництво, господарство і право. 2016. № 12. С. 196-201.

22. Войтович П.П. Международное право. Національний Університет «Одеська юридична академія» Міжнародноправове регулювання обмеження розповсюдження приватної інформації. Право. №13. URL: http:.www.rusnauka.com/27_OINXXI_2011/Pravo/13_92801.doc.htm (дата звернення: 20.05.2022).

23. Галунько В.В. Єщук О.М. Поняття та зміст адміністративно-правового регулювання. Actual problems of corruption prevention and counteraction. 2011. URL: http:.www.lawproperty.in.ua/ (дата звернення: 17.05.2022).

24. Горшенев В. М. Структура правового статуса гражданина в свете Конституции СССР 1977г. / В. М. Горшенев // Правопорядок и правовой статус личности в развитом социалистическом обществе в свете Конституции СССР 1977 г. Саратов: Издво Сарат. ун-та, 1980. С. 51–58.

25. Гумін О. М. Адміністративно-правове забезпечення: поняття та структура / О. М. Гумін, Є. В. Пряхін // Наше право. 2014. № 4. С. 46-50. URL: http://nbuv.gov.ua/UJRN/Nashp_2014_4_9

26. Горбач А. М. Зміст адміністративно-правових відносин: теорія та практика/ А. М. Горбач// Науковий вісник Ужгородського національного університету, 2017.Серія Право. Випуск 43. Том 3. С. 91-96. URL: http://www.visnyk-juris.uzhnu.uz.ua/file/No.43/part_3/20.pdf

27. Гербут В. С. Правовідносини в сфері захисту персональних даних про стан здоров`я людини/ В. С. Гербут// Науковий вісник Ужгородського університету, 2012. Серія Право, випуск 18.С. 146-149. URL: https://dspace.uzhnu.edu.ua/jspui/bitstream/lib/12993/1/98.pdf

28. Геращенко припускає контроль за дотриманням карантину через моніторинг мобільних мереж. Радіо Свобода : веб-сайт. URL: https://www.radiosvoboda.org/a/news-herashchenko-kontrol-za-karantynom-cherez-mobilni/30505782.html (дата звернення: 17.05.2022)

29. Гронь О.В. Погореленко А.С. Проблеми захисту персональних даних у контексті сучасної комунікації. Науковий вісник Ужгородського національного університету. Випуск 19. Ч. 1. 2018. С. 102-108.

30. Гуцалюк М. Ідентифікація фізичних осіб в Україні // Правова інформатика.2005.№ 3 (7).С. 43- 47.

31. Директива 97/66/ЄС Європейського Парламенту і Ради «Стосовно обробки персональних даних і захисту права на невтручання в особисте життя в телекомунікаційному секторі» від 15 грудня 1997 року URL : http://zakon.rada.gov.ua/laws/show/994_243

32. Директива про захист персональних даних, пп. 16 і 17 преамбули; рішення ЄСПЛ у справі «П.Г. і Дж.Х. проти Сполученого Королівства» (P.G. and J.H. v. the United Kingdom), No 44787/98 від 25 вересня 2001 р., пп. 59 та 60; рішення ЄСПЛ у справі «Віcс проти Франції» (Wisse v. France), No 71611/01 від 20 грудня 2005 р. 66 СЄС, С 101/01, «Боділ Ліндквіст» (Bodil Lindqvist) від 6 листопада 2003 р., п. 51.

33. Директива 95/46/ЄС Європейського Парламенту і Ради "Про захист фізичних осіб при обробці персональних даних і про вільне переміщення таких даних" № 994_242, в редакції від 24.10.1995. URL: http://pgp-journal.kiev.ua/archive/2018/4/7.pdf

34. Додатковий протокол до Конвенції про захист осіб у зв'язку з автоматизованою обробкою персональних даних щодо органів нагляду та транскордонних потоків даних : Міжнародний документ від 08.11.2001 URL : http://zakon4.rada.gov.ua/laws/show/994_363.

35. Директиви 95/46/ЄС (Загальний регламент про захист даних)» від 27 квітня 2016 року. Офіційний переклад українською мовою. URL: https://www.kmu.gov.ua/storage/app/media/uploaded-files/es-2016679.pdf

36. Додаток мобільний «Дія». URL: https://play.google.com/store/apps /details?id=ua.gov.diia.app (дата звернення: 17.05.2022).

37. Додаток «Дія»: як працює головний цифровий сервіс України. Телеканал ZIK : веб-сайт URL: https://zik.ua/article/dodatok_diia_yak_pratsiuie_holovnyi_tsyfrovyi_servis_ukrainy_958536 (дата звернення: 17.05.2022).

38. Дозвіл на оброблення персональних даних хворих не дозволяє ЗМІ поширювати цю інформацію – юридичне роз'яснення. Інститут масової інформації: веб-сайт. URL: https://imi.org.ua/monitorings/dozvil-na-obrobku personalnyh-danyh-hvoryh-ne-dozvolyaye-zmiposhyryuvaty-tsyu-informatsiyu-i32661 (дата звернення: 14.05.2022).

39. Експерти із захисту даних застерігають від використання сканеру відбитків пальців на новому смартфоні Apple. URL: https://ms.detector.media/web/online_media/eksperti_iz_zakhistu_danikh_zasterigayut_vid_vikoristannya_skaneru_vidbitkiv_paltsiv_na_novomu_smartfoni_apple/

40. Заярний О. А. Деякі проблеми правового забезпечення правомірної обробки біометричних персональних даних у процесі використання інтернету речей/ матеріали 2-ї науково-практичної конференції "Інтернет речей: проблеми правового регулювання та впровадження". К. 2018.С. 93-96.

41. Зуй В. В. Адміністративно-правовий статус громадян в Україні / В. В. Зуй // Правова держава Україна: Проблеми, перспективи розвитку: Короткі тези доп. та наук. повід. респ. н-пр. конфер. 9-11 лист. 1995. Х., 1995. С. 107–108.

42. Загальний регламент про захист даних. URL: https://uk.wikipedia.org/wiki/

43. Захист персональних даних. Правове регулювання та практичні аспекти: [науково-практичний посібник]/М. В. Бем, І. М. Городинський, Г. Саттон та ін.. К.:К.І.С., 2015. 220 с.

44. Загальна Декларація прав людини ООН від 10 грудня 1948 року URL: http://zakon2.rada.gov.ua/laws/show/995_015?test=XX7MfyrCSgkyS5FIZiTwXTZNHdlyUsFggkRbI1c.

45. Загальна декларація прав людини : Міжнародний документ від 10.12.1948 URL: http://zakon4.rada.gov.ua/laws/show/995_015.

46. Інформаційне законодавство : Збірник законодавчих актів: У 6 т./ За заг. ред. Ю. С. Шемшученка, І. С. Чижа. Т. 5. Міжнародно-правові акти в інформаційній сфері. К. : ТОВ «Видавництво «Юридична думка», 2005. 328 с.

47. Ільницький М. П. Адміністративно-правове забезпечення доступу до баз даних в публічному управлінні в Україні. Науковий вісник УжНУ. Серія: Право Спецвипуск. 2013. С. 74 – 78.

48. Ільницький М.П. Адміністративно-правове регулювання захисту персональних даних, що містяться в електронних офіційних реєстрах в Україні / М.П.Ільницький // Порівняльно-аналітичне право. 2016. № 4. С. 289 -292.

49. Иоффе О. С. Правоотношения по советскому гражданскому праву. Л.: изд-во ЛГУ, 1949. 141 с.

50. Конвенція про захист осіб у зв'язку з автоматизованою обробкою персональних даних : Міжнародний документ від 28.01.1981 URL: http://zakon4.rada.gov.ua/laws/show/994_326.

51. Конвенція про захист прав людини і основоположних свобод : Міжнародний документ від 04.11.1950 URL : http://zakon4.rada.gov.ua/laws/show/995_004.

52. Колесников Є.Є. Поняття та особливості адміністративно-правового забезпечення захисту прав споживачів / Є.Є. Колесников // Форум права. 2011. № 2. С. 432-438.

53. Конвенція № 108 Ради Європи про захист осіб у зв'язку з автоматизованою обробкою їх персональних даних від 28.01.1981р. № 994_326; ратифікована Україною 06.07.2010 року . URL: https://zakon.rada.gov.ua/laws/show/994_326

54. Конвенція про захист прав людини та основоположних свобод. URL: https://zakon.rada.gov.ua/laws/show/995_004#Text (дата звернення: 17.05.2022).

55. Конституція України. Документ № 254к/96-ВР. URL: https://zakon.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80

56. Корж І. Ф. Трансформація суспільних відносин у процесі утворенням об’єднаних територіальних громад. Інформація і право. 2020. № 2(33). С. 149-157.

57. Кравчук М. М. Міжнародний досвід правового регулювання захисту персональних даних у мережі інтернет. URL: file:///C:/Users/User/Downloads/Nzizvru_2013_3_24.pdf

58. Конвенція № 108 Ради Європи про захист осіб у зв'язку з автоматизованою обробкою їх персональних даних від 28.01.1981р. № 994_326; ратифікована Україною 06.07.2010 року . URL: https://zakon.rada.gov.ua/laws/show/994_326

59. КСУ взявся за подання Денісової щодо накопиченої в поліції біометрики. Укрінформ. URL: https://www.ukrinform.ua/rubric-society/2536965-ksu-vzavsa-za-podanna-denisovoi-sodo-nakopicenoi-v-policii-biometriki.html

60. Лист Уповноваженого Верховної Ради України з прав людини «Щодо захисту персональних даних» від 03.03.2014 року № 2/9-227067.14-1/НД-129

61. Ляхович У. І. Організаційно-правове забезпечення реалізації адміністративноправового статусу державного службовця: дис… канд. юрид. наук: спец. 12.00.07 / Уляна Іванівна Ляхович. К., 2008 // URL: http:// adminpravo.com.ua

62. Малиновський В. Я. Державне управління: навч. посібник / В. Я. Малиновський. К.: Атіка, 2003. 576 с.

63. Матузов Н. И. Личность, права, демократия. Теоретические проблемы субъективного права / Н. И. Матузов. Саратов: Изд-во Сарат ун-та, 1972 292 с.

64. Матузов Н.И., Малько А.В. Правовые режимы: вопросы теории и практики // Правоведение. 1996. №1. С. 17.

65. Максименко Ю. Е. Теоретико-правові засади забезпечення інформаційної безпеки України. Дисертація кандидата юридичних наук :12.00.01 / Київський Національний університет внутрішніх справ. Київ 2007. С. 41.

66. Мінцифра використовує big data для боротьби з пандемією. Міністерство та Комітет цифрової трансформації України : вебсайт. URL: https://thedigital.gov.ua/news/mintsifra-vikoristovue-big-data-dlya-borotbi-z-pandemieyu (дата звернення: 17.05.2022).

67. Новоселов В. И. Правовое положение граждан в советском государственном управлении / В. И. Новоселов. Саратов: Изд-во Сарат. ун-та, 1976. 216 с.

68. Общая теория права и государства: учебник / под ред. В. В. Лазарева. – М.: Юристь, 2001. 520 с.

69. Олійник А.Ю. Конституційно-правовий механізм забезпечення основних свобод людини і громадянина в Україні: Монографія. /А.Ю. Олійник К.: Алерта, КНТ, Центр навчальної літератури, 2008. 472 с.

70. Омбудсмен закликає Януковича ветувати закон про біометричні паспорти. Радіо Свобода. URL: https://www.radiosvoboda.org/a/24740263.html

71. Офіційна веб-сторінка Уповноваженого Верховної Ради України з прав людини. Розділ Секретаріат Уповноваженого. URL: http://www.ombudsman.gov.ua/ua/page/secretariat/

72. Про Національну поліцію. Закон України № 580-VIII в редакції від 01.01.2019. URL: https://zakon.rada.gov.ua/laws/show/580-19

73. Про Уповноваженого Верховної Ради України з прав людини. Закон України № 776/97-ВР, в редакції від 04.11.2018.

74. Про Стратегію сталого розвитку «Україна – 2020»: Указ Президента України; Стратегія від 12.01.2015 р. № 5/2015 URL: http://zakon4.rada.gov.ua/laws/show/5/2015 (дата звернення 19.05.2022)

75. Писарев О. Омбудсмен просить КС заборонити правоохоронцям створювати ДНК-базу громадян. URL: https://zib.com.ua/ua/127637-ombudsmen_zvernulasya_do_ks_schodo_zboru_ zrazkiv_dnk_policie.html

76. Про доступ до публічної інформації. Закон України № 2939-VI, в редакції від 01.05.2015. URL: https://zakon.rada.gov.ua/laws/main/2939-17

77. Про інфоррмацію. Закон України № 2657-XII, в редакції від 01.01.2017. URL: https://zakon.rada.gov.ua/laws/main/2657-12

78. Про лікарські засоби. № 123/96-ВР, в редакції від 04.11.2018. URL: https://zakon.rada.gov.ua/laws/main/123/96-%D0%B2%D1%80

79. Про затвердження Порядку ведення Реєстру пацієнтів в електронній системі охорони здоров'я : Наказ Міністерства охорони здоров'я України від 30.11.2020 № 2755. Офіційний вісник України. 2021. 29 січ. (№ 7). Ст. 452.

80. Про доступ до судових рішень. Закон України № 3262-IV, в редакції від 15.12.2017 URL: https://zakon.rada.gov.ua/laws/main/3262-15

81. Публічна інформація та інформація суспільного інтересу: Аналітичний матеріал за результатами реалізації проекту «Інформація про публічних осіб та впровадження систем обліку публічної інформації»; за заг. ред. Булгакової М.Г., Львів: ЕДЦ «Правова аналітика», К. С. 24.

82. Попов А. О. Зарубіжний досвід правового регулювання захисту відомчих інформаційних ресурсів / А. О. Попов // Форум права. 2009. № 3. С. 513–519.

83. Про судову практику у справах про захист гідності та честі фізичної особи, а також ділової репутації фізичної та юридичної особи: Постанова Пленуму Верховного Суду України № 1 від 27 лютого 2009 року // URL: http://zakon4.rada.gov.ua/laws/show/v _001700-09

84. Пазюк А. В. Міжнародно-правовий захист права людини на приватність персоніфікованої інформації : дис. ... канд. юрид. наук / А. В. Пазюк . К., 2004 р. 205 с.

85. Пазюк А. В. Захист прав людини стосовно обробки персональних даних: міжнародні стандарти. МГО Прайвесі Юкрейн. К. : Інтертехнодрук, 2000 р. URL: https://docs.google.com/document/d/1hvVJPeoCVqBAauBZWjopyn58h1VbBehAucIDV0uYEQU/edit?hl=ru&pli=1.

86. Панчишин А. В. Поняття, ознаки та структура категорії «правовий статус» / А. В. Панчишин // Часопис Київського університету права. 2010. № 2. С. 95–98.

87. Питання вдосконалення законодавства України у сфері інформації та інформатизації. Л. Задорожня, М. Коваль, В. Брижко та ін.; за ред. М.Я. Швеця. К.: Футарі-Прінт, 2005. с. 21.

88. Про захист персональних даних: Закон України від 01.06.2010 р. № 2297-VI. : URL: http://zakon4.rada.gov.ua/laws/show/2297-17/page.

89. Проект Закону України «Про захист персональних даних» (реєстраційний № 5628 від 07.06.2021). URL: http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=72160

90. Пазюк А. В. Захист прав людини стосовно обробки персональних даних: міжнародні стандарти / А. В. Пазюк // МГО Прайвесі Юкрейн К. : Інтертехнодрук, 2000. 69 с.

91. Про затвердження плану дій щодо поглиблення співробітництва між Україною та Організацією економічного співробітництва та розвитку на 2013-2016 роки : Розпорядження Кабінету Міністрів України від 06.02.2013 № 132-р URL: http://zakon4.rada.gov.ua/laws/show/132-2013-р.

92. Про персональні дані. Закон України № 2297-VI, у редакції від 30.01.2018. URL: https://zakon.rada.gov.ua/laws/show/2297-17

93. Посібник з європейського права у сфері захисту персональних даних. К. : К.І.С., 2015. 115 с.

94. Про Національну програму інформатизації: Закон України від 4 лютого 1998 року // Відомості Верховної Ради України. 1998. № 27-28. Ст. 181.

95. Про Державну службу спеціального зв'язку та захисту інформації України: Закон України в редакції від 09 квітня 2014 року // Відомості Верховної Ради України. 2014. № 25. Ст. 89.

96. Про затвердження Правил забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних

системах: Постанова Кабінету Міністрів України від 29 березня 2006 року № 373 // Офіційний вісник України. 2006. № 13. Ст. 878.

97. Різак М. В. Особливості правового регулювання безпеки обігу «вразливих» персональних даних в Україні / М. В. Різак // Наукові записки Інституту законодавства Верховної Ради України. 2012. № 2. С. 50–54.

98. Різак М.В. Забезпечення незалежності органу із захисту персональних даних, що є найважливішою вимогою європейських норм // Стенограма комітетських слухань на тему: «Збір та використання персональних даних про особу в контексті захисту прав людини». Комітет Верховної Ради України з питань прав людини, національних меншин і міжнаціональних відносин. URL: http://kompravlud.rada.gov.ua/.

99. Римарчук Г.С. Адміністративно-правове забезпечення права інтелектуальної власності: автореф. дис. … канд. юрид. наук: 12.00.07 / Г.С. Римарчук. Львів, 2013. 18 с.

100. Регламент Європейського парламенту і Ради Європи «Про захист фізичних осіб у зв`язку з опрацюванням персональних даних і про вільний рух таких даних, та про скасування Директиви 95/46/ЄС (Загальний регламент про захист даних)» від 27 квітня 2016 року. Офіційний переклад українською мовою. URL: https://www.kmu.gov.ua/storage/app/media/uploaded-files/es-2016679.pdf

101. Роз’яснення Уповноваженого Верховної Ради України з прав людини від 08.01.2014 р. «Роз’яснення основних положень Порядку повідомлення Уповноваженого щодо визначення обробки персональних даних, яка становить особливий ризик для прав і свобод суб’єктів персональних даних»

102. Різак М. В. Діяльність Уповноваженого Верховної Ради України з прав людини щодо захисту персональних даних. URL: http://www.nvppp.in.ua/vip/2016/6/tom_1/12 .pdf

103. Роз’яснення до Порядку здійснення Уповноваженим контролю за додержанням законодавства про захист персональних даних № 0002715-14, в редакції від 08.01.2014

104. Річний звіт: Інституту медіа права URL: http://medialaw.kiev.ua/userimages/files/Annual_Report_MLI_ 2012_ukr.pdf

105. Рішення Святошинського районного суду м. Києва від 25 грудня 2013 року у справі №2608/18606/12 URL: http://www.reyestr.court.gov.ua/

106. Рішення Печерського районного суду м. Києва від 14 березня 2014 року у справі № 757/24796/13-ц URL: http://www.reyestr.court.gov.ua/

107. Рішення Житомирського окружного адміністративного суду від 01 березня 2018 року у справі № 806/3744/17. URL: http://www.reyestr.court.gov.ua/Review/72588232

108. Рішення ЄСПЛ у справі «Аманн проти Швейцарії» (Amann v. Switzerland) [ВП], No 27798/95 від 16 лютого 2000 р., п. 50; див. також рішення ЄСПЛ у справі «Копп проти Швейцарії» (Kopp v. Switzerland), No 23224/94 від 25 березня 1998 р., п. 55 та рішення ЄСПЛ у справі «Йордачі проти Молдови» (Iordachi and Others v. Moldova), No 25198/02 від 10 лютого 2009 р., п. 50.

109. Рішення ЄСПЛ у справі «Аманн проти Швейцарії» (Amann v. Switzerland) [ВП], No 27798/95 від 16 лютого 2000 р., п. 56; див. також рішення ЄСПЛ у справі «Малоун проти Сполученого Королівства» (Malone v. the United Kingdom), No 8691/79 від 2 серпня 1984р., п. 66; рішення ЄСПЛ у справі «Сільвер проти Сполученого Королівства» (Silver and Others v. the United Kingdom), NoNo 5947/72, 6205/73, 7052/75, 7061/75, 7107/75, 7113/75 від 25 березня 1983 р., п. 88.

110. Рішення ЄСПЛ у справі «Санді Таймс» проти Сполученого Королівства» (The Sunday Times v. the United Kingdom), No 6538/74 від 26 квітня 1979 р., п. 49; див. також «Сільвер проти Сполученого Королівства» (Silver and Others v. the United Kingdom), № № 5947/72, 6205/73, 7052/75, 7061/75, 7107/75, 7113/75 від 25 березня 1983 р., п. 8.

111. Саприкіна І.В. Захист честі, гідності, ділової репутації фізичної особи за законодавством України (за матеріалами судової практики): автореф. дис. на здобуття наук. ступеня канд. юрид. наук / І.В. Саприкіна. К., 2006. С. 17-18.

112. Скакун О. Ф. Теорія держави і права: підручник / О. Ф. Скакун. 2-ге вид. К.: Алерта; ЦУЛ, 2011. 520 с.

113. Салищева Н. Г. Административный процесс в СССР / Н. Г. Салищева. М.: Юрид. лит., 1964. 158 с.

114. Солодка О. М. Пріоритети удосконалення інформаційної безпеки України/ О. М. Солодка // Інформація і право. 2015. № 3. С.41.

115. Стеценко С.Г. Адміністративне право України: навч. посіб. / С.Г. Стеценко К.: Атіка, 2008. 624 с.

116. Сэмюэл Грингард. Интернет вещей: будущее уже здесь. / Сэмюэл Грингард. – изд. МАН Иванов и Ферберг. М. 2016. С.6.

117. Татаров О. Чи суперечать Конституції повноваження поліції щодо збору біометричних даних? URL: https://zib.com.ua/ua/127637-ombudsmen_zvernulasya_do_ks_schodo_zboru_zrazkiv_dnk_policie.html

118. Хартія основних прав Європейського Союзу, OJ. 2012. C. 326.

119. Теорія держави і права. Академічний курс: підручник / О. В. Зайчук, Н. М. Оніщенко. К.: Юрінком Інтер, 2008. 688 с.

120. Теремецький В. І., Цвірюк Д. В. Застосування зарубіжного досвіду правового захисту персональних даних в Україні. URL: http://e-pub.aau.edu.ua/index.php/chasopys/article/view/662

121. Теория государства и права / А. В. Малько, Н. И. Матузов. М.: Юристь, 1996. 672 с.

122. Толстой Ю. К. К теории провоотношения / Ю. К. Толстой. Л.: Изд-во Ленингр. ун-та, 1959. 87 с.

123. Томаш Л.В. Правовой режим: понятие и признаки / Л. В. Томаш // Научный вестник Чернивецького университета. 2005. Вып. 282. С. 25.

124. Тунік А. В. Захист персональних даних: аналіз національного законодавства / А. В. Тунік // Підприємництво, господарство і право. 2011. № 8. С. 97–102.

125. Фарбер И. Е. Свобода и права человека в советском государстве / И. Е. Фарбер. Саратов: Изд-во Сарат. ун-та, 1974. 187 с.

126. Травкин Ю. В. Персональные данные. М.: Амалданик, 2007. 432 с.

127. Цвік М.В. Загальна теорія держави і права: підруч / М.В. Цвік, В.Д. Ткаченко, Л.Л. Рогачова, О.В. Петришин, С.М. Олейников; М.В. Цвік (ред.). Х.: Право, 2002. 432 с.

128. Уряд зобов'язав Мінцифри забезпечити функціонування електронного сервісу «дій вдома», зокрема, інформаційної системи епідеміологічного контролю за поширенням COVID-19, що є частиною сервісу. УКРІНФОРМ : веб-сайт. URL: https://www.ukrinform.ua/rubricsociety/3011567-v-ukraini-zapuskaut-dodatok-dij-vdoma-dla-kontrolu-samoizolacii.html (дата звернення: 17.05.2022).

129. Шайкенов Н. А. Правовое обеспечение интересов личности / Н. А. Шайкенов. Свердловск: Изд-во Урал. ун-та, 1990. 200 с.

130. Шестаков С. В. Адміністративно-правовий статус працівника міліції: дис… канд. юрид. наук: спец. 12.00.07 / Сергій Володимирович Шестаков. Х., 2003. 203 с.

131. Щорічна доповідь Уповноваженого Верховної Ради України з прав людини про стан дотримання прав і свобод людини і громадянина. К., 2020. С. 70.

132. Щорічна доповідь Уповноваженого Верховної Ради України з прав людини про стан дотримання прав і свобод людини і громадянина в Україні. К., 2021. С. 194–199.

133. Щербина А.О. Адміністративно-правове регулювання використання персональних даних суб'єктами владних повноважень в Україні. Рукопис. Дисертація на здобуття наукового ступеня кандидата юридичних наук зі спеціальності 12.00.07 – адміністративне право і процес; фінансове право; інформаційне право. – Запорізький національний університет, Запоріжжя, 2020. С. 176.

134. Щербина А. О. Суспільний інтерес чи захист персональних даних: межі та пріоритети в умовах пандемії. Науковий вісник Ужгородського національного університету. Серія «Право». 2020. № 61. С. 135–141.

135. Як медикам працювати з персональними даними пацієнтів. Міністерство охорони здоров'я України: веб-сайт. URL: https://moz.gov.ua/article/for-medical-staff/jak-medikam-pracjuvati-z-personalnimi-danimi-pacientiv (дата звернення: 14.05.2022).

136. Mordini E., Tzovaras Second Generation Biometrics: The Ethical, Legal and Social Context. New York: Springer, 2012. 353 pp.

137. Franjieh Iris Biometric Model for Secured Network Access. NY: CRC Press, 2013. 220 pp.

138. Newbold R. Newbold's Biometric Dictionary For Military And Industry. 2nd ed. NY: Authorhouse, 2008. 236 pp.

139. Gavrilova M., Monwar M. Multimodal Biometrics and Intelligent Image Processing for Security Systems. NY: IGI Gloabal, 2013. 232 pp.

140. The Freedom of Information Act // 2013. URL: http://www.justice.gov/oip/foia_ updates/Vol_XVII_4/page2.htm

141. The Fair Credit Reporting Act // 2013. URL: http://www.ftc.gov/os/statutes/031224fcra.pdf

142. The Privacy Act of 1974 // 2013. URL:www.justice.gov/opcl/privstat.htm

143. U.S. Department of Health & Human Services. Health In surance Portability and Accountability Act of 1996 URL: https://www.cms.gov/HIPAAGenInfo/Downloads/HIPAALaw.pdf

144. Teleservices Data Protection Act URL: http://ourworld.compuserve.com/homepages/ckune r/multimd3.htm.

145. Prins (n 23). 32 A29WP, WP 80 (n 7) 10.

146. Ibid footnote 11, 5. 34 A29WP, Opinion 3/2012, WP 193 (n 8) 7.

147. A29WP, 'Opinion 4/2007 on the concept of personal data' (20 June 2007) 01248/07/EN WP 136, 8.

148. EDPS, 'Opinion on a Research Project Funded by the European Union under the Seventh Framework Programme (FP7) for Research and Technology Development - Turbine (TrUsted Revocable Biometric IdeNtitiEs)' (1 February 2011) (hereinafter Opinion on Turbine Project).

149. A29WP, Opinion 3/2012, WP 193 (n 8).

150. European Commission, Proposal for the General Data Protection Regulation (n 16), art 4(11).

# ВЕРХОВНА РАДА УКРАЇНИ

**Комітет з питань гуманітарної та інформаційної політики**

01008, м. Київ-8, вул. М. Грушевського, 5, тел.: 255-24-36, факс: 255-39-64

Акт

впровадження результатів дисертаційного дослідження аспірантки Київського національного університету імені Тараса Шевченка Бойко Анни Миколаївни на тему «Адміністративно-правове забезпечення обігу та захисту біометричних персональних даних» у законотворчу діяльність

Наукові положення дисертаційного дослідження аспірантки інституту права Київського національного університету імені Тараса Шевченка Бойко Анни Миколаївни на тему: «Адміністративно-правове забезпечення обігу та захисту біометричних персональних даних», були подані у вигляді обґрунтованих пропозицій до удосконалення законодавства.

В дисертації запропоновані зміни до законодавчих актів в частині захисту біометричних персональних даних з урахуванням зарубіжного досвіду, зокрема до Закону України «Про захист персональних даних в Україні».

Положення дисертаційного дослідження Бойко Анни Миколаївни на здобуття наукового ступеня доктора філософії з права є актуальними, мають необхідний теоретичний і методологічний рівень, практичне значення та характеризуються науковою новизною і можуть бути враховані у процесі вдосконалення чинного законодавства України.

**Голова Комітету** **Микита Потураєв**

# КИЇВСЬКА МІСЬКА РАДА

IX СКЛИКАННЯ

**ПОСТІЙНА КОМІСІЯ З ПИТАНЬ ЦИФРОВОЇ ТРАНСФОРМАЦІЇ ТА АДМІНІСТРАТИВНИХ ПОСЛУГ**

*01044, м. Київ, вул. Хрещатик, 36, .....* *тел./факс: (044) 202-71-07*

04.02.2022 № 08/197-1 вих

на № _____ від _____

Київський національний університет імені Тараса Шевченка

*Акт впровадження результатів дисертаційного дослідження*

Наукові положення та пропозиції, викладені у дисертаційному дослідженні аспірантки інституту права Київського національного університету імені Тараса Шевченка Бойко Анни Миколаївни на тему: «Адміністративно-правове забезпечення обігу та захисту біометричних персональних даних» є обґрунтованими, ефективними та можуть бути враховані під час функціонування постійної комісії з питань цифрової трансформації та адміністративних послуг, а також під час підготовки проектів рішень Київської міської ради у сфері цифрової трансформації та адміністративних послуг.

Разом із тим, положення дисертаційного дослідження Бойко Анни Миколаївни на здобуття наукового ступеня доктора філософії є актуальними під час розробки та вдосконалення нормативно-правових актів місцевого значення.

Заступник голови комісії Ксенія СЕМЕНОВА

# ДЕПУТАТ

КИЇВСЬКОЇ МІСЬКОЇ РАДИ IX СКЛИКАННЯ

«03» листопада 2022 р. № 08/231/07/08-43

*Щодо впровадження результатів дисертаційного дослідження аспірантки Київського національного університету імені Тараса Шевченка Бойко Анни Миколаївни тему «Адміністративно-правове забезпечення обігу та захисту біометричних персональних даних» у законотворчу діяльність*

Положення дисертаційного дослідження Бойко Анни Миколаївни на тему: «Адміністративно-правове забезпечення обігу та захисту біометричних персональних даних» є актуальними та ефективними у разі їх імплементації у нормативно-правові акти місцевого значення.

Крім того, положення вищезазначеного дисертаційного дослідження будуть враховані під час підготовки низки проектів рішень Київської міської ради протягом декількох років поточного скликання Київської міської ради, що свідчить про практичне значення результатів даного дисертаційного дослідження.

Наукові положення дисертаційного дослідження Бойко Анни Миколаївни є такими, що будуть враховані під час розробки нормативно-правових актів місцевого значення.

**Депутат Київської міської ради** **Володимир КРАВЕЦЬ**

**Документ підписано у сервісі Вчасно (продовження)**
МАРТИНОВА_Анна_дисертація_НОВА_PDF.pdf

Документ відправлено: 13:58 08.12.2022

**Власник документу**

**Електронний підпис**
13:58 08.12.2022
Ідентифікаційний код: 3441301887
МАРТИНОВА АННА МИКОЛАЇВНА
Власник ключа: МАРТИНОВА АННА МИКОЛАЇВНА
Час перевірки КЕП/ЕЦП: 13:58 08.12.2022
Статус перевірки сертифікату: Сертифікат діє
Серійний номер: 248197DDFAB977E504000000107FDF0080A5C203
Тип підпису: удосконалений