УДК 347.1
DOI https://doi.org/10.32782/2524-0374/2024-6/47

ПРАКТИЧНЕ ЗНАЧЕННЯ РОЗМЕЖУВАННЯ ПЕРСОНАЛЬНИХ ДАНИХ ТА ІНШИХ ТИПІВ ДАНИХ У КОНТЕКСТІ ЇХ ОБРОБКИ: ЗАРУБІЖНИЙ ТА ВІТЧИЗНЯНИЙ ДОСВІД

THE PRACTICAL SIGNIFICANCE OF DISTINGUISHING BETWEEN PERSONAL DATA AND OTHER TYPES OF DATA IN THE CONTEXT OF THEIR PROCESSING: FOREIGN AND DOMESTIC EXPERIENCE

Дрогін Є.Р., магістр
Навчально-науковий інститут права Київського національного університету імені Тараса Шевченка

Статтю присвячено комплексному дослідженню проблематики розмежування персональних даних та інших типів даних через призму аналізу таких типів даних як «персональні», «неперсональні» та «чутливі», враховуючи як національне законодавство у сфері захисту даних, так і зарубіжне, зокрема Закон України «Про захист персональних даних» № 2297-VI, Закон України «Про інформацію» № 2657-XII, законопроєкт № 8153, Конвенцію №108, GDPR, PIPL, DGA. Підкреслено важливість розмежування персональних даних та інших типів даних на законодавчому рівні, враховуючи стрімкий розвиток цифрових технологій, а також встановлено законодавчі прогалини у даній сфері. Виокремлено відповідні критерії розмежування вищезгаданих типів даних.

Актуальність порушення даного питання обумовлена низкою чинників, серед яких ключову роль відіграє правова невизначеність, що може виникати при спробі розмежування персональних даних, неперсональних даних та чутливих даних на практиці через законодавчі прогалини, що набуває критичного значення, оскільки кваліфікація конкретного типу даних ініціює застосування різних правових норм та механізмів регулювання (захисту).

Важливість даної теми також підкріплюється стрімким розвитком законодавчих ініціатив у сфері захисту даних, що вимагає від правової науки глибокого та системного аналізу як існуючих проблем, так і шляхів їх розв'язання, зокрема з метою сприяння інтеграції України до Єдиного цифрового ринку Європейського Союзу та адаптації національного законодавства у відповідності до європейських стандартів у сфері захисту персональних даних, 25 жовтня 2022 року у Верховній Раді України було зареєстровано законопроєкт № 8153, який покликаний привести національне законодавство у сфері захисту персональних даних у відповідність до міжнародних норм, зокрема, GDPR та Конвенції №108, враховуючи зобов'язання України, що випливають зі ст. 15 Угоди про асоціацію між Україною та ЄС.

Ключові слова: персональні дані, неперсональні дані, захист даних, глобалізація, цифровізація, GDPR, PIPL, законодавство України, чутливі дані, ідентифікація, анонімізація, знеособлення даних.

The article is devoted to a comprehensive study of the issues of distinguishing between personal data and other types of data through the prism of analysis of such types of data as "personal", "non-personal" and "sensitive", taking into account both national and foreign data protection legislation, in particular, the Law of Ukraine "On Personal Data Protection" No. 2297-VI, the Law of Ukraine "On Information" No. 2657-XII, Draft Law No. 8153, Convention No. 108, GDPR, PIPL, DGA. The author emphasizes the importance of distinguishing between personal data and other types of data at the legislative level, given the rapid development of digital technologies, and identifies legislative gaps in this area. The relevant criteria for distinguishing between the above-mentioned types of data are highlighted.

The urgency of raising this issue is due to a number of factors, among which the key role is played by the difficulties that may arise when trying to distinguish between personal data, non-personal data and sensitive data in practice due to legislative gaps, which is of critical importance, since the qualification of a particular type of data initiates the application of different legal norms and regulatory (protection) mechanisms.

The importance of this topic is also reinforced by the rapid development of legislative initiatives in the field of data protection, which requires from legal science a deep and systematic analysis of both existing problems and ways of solving them, in particular with the aim of promoting the integration of Ukraine into the Single Digital Market of the European Union and the adaptation of the national legislation in accordance with European standards in the field of personal data protection, on October 25, 2022, draft law № 8153 was registered in the Verkhovna Rada of Ukraine, which is designed to bring national legislation in the field of personal data protection into compliance with international norms, in particular, GDPR and Convention № 108, taking into account Ukraine's obligations under Article 15 of the EU-Ukraine Association Agreement.

Key words: personal data, non-personal data, data protection, globalization, digitalization, GDPR, PIPL, Ukrainian legislation, sensitive data, identification, anonymization, depersonalization of data.

У контексті невпинної глобалізації та стрімкого розвитку цифрових технологій, поняття «персональні дані» набуває особливої актуальності. Цифровізація життя, активний розвиток електронної комерції, поширення та еволюція штучного інтелекту, соціальних мереж, Інтернет речей супроводжується збільшенням обсягів генерації, обігу та обробки даних, що стосуються фізичних осіб. Водночас, умови глобалізації зміщують акценти з локального правового регулювання правовідносин у сфері захисту персональних даних на потребу в уніфікованих міжнародних стандартах.

Значимість правильної кваліфікації даних як персональних лежить у площині захисту основоположних прав та свобод індивіда, зокрема права на приватність. В умовах, коли інформація про фізичну особу може бути зібрана без її відома, оброблена та використана у способи, які можуть мати непередбачувані наслідки, критично важливим стає ефективний захист персональних даних, тому глибоке розуміння поняття персональних даних є певним підґрунтям для формування механізмів їхнього захисту, а також є орієнтиром для визначення матеріальної сфери дії та меж застосування законодавства у сфері захисту персональних даних.

У розрізі даного питання дуже влучним є розкриття квінтесенції поняття персональних даних А. В. Пазюком, який у своїй дисертації робить висновок про те, що «персоніфікована інформація відображає індивідуальність кожної людини і, з огляду на доступність і поширеність засобів її збирання й використання, несе загрозу можливого неправомірного використання, розголошення відомостей щодо приватного життя, заподіяння шкоди репутації і добробуту людини тощо» [1, с. 7].

З огляду на дане тлумачення сутності поняття персональних даних, можна зробити висновок, що даній категорії притаманна така властивість як «індивідуалізація фізичної особи», оскільки за комбінацію певних даних ми можемо ідентифікувати (встановити, виокремити) конкретну особу з-поміж інших осіб (групи осіб), а також властиві такі ознаки як «вразливість», так як витік або неправомірний доступ до персональних даних може становити ризик порушення прав та свобод конкретної фізичної особи, так і групи осіб та «невідчужуваність»,

оскільки суб'єкт даних наділений особистими немайновими правами, такими як право на ім'я, право надавати та відкликати згоду на обробку персональних даних, право на невтручання у приватне та сімейне життя.

Одним із перших міжнародних правових актів, в якому було закладено нормативне визначення поняття персональних даних є Конвенція Ради Європи № 108 від 28 січня 1981 року «Про захист осіб у зв'язку з автоматизованою обробкою персональних даних» (надалі – Конвенція № 108).

Відповідно до п. «а» ст. 2 Конвенції № 108 «персональні дані» – це будь-яка інформація, що стосується фізичної особи, яку ідентифіковано чи можна ідентифікувати («суб'єкт даних») [2].

Дане визначення прописано доволі широко, що в результаті може породжувати значну правову невизначеність щодо того, які саме дані вважаються персональними, і це може призводити до появи різних інтерпретацій та складнощів у застосуванні законодавства на практиці, а також це потенційно може обтяжити компанії непропорційно суворими вимогами до захисту даних, що може надмірно ускладнити процеси обробки даних і стримувати інноваційний розвиток даної сфери.

Але важливо підкреслити, що це було зроблено навмисно з метою забезпечення всеохоплюючого захисту права людини на приватність у змінному цифровому світі, тобто прослідковується певна гарантія, що майже будь-який тип інформації, який може вплинути на особистісну сферу індивіда, підпадає під дію законодавства про захист даних, відіграючи ключову роль у забезпеченні недоторканності приватного життя. Однак, на нашу думку, важливо знайти баланс між захистом персональних даних та забезпеченням гнучкості для інновацій, ефективної обробки даних, а також налагодженням міжнародних відносин між різними національними юрисдикціями.

Беззаперечно можна зазначити, що Конвенція № 108 стала світовим стандартом у сфері захисту персональних даних, став фундаментом для розробки регіональних правових актів, зокрема, Директиви 95/46/ЄС Європейського Парламенту і Ради «Про захист фізичних осіб при обробці персональних даних і про вільне переміщення таких даних» від 24 жовтня 1995 року (надалі – Директива), яка втратила чинність та у 2018 році була замінена Регламентом Європейського Парламенту і Ради (ЄС) 2016/679 «Про захист фізичних осіб у зв'язку з обробкою даних і про вільний рух таких даних, та про скасування Директиви 95/46/ЄС (Загальний регламент про захист даних)» від 27 квітня 2016 року (англ. General Data Protection Regulation) (надалі – GDPR або Регламент). В Директиві було надано значно більш уточнене і деталізоване визначення поняття «персональні дані» у порівнянні з первісними положеннями, викладеними в Конвенції № 108. Це уточнене тлумачення персональних даних продовжило залишатися актуальним і не зазнало змін при переході до GDPR.

Відповідно до ст. 4(1) GDPR «персональні дані» означають будь-яку інформацію, що стосується фізичної особи, яку ідентифіковано чи можна ідентифікувати («суб'єкт даних»); фізична особа, яку можна ідентифікувати, є такою особою, яку можна ідентифікувати, прямо чи опосередковано, зокрема, за такими ідентифікаторами як ім'я, ідентифікаційний номер, дані про місце проживання, онлайн-ідентифікатор або за одним чи декількома факторами, що є визначальними для фізичної, фізіологічної, генетичної, розумової, економічної, культурної чи соціальної сутності такої фізичної особи [3].

Визначення поняття персональних даних, яке закріплене у Конвенції №108, а згодом розширене у Директиві та GDPR стало певним орієнтиром для інших країн, які на основі нього сформували власні дефініції поняття «персональні дані» у національних нормативно-правових актах.

Законодавство України у сфері захисту персональних даних не стало виключенням. Визначення поняття «персональні дані» знайшло своє відображення у Законі України «Про захист персональних даних» (надалі – Закон України № 2297-VI) та Законі України «Про інформацію» (надалі – Закон України № 2657-XII), в яких зазначено, що до персональних даних відносяться відомості чи сукупність відомостей про фізичну особу, яка ідентифікована або може бути конкретно ідентифікована (ст. 2, ст. 11) [4; 5].

З метою сприяння інтеграції України до Єдиного цифрового ринку Європейського Союзу (надалі – ЄС або Союз) та адаптації національного законодавства у відповідності до європейських стандартів у сфері захисту персональних даних, 25 жовтня 2022 року у Верховній Раді України було зареєстровано законопроєкт «Про захист персональних даних» № 8153 (надалі – законопроєкт № 8153) в якому поняття «персональні дані» визначено як будь-яка інформація, що стосується фізичної особи, яку ідентифіковано, або може бути ідентифіковано (ст. 2) [6].

Дана дефініція узгоджується із положеннями Конвенції №108 та частково з положеннями GDPR, оскільки останній містить більш деталізовану дефініцію, що глибше розкриває сутність категорії «персональні дані» у розрізі сучасних тенденцій. У контексті євроінтеграційних процесів доречно було б у повній мірі узгодити національне законодавство у сфері захисту персональних даних, зокрема, адаптувавши визначення поняття персональних даних до європейських стандартів, шляхом його коригування у відповідності до GDPR.

На думку М. В. Різаки, визначення поняття «персональні дані», яке наведене у національному законодавстві є за своїм змістом доволі широким, що підтверджується відкритістю переліку відомостей, віднесених до числа персональних даних. Проте важливо розуміти, що враховуючи природу персональних даних, повністю їх перерахувати досить складно, відповідно це спричинило формування зі сторони законодавця підходу, згідно з яким суб'єкт має право частково самостійно формувати свій «інформаційний портрет», вирішуючи, які з характеристик, що його ідентифікують, слід віднести до числа персональних даних, а які – ні [7, с. 25].

З іншої сторони, занадто широке тлумачення поняття персональних даних може спричинити певні негативні наслідки, такі як поява різних інтерпретацій даного поняття, які за своїм змістом не будуть відповідати ознакам та властивостям, які притаманні персональним даним, внаслідок чого дані інтерпретації не будуть підпадати під дію спеціального правового режиму персональних даних, тобто це призводить до ускладнення процесу ідентифікації (кваліфікації), яка саме інформація про індивіда вважається персональними даними, доступ до яких можливий за згодою суб'єкта персональних даних тощо, а які дані можна використовувати і без такої згоди.

Водночас, ми не можемо заперечувати той факт, що під впливом динамічного розвитку цифрових технологій, прогресом в аналітиці даних зміст поняття персональних даних буде надалі розширюватися та еволюціонувати, і це буде вимагати періодичного оновлення законодавства та механізмів захисту персональних даних з метою відповідності новітнім реаліям і гарантування ефективного захисту даних в усе більш цифровізованому світі.

У Китайській Народній Республіці (надалі – КНР) у 2021 році був прийнятий Закон КНР «Про захист персональних даних» (кит. 中华人民共和国个人信息保护法) (англ. The China Personal Information Protection Law) (надалі – PIPL), який є своєрідними аналогом GDPR у контексті правового регулювання питань пов'язаних із захистом персональних даних у КНР.

Відповідно до ст. 4 PIPL «персональні дані» – це будь-яка інформація, зафіксована в електронному або

іншому вигляді, що стосується фізичної особи, яку ідентифіковано чи можна ідентифікувати, за винятком анонімної інформації (інформації, яка є результатом процесу анонімізації) [8].

Аналізуючи дане положення, можна висунути гіпотезу, що дане визначення персональних даних було частково запозичене з GDPR, хоч і було стилістично видозмінене, в результаті чого персональні дані за GDPR є більш деталізованою категорією.

Окремо варто відмітити, що у визначенні поняття персональних даних, яке викладене у PIPL законодавець додатково робить акцент на тому, що анонімна інформація не відноситься до категорії персональних даних, і відповідно не охоплюється сферою застосування PIPL. Однак GDPR містить подібне застереження у п. 26 Преамбули «...цей Регламент не стосується обробки такої анонімної інформації, у тому числі для статистичних чи дослідницьких цілей» [3]. Передусім це пояснюється тим, що анонімна інформація, яка не дає можливості ідентифікувати фізичну особу (відсутній розумний ризик ідентифікації) не підпадає під сферу дії відповідних правових документів щодо захисту персональних даних.

В рамках даного дискурсу важливо розрізняти поняття «персональні дані» та «неперсональні (неособисті) дані» (англ. non-personal data), оскільки до кожного з цих типів даних застосовується спеціальний («унікальний» саме для цього типу даних) правовий режим захисту та обробки.

В ЄС питання пов'язані з неперсональними даними регулюються Регламентом про вільний потік неперсональних даних (англ. Regulation (EU) 2018/1807 of the European Parliament and of the Council of 14 November 2018 on a framework for the free flow of non-personal data in the European Union), який має на меті забезпечити вільний потік даних, відмінних від персональних. У тексті даного Регламенту використовується термін «дані», який слід розуміти як «дані, відмінні від персональних даних, визначених у пункті 1 статті 4 GDPR. Також цей тип даних іменується в Регламенті як «неперсональні дані», кваліфікація яких здійснюється шляхом протиставлення (a contrario) персональним даним, які визначені GDPR [9].

Відповідно до п. 26 Преамбули GDPR, дані є персональними, якщо контролер або інша особа може прямо чи опосередковано ідентифікувати суб'єкта даних (фізичну особу) за допомогою «засобів, які можуть бути використані з розумною ймовірністю». Якщо персональні дані ніколи не були пов'язані з фізичною особою, яку ідентифіковано чи можна ідентифікувати або більше не можуть бути з розумною ймовірністю пов'язані з такою фізичною особою, вони кваліфікуються як «анонімна інформація» (неперсональні дані) і не підпадають під сферу застосування Регламенту [3].

Аналізуючи вищезазначене положення, можна виокремити своєрідний «юридичний тест», що охоплює підхід, який ґрунтується на оцінці ризиків з метою кваліфікації інформації (віднесення інформації до певного типу даних), тобто, якщо існує «розумний ризик ідентифікації» – дані повинні розглядатися як персональні, а якщо такий ризик є незначним – дані можуть розглядатися як неперсональні.

При цьому для того, щоб визначити, чи існує «розумний ризик ідентифікації» (розумна ймовірність використання засобів для ідентифікації фізичної особи), слід враховувати всі об'єктивні фактори, такі як витрати та кількість часу, необхідні для ідентифікації, а також брати до уваги технології, доступні на момент обробки персональних даних, та технологічні досягнення (технологічний прогрес), які можна очікувати у майбутньому тощо [3].

Слід зауважити, що вищезгаданий перелік факторів не є вичерпним, тому також необхідно звернути увагу на такі фактори, як мета обробки, яку переслідує контролер, тобто, якщо мета обробки передбачає ідентифікацію фізичних осіб, можна припустити, що контролер або будь-яка інша залучена особа має або матиме засоби, які «з високою ймовірністю можуть бути використані» для ідентифікації суб'єкта даних та ризик організаційних дисфункцій (відхилень) (наприклад, порушення обов'язків щодо конфіденційності) і технічних збоїв тощо [10, с. 16].

При аналізі положень національного законодавства в контексті захисту персональних даних, стає можливим виділити поняття «знеособлені дані», що являють собою дані за допомогою яких неможливо прямо чи опосередковано ідентифікувати особу. Ці дані є результатом процесу «знеособлення», що має на меті вилучення відомостей, які дають змогу прямо чи опосередковано ідентифікувати особу. Варто відмітити, що термінологічно дане положення не узгоджується з положеннями європейських правових актів у сфері захисту персональних даних (ст. 2) [4].

У законопроєкті № 8153 також можна виділити поняття «знеособлені дані», яке змістовно було розширене та деталізоване, оскільки, крім інформації, яка не дозволяє ідентифікувати фізичну особу, воно також включає в себе інформацію, яка стосувалася фізичної особи, але в результаті процесу «знеособлення» більше не дозволяє встановити будь-який зв'язок з даною фізичною особою, тобто даний процес позиціонується як незворотній (ст. 2) [6].

На рівні національного законодавства також варто виділити Закон України № 2657-XII, який встановлює правові рамки для регулювання відносин, пов'язаних із створенням, збором, отриманням, зберіганням, використанням, поширенням, захистом та охороною інформації. У контексті даного Закону «інформація» визначається як будь-які відомості та/або дані, які можуть бути збережені на матеріальних носіях або відображені в електронному вигляді (ст. 1) [5]. На нашу думку, дане визначення дозволяє констатувати, що сфера дії даного правового акта може охоплювати відносини, які пов'язані з обробкою неперсональних даних, оскільки даний Закон охоплює широке коло інформаційних відносин, не встановлюючи при цьому прямих обмежень щодо характеру, змісту та типу інформації.

Враховуючи сучасну міжнародну практику, де розмежування персональних та неперсональних даних має важливе значення для визначення сфери застосування регуляторних вимог, таке широке тлумачення понять «персональні дані» та «неперсональні дані» в законодавстві потребує додаткової уваги. Оскільки на сьогодні національне законодавство не робить явного розмежування між цими категоріями (типами) даних, існує простір для аналізу та інтерпретації щодо того, яким чином неперсональні дані підпадають під дію вищезгаданого нормативно-правового акта, тому доцільно було б надати більш деталізоване тлумачення даних категорій у законодавчих актах у сфері захисту як персональних, так і неперсональних даних.

Виходячи із змісту статті 73 PIPL поняття «неперсональні дані» («анонімна інформація») охоплює собою персональну інформацію, яка внаслідок «анонімізації» не дає можливості ідентифікувати конкретну фізичну особу та не може бути відновлена [8].

Отже, у положеннях Закону України № 2297-VI, законопроєкті № 8153 та PIPL прослідковується більш категоричний підхід, який ґрунтується на тому, що наявність ризику є недопустимою, оскільки поточне тлумачення процесу «знеособлення» та «анонімізації», яке закладено у вищезгаданих законодавствах відображає концепцію «незворотності», повністю виключаючи наявність ризику ідентифікації фізичної особи або відновлення первісних персональних даних у майбутньому.

Важливо пам'ятати, що абсолютно виключити ризик ідентифікації наразі неможливо, оскільки, по-перше, «дані» є динамічною категорією, вони постійно цирку-

люють, формуючи «екосистему даних», генеруються нові дані, здійснюється транскордонна передача (обмін) даними, і треті особи можуть володіти певними даними, що дозволяють встановити зв'язок з відповідною особою, і в результаті ідентифікувати конкретну фізичну особу, водночас контролер первісних даних може про це навіть не здогадуватися. Наприклад, лікар, який володіє інформацією, що результати анонімного дослідження певного випадку, які викладені у науковій статті стосуються одного з його пацієнтів (контролером в даному випадку є лікарня), тому, у випадку публічного оприлюднення анонімної інформації, важливо не лише визначити, чи дійсно це анонімна інформація з точки зору контролера, який їх оприлюднює, а й те, чи є треті особи, які з високою ймовірністю можуть використати попередні знання для полегшення повторної ідентифікації (суб'єктний підхід) [11, с. 19], по-друге, спрогнозувати, які технологічні зміни відбудуться у майбутньому дуже складно, тому залишається потенційний ризик, що за допомогою певних технологій можна буде провести повторну ідентифікацію (деанонімізацію), і в результаті анонімна інформація (неперсональні дані) може знову набути статусу персональних даних (фактично процес анонімізації не є абсолютним), що є наслідком застосування спеціального правового режиму.

Крім кваліфікації та розмежування таких категорій як «персональні дані» та «неперсональні дані», важливим аспектом у контексті обробки даних є визначення, чи відносяться відповідні дані до «особливої категорії даних» («чутливих даних»), оскільки це має наслідком застосування більш суворих правових рамок.

На нашу думку, це дві фундаментально важливі, але концептуальні різні категорії даних. З одного боку, «особлива категорія персональних даних» («чутливих даних») включає інформацію, обробка якої вимагає підвищеної уваги та захисту через потенційний ризик для основоположних прав та свобод індивіда. З іншого боку, поняття «неперсональних чутливих даних» вимагає уточнення та деталізації, оскільки традиційно законодавство зосереджене на захисті персональних даних, в той час як обробка неперсональних чутливих даних може також нести в собі певні ризики та виклики.

GDPR виокремлює у своїх положеннях «особливу категорію персональних даних» («чутливі дані») до якої відносяться персональні дані, що стосуються расового та етнічного походження, політичних поглядів, релігійних або світоглядних переконань, членства у професійних спілках, а також генетичні дані, біометричні дані (які обробляються з метою однозначної ідентифікації фізичної особи), дані про стан здоров'я, статеве життя чи сексуальну орієнтацію фізичної особи (стаття 9(1)) [3].

У Законі України № 2297-VI не фігурують поняття «особлива категорія персональних даних» або «чутливі персональні дані», однак ч. 1 ст. 7 даного Закону містить вичерпний перелік даних, обробка яких здійснюється у відповідності до особливих вимог, а саме персональні дані про расове або етнічне походження, політичні, релігійні або світоглядні переконання, членство в політичних партіях та професійних спілках, засудження до кримінального покарання, а також дані, що стосуються здоров'я, статевого життя, біометричних або генетичних даних [4]. На нашу думку, це є достатньою підставою вважати, що ці дані мають «особливий правовий статус», а тому за своїм змістом цілком відповідають вищезгаданим поняттям.

Натомість законопроєкт № 8153 оперує поняттям «чутливі персональні дані», а його норми щодо встановлення переліку даних, які можна кваліфікувати як «чутливі» у повній мірі узгоджуються з положеннями GDPR, на відміну від положень Закону України № 2297-VI, які не відносять дані щодо сексуальної орієнтації до «чутливих», а також навпаки кваліфікують як «чутливі» дані про членство в політичних партіях та засудження до кримінального покарання, що наразі не відповідає тлумаченню «особливої категорії персональних даних» («чутливих даних») GDPR.

Згідно із статтею 28 PIPL «чутливі персональні дані» – це персональні дані, витік або незаконне використання яких може призвести до приниження людської гідності фізичної особи або заподіяння шкоди її особистій чи майновій безпеці, зокрема біометричні дані, релігійні переконання, конкретні ідентифікаційні дані, дані про стан здоров'я, фінансові рахунки та місцезнаходження і траєкторію пересування, а також персональні дані про неповнолітніх віком до 14 років [8].

На початку даної дефініції спостерігається, що законодавець приділяє значну увагу наданню широкого інтерпретаційного поля категорії «чутливі дані», прагнучи охопити відповідно більш розширений діапазон даних. Однак, паралельно наводиться й конкретизується перелік даних, які можуть бути кваліфіковані як чутливі, тим самим намагаючись балансувати між широким та вузьким тлумаченням даної категорії, і це демонструє, що законодавець визнає різноманіття сценаріїв, у яких можуть бути використані чутливі дані.

На нашу думку, це відображає глибоке розуміння потенційної шкоди, що може бути завдана фізичній особі внаслідок неправомірного обігу, обробки або використання її особистої інформації, але в той же час важливо дотримуватися балансу між тлумаченням даної категорії і практичною необхідністю захисту чутливих персональних даних без створення перешкод для обробки даних, яка відбувається в законних цілях.

Додатково варто звернути увагу на те, що на відміну від GDPR, PIPL визнає персональні дані неповнолітніх віком до 14 років чутливими даними, але важливо підкреслити, що GDPR зі свого боку відносить дітей (фізичні особи до 16 років) до такої категорії як «вразливі фізичні особи» (п. 75 Преамбули GDPR) та акцентує увагу на необхідності застосування особливого захист персональних даних дітей (п. 38 Преамбули GDPR).

У контексті Європейської стратегії даних в ЄС були прийняті Закон про управління даними (англ. Data Governance Act) (надалі – DGA) (який набув чинності 23 червня 2022 року та почав діяти з 24 вересня 2023 року) та Закон про дані (англ. Data Act) (який набув чинності 11 січня 2024 року та почне діяти з 12 вересня 2025 року), які у своїх положеннях виділяють такі категорії як «комерційно чутливі неперсональні дані» (англ. commercially sensitive non-personal data) – неперсональні дані, що становлять комерційну таємницю та/або представляють зміст, захищений правами інтелектуальної власності, а також «високочутливі неперсональні публічні дані» (англ. highly sensitive non-personal public data), які визначаються законодавством ЄС, наприклад в контексті Європейського простору даних про охорону здоров'я або іншого галузевого законодавства [12; 13].

Отже, важливість врахування вищезгаданих норм та розмежування персональних даних та інших типів даних полягає в тому, що персональні, неперсональні та чутливі дані можуть бути змішані в наборах даних, як приклад можна навести дані, де захист прав інтелектуальної власності/комерційної таємниці та захист даних можуть перетинатися, оскільки захист прав інтелектуальної власності та комерційної таємниці діє незалежно від типу (характеру) даних, в результаті буде виникати така категорія як «змішані набори даних» (англ. mixed datasets), що буде ускладнювати процес визначення, які правові приписи слід використовувати при обробці вищезгаданих даних. На сьогодні ЄС підкреслив значення цієї проблематики, ухваливши DGA та Data Act, які детально визначають

концепцію «чутливих неперсональних даних», а також, заклавши в GDPR ризик-орієнтований підхід до розмежування «персональних» та «неперсональних (анонімних)» даних, який, на нашу думку, відповідає сучасним викликам. Ми вважаємо, такий підхід має слугувати зразком для інших країн, включаючи наше національне законодавство. У цьому контексті пропонуємо доповнити законопроєкт № 8153 наступним положенням: «Для визначення того, чи наявна можливість прямо чи опосередковано ідентифікувати фізичну особу, слід враховувати всі засоби, які можуть бути використані контролером або іншою особою з розумною ймовірністю, наприклад, виокремлення. Для того, щоб визначити, чи існує розумна ймовірність використання засобів для ідентифікації фізичної особи, слід враховувати всі об'єктивні фактори, такі як витрати та кількість часу, необхідні для ідентифікації, технології, доступні на момент обробки персональних даних, та технологічні досягнення, які можна очікувати у майбутньому, мета обробки, яку переслідує контролер та ризик організаційних відхилень і технічних збоїв тощо».

ЛІТЕРАТУРА

1. Пазюк А. В. Міжнародно-правовий захист права людини на приватність персоніфікованої інформації: автореф. дис. канд. юрид. наук. Київ, 2004. 20 с. URL: http://cyberpeace.org.ua/files/aref-1.pdf (дата звернення: 01.06.2024).
2. Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data. opened for signature 28 January 1981. in force 1 October 1985. European Treaty Series. № 108. URL: https://eur-lex.europa.eu/eli/reg/2016/679/oj (date of access: 01.06.2024).
3. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). URL: https://eur-lex.europa.eu/eli/reg/2016/679/oj (date of access: 01.06.2024).
4. Про захист персональних даних: Закон України від 01.06.2010 № 2297-VI. URL: https://zakon.rada.gov.ua/laws/show/2297-17#Text (дата звернення: 01.06.2024).
5. Про інформацію: Закон України від 2 жовтня 1992 року № 2657-XII. URL: https://zakon.rada.gov.ua/laws/show/2657-12#Text (дата звернення: 01.06.2024).
6. Про захист персональних даних: проєкт Закону України від 25 жовтня 2022 р. № 8153. URL: https://itd.rada.gov.ua/billInfo/Bills/Card/40707 (дата звернення: 01.06.2024).
7. Різак М. В. Адміністративно-правове забезпечення відносин обігу та обробки персональних даних в Україні: автореф. дис. ... докт. юрид. наук. Харків, 2018. 39 с.
8. 中华人民共和国个人信息保护法. 2021年8月20日第十三届全国人民代表大会常务委员会第三十次会议通过. URL: https://www.gov.cn/xinwen/2021-08/20/content_5632486.htm (申请日期: 01.06.2024).
9. Regulation (EU) 2018/1807 of the European Parliament and of the Council of 14 November 2018 on a framework for the free flow of non-personal data in the European Union. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32018R1807 (date of access: 01.06.2024).
10. Opinion 4/2007 on the concept of personal data. Article 29 Data Protection Working Party. Adopted June 20, 2007. URL: https://www.clinicalstudydatarequest.com/Documents/Privacy-European-guidance.pdf (date of access: 01.06.2024).
11. Finck M., Pallas F. They who must not be identified—distinguishing personal from non-personal data under the GDPR. International Data Privacy Law. Volume 10. Issue 1. February 2020. Pages 11–36. URL: https://doi.org/10.1093/idpl/ipz026 (date of access: 01.06.2024).
12. Regulation (EU) 2022/868 of the European Parliament and of the Council of 30 May 2022 on European data governance and amending Regulation (EU) 2018/1724 (Data Governance Act). URL: https://eur-lex.europa.eu/eli/reg/2022/868/oj (date of access: 01.06.2024).
13. Regulation (EU) 2023/2854 of the European Parliament and of the Council of 13 December 2023 on harmonised rules on fair access to and use of data and amending Regulation (EU) 2017/2394 and Directive (EU) 2020/1828 (Data Act). URL: https://eur-lex.europa.eu/eli/reg/2023/2854 (date of access: 01.06.2024).