

ЩОДО ВИЗНАЧЕННЯ ПЕРСОНАЛЬНИХ ДАНИХ В УМОВАХ ЄВРОІНТЕГРАЦІЙНИХ ПРОЦЕСІВ

Токарева В. О.

Стаття присвячена питанню тлумачення персональних даних за законодавством ЄС в умовах потужного розвитку інформаційно комунікаційних технологій, посилення євроінтеграційних процесів та потреби адаптації українського законодавства до законодавства ЄС в умовах війни. В означених умовах питання адаптації вітчизняного законодавства до підходів, вироблених в ЄС, стає вельми актуальним. Підходи для встановлення персональних даних та їх відмежування від інформації про особу, яка не є персональними даними, розроблені у законодавстві ЄС, мають бути використані та імплементовані в українське законодавство.

Встановлено, що Регламент ЄС 2016/679 навмисно передбачає досить широке визначення персональних даних, яке не має чітко встановлених меж та єдиних критеріїв, щоб охопити максимальну значну кількість даних в умовах потужної цифровізації. З'ясовано, що у сучасних реаліях обробка даних з одноразової дії перетворилася у досить незначний та майже безперервний процес, коли суб'єкти даних не усвідомлюють обсяги даних, які збираються та обробляються щодо них, та факту такої обробки. Означена ситуація призводить до певного стирання різниці між персональними та неперсональними даними. Встановлено, що в ЄС застосовується підхід до правового регулювання обробки персональних даних, заснований на дихотомічній концепції розділення інформації та правових режимів обробки персональних та неперсональних даних. З'ясовано, що ЄСПЛ визначає збір та обробку даних, що дозволяє ідентифікувати фізичних осіб як втручання у приватне життя. Проаналізований алгоритм виявлення та віднесення даних до персональних даних та відмежування їх від інших іншої інформації, яка не є персональними даними, розроблений в законодавстві ЄС. В окремих випадках встановлені критерії розмежування персональних даних від неперсональних є досить розпливчастим, ускладнюючи відмежування означених категорій на практиці.

Дослідженні критерії розмежування персональних та неперсональних даних, засновані на властивостях оброблюваної інформації, особливостях суб'єктів даних та можливості їх ідентифікації. Проаналізовано місце псевдоанімізованих та анонімізованих даних.

Ключові слова: фізична особа, цифрові прав людини, захист персональних даних, персональні данні, анонімізовані данні, інформація, ЄСПЛ, демократичне суспільство, євроінтеграція, засоби індивідуалізації.

Tokareva V. O. Concerning the definition of personal data in the terms of European integration processes

The article is devoted to the issue of determining personal data in terms of massive development of information and communication technologies. The European integration processes and the need to adapt the legislation of Ukraine to the EU standart are strengthening in terms of war.

Development of a digital economy based on information communication and digital technologies, e-governance, ensuring access to information of data subjects, state and local authorities raise the issue of differentiation personal data from non-personal data and other related categories, and the protection of personal data. Approaches and criteria of determining personal data and distinguishing them from other information in the EU should be used and implemented in the Ukrainian legislation and doctrine.

The General Data Protection Regulation (EU GDPR) 2016/679 intentionally provides quiet broad definition of personal data, which does not contain limits and unified criteria, in order to cover the broad set of data from the prospect of developing of the digital society. It was found that nowadays data processing has turned from a one-time operation into quiet insignificant and almost continuous process. That data subjects are not even aware of the scale of data that is collected and processed related to them and the fact of such processing. This lead for disseminating mergers between personal and non-personal. The algorithm for identifying personal data and nonpersonal data are analyzed. In some cases, establishing criteria for distinguishing personal data from non-personal data is quite vague, making it difficult to delimit the specified categories in practice.

The application of the approach to legal regulation of personal data processing based on the dichotomous concept of separation of information and legal regimes

of personal and non-personal data processing in the EU is analyzed. It was found that the ECHR defines the collection and processing of data, which allows the identification of individuals, as interference in private life. The criteria for distinguishing personal and non-personal data based on processed information, features of data subjects have been investigated. Determination of pseudonymized and anonymized data were analyzed.

Key words: *natural person; digital human rights; protection of personal data; personal data; anonymized data; information; ECtHR; democratic society; European integration; means of individualization.*

Актуальність.

Розвиток цифрового суспільства цифрової економіки, е-держави [1] та євроінтеграційних процесів вносять свої неминучі трансформації, де обробка даних з одноразової дії перетворюється у майже безперервний процес. Суб'єкти даних не усвідомлюють масштаби даних, які збираються та обробляються, та факт такої обробки, коли втрачається межа між персональними та неперсональними даними [2]. Розбудова цифрової економіки, заснованої на інформаційно-комунікаційних та цифрових технологіях, електронної держави та забезпечення доступу до інформації громадян, органів державної влади та місцевого самоврядування ставить нагальним питання забезпечення належного захисту персональних даних, а з тим і питання їх визначення та відмежування від неперсональних даних та інших суміжних категорій.

З урахуванням зазначеного та прийняттям Регламенту ЄС 2016/679, який замінює Директиву про захист персональних даних ЄС 95/46, який є документом прямої дії в усіх державах ЄС та поширюється на організації та компанії, які збирають та обробляють персональні дані резидентів та громадян ЄС, в умовах стрімкої інтеграції в європейське співтовариство актуальною стає потреба відповідності українських компаній стандартам ЄС у галузі захисту персональних даних.

Аналіз стану дослідження. У різні часи дослідження проблематики визначення персональних даних та їх співвідношення із суміжними категоріями займалися: А.В. Кардаш, О.О. Серебрянник, Т.І. Обуховська, Р.С. Концевой, О.А. Дмитренко та інші.

Метою статті є аналіз законодавства Європейського Союзу стосовно визначення та тлумачення таких категорій, як персональні дані та неперсональні дані для розробки шляхів імплементації та застосування в українській практиці.

Виклад матеріалу. З огляду на стрімкий розвиток інформаційно-комунікаційних технологій, сучасного стану розвитку законодавства ЄС, збіль-

шення масштабів збору та обробки персональних даних актуальним постає відмежування персональних даних та іншої інформації про особу та неперсональних даних [3]. Закон України «Про захист персональних даних» у ст. 2 розуміє під персональними даними відомості чи сукупність відомостей про фізичну особу, яка ідентифікована або може бути конкретно ідентифікована. Частина 1 статті Регламенту ЄС 2016/679 передбачає визначення персональних даних як будь-якої інформації, яка відноситься до «суб'єкта даних», тобто ідентифікованої та підлягаючої ідентифікації фізичної особи; фізична особа, яка піддається ідентифікації, – це особа, яку можна прямо або опосередковано ідентифікувати, зокрема за допомогою посилання на ідентифікатор, такий як ім'я, ідентифікаційний номер, дані про місцезнаходження, онлайн-ідентифікатор, або на один або кілька факторів, специфічних для фізичної, фізіологічної, генетичної, розумової, економічної, культурної чи соціальної ідентичності цієї фізичної особи.

Для з'ясування питання співвідношення «персональних даних» та «засобів ідентифікації» поряд із Регламентом ЄС 2016/679 необхідно звернутися до Позиції WP29 4/2007 Про концепцію персональних даних від 20.06.2007 (надалі Позиції WP29 4/2007) [4]. Відповідно до статті 4 Регламенту ЄС 2016/679 під персональними даними розуміється будь-яка інформація, яка відноситься до ідентифікованої або фізичної особи, яка підлягає ідентифікації («суб'єкт даних»); під ідентифікованою фізичною особою розуміється особа, яка може бути ідентифікована прямо або опосередковано, зокрема за допомогою посилання на ідентифікатор, такий як ім'я, прізвище, ідентифікаційний номер, дані про місцезнаходження, онлайн-ідентифікатор або один або декілька характерних для зазначеної особи фізичних, фізіологічних, генетичних, духовних, економічних, культурних факторів або посилаючись на фактори соціальної ідентичності.

Відтак Регламент ЄС 2016/679 навмисно передбачає досить широке визначення персональних даних, яке не має чітко встановлених меж та єдиних критеріїв для того, щоб охопити максимальну велику кількість даних. Попередня діюча Директива 95/46/ЄС про захист фізичних осіб при обробці персональних даних та про обіг таких даних [5] передбачала застереження щодо: визначення поняття персональних даних навмисно дається досить широким, аналогічно визначенню, передбаченому Конвенцією Ради Європи про захист фізичних осіб під час автома-

тизованої обробки персональних даних, щоб охопити всю інформацію, пов'язану із особою. Із цією позицією надалі погодився парламент ЄС, зазначивши, що визначення поняття «персональних даних» має бути досить загальним, щоб охопити досить широке коло даних, пов'язаних із особою, яка ідентифікується. Надалі ця думка була підтримана Радою ЄС та знайшла подальше відображення у судовій практиці ЄСПЛ.

ЄСПЛ виходить із того, що захист персональних даних охоплюється правом на повагу до приватного життя та гарантується ст. 8 Конвенції про захист прав людини і основних свобод. Адже ЄСПЛ визначає збір та обробку даних, що дозволяють ідентифікувати фізичну особу як втручання у приватне життя [6]. ЄСПЛ відносить до персональних даних досить широке коло даних, що пов'язані з різними аспектами фізичної та соціальної ідентичності людини [7], зокрема, ім'я, відомості про гендерну та етнічну приналежність, сексуальну орієнтацію та сексуальне життя [8], здоров'я [9], зображення (фотографії) [10], зразки голосу [11], відбитки пальців, ДНК-профілі та клітинні зразки [12]. За таких умов до категорії персональних даних відноситься досить широке коло даних [13].

За визначенням М.С. Крилової, в ЄС використовується підхід до правового регулювання обробки персональних даних, заснований на дихотомічній концепції розділення інформації та правових режимів обробки персональних та неперсональних даних. В межах даного підходу відповідні категорії виступають як додаткові категорії одна до одної та як взаємовиключні. Проявом взаємовиключності означених категорій є те, що ці категорії формульовані в законодавстві від зворотного, де персональні дані розуміються як будь-яка інформація, яка відноситься до ідентифікованої або фізичної особи, яка підлягає ідентифікації, в свою чергу, до неперсональних даних відносяться дані за виключенням персональних [14]. Подібне формулювання визначення неперсональних даних свідчить про їхній похідний характер та безпосередній зв'язок із персональними даними. Означене позиція також відображається у науці, де дається визначення неперсональних даних, засноване на розумінні персональних даних як будь-якої інформації, яка не відноситься до фізичної особи, коли така інформація не приводить прямо або опосередковано до ідентифікації.

Фахівець у галузі приватності С. Воронкевич на підставі аналізу Позиції WP29 4/2007 звертає увагу на такі складові елементи у конструкції визначення персональних даних передбачених Регла-

ментом ЄС 2016/679: «Будь-яка інформація», «що стосується», «ідентифікованої особи або фізичної особи яка підлягає ідентифікації» [15]. За допомогою цих елементів законодавець запровадив алгоритм виявлення та віднесення даних до персональних даних з-поміж решти оброблюваних даних. Необхідно брати до уваги, що в окремих випадках встановлення критеріїв розмежування персональних даних від неперсональних є досить неоднозначними, що може ускладнювати відмежування означених категорій на практиці [14].

Регламент ЄС 2016/679 передбачає під суб'єктами даних виключно фізичних осіб, що автоматично призводить до того, що дані, які стосуються юридичних осіб, не визнаються персональними даними. Проте ЄСПЛ у рішенні по справі *Volker und Markus Schecke GbR* [16] зазначив, що у разі якщо офіційне найменування юридичної особи дозволяє ідентифікувати одну або декількох фізичних осіб (коли назва компанії є ім'ям суб'єкта даних або декількох суб'єктів даних), у такому разі юридична особа може вимагати захисту права на недоторканність приватного життя та права на охорону персональних даних, закріплених у Хартії ЄС про основні права.

Не визнається персональними даними інформація стосовно померлих осіб, оскільки померлі не виступають суб'єктами цивільного права. Однак у певних випадках дані померлої можуть отримати певний захист, якщо стосуються живих осіб, та у такому разі дані померлого охоплюються Директивою, опосередковано підлягають захисту. Наприклад, інформація про те, що особа страждала на гемофілію, вказує на те, що нащадки також страждають на цю ж хворобу, оскільки хвороба є генетичною.

При визначенні того, як відносяться дані до конкретної особи, необхідно брати до уваги кількісні характеристики отримуваних даних та якісні характеристики, такі як зміст, мета, для якої провадиться збір [17]. Аналогічно зміст, мету та результат в якості елементів, кожний з яких незалежно від наявності інших може зробити будь-яку інформацію такою, що «стосується» суб'єкта, називає Позиція WP29. Інформація може стосуватися суб'єкта за змістом, якщо вона про конкретну фізичну особу, наприклад, результати здачі іспиту, номер телефону конкретної особи, профіль певного користувача в соціальній мережі. Інформація може стосуватися суб'єкта за метою, якщо вона використовується або, найімовірніше, може бути використана з метою оцінки, впливу на статус або поведінку суб'єкта, прояву певного

відношення до суб'єкта. Наприклад, список відвідувань сторінок в Інтернеті співробітниками компанії може бути використаний для моніторингу ефективності впродовж робочого часу кожним співробітником або з метою блокування певних сайтів певним співробітником. Інформація може стосуватися суб'єкта персональних даних, навіть за відсутності ознак «змісту» та «мети», якщо є ознака результату: якщо обробка даних, найімовірніше, вплине на права та інтереси суб'єкта, наприклад, у разі навіть неістотної зміни відношення оточуючих до особи вплине на виокремлення особи серед його кола оточуючих. Наприклад, інформація про школяра, що його родичі отримали премію Астрід Ліндгрєн або нагороду Праведник народів світу, може призвести до глузування та знущання з боку однолітків. Ці три елементи відношення даних до суб'єкта застосовуються кожен окремо, але якщо є хоча б один елемент, немає потреби виявляти інші два – дані визнаються такими, що відносяться до суб'єкта. Тож при встановленні, чи відносяться дані до неперсональних, необхідно брати до уваги, чи можна визнати за правом ЄС дані про об'єкт до персональних даних за умови, якщо такі дані дозволяють ідентифікувати суб'єкта даних [14].

Третім елементом, який покликаний встановити, чи відносяться дані до персональних даних, є стосуються «ідентифікованої або фізичної особи, яка підлягає ідентифікації». Означене має кваліфікуюче значення для номерів телефонів та інших номерів, характеристик об'єктів, живих істот, які стосуються суб'єкта даних.

Позиція WP29 визначає особу як таку, що підлягає ідентифікації, якщо вона ще не ідентифікована але її можна ідентифікувати безпосередньо, наприклад, за ім'ям (якщо воно дозволяє виокремити суб'єкта з-поміж інших), або опосередковано – за номером паспорта, автотранспортного засобу, телефону або комбінації істотних ознак, що дозволяють виокремити суб'єкта (за віком, місцем проживання, зовнішнім виглядом тощо).

Дані, «які відносяться до», включають не лише інформацію про самого суб'єкта даних, але й про належні йому або пов'язані з ним об'єкти. Наприклад, домашніх тварин та характеристики цих об'єктів, такі як вартість, стан зношення, серійний номер, діагноз, результати аналізів та обстежень тощо. Так, в окремих випадках інформація, що стосується об'єкта, може опосередковано бути джерелом інформації про особу. Вартість транспортного засобу є даними про об'єкт, а інформація про сплату транспортного податку власником

зазначеного транспорту може визнаватися в якості персональних даних [14]. Дані можуть як безпосередньо стосуватися фізичної особи (як ім'я, ДНК, чіп біометричного паспорта, RFID-мітка), так і опосередковано (наприклад, логи телефонних дзвінків на роботі), або можуть залежно від їх використання породжувати наслідки для фізичної особи (наприклад, GPS-дані у службових автомобілях).

Водночас вірогідна або гіпотетична ймовірність ідентифікації суб'єкта не робить автоматично інформацію персональними даними. Якщо можливість ідентифікувати суб'єкта відсутня або досить низька, такі дані не будуть визнаватися персональними даними. Означена теза може бути використана контролером в якості маніпуляції та виправдання збору персональних даних, яке не мало наміру ідентифікувати особу, персональні дані якої збираються. Проте за номерами телефонів, автотранспортних засобів, карток особу можна ідентифікувати у разі співставлення цих даних із даними з інших баз, наприклад, в випадку міжвідомчого обміну даними, отримання даних від операторів мобільного зв'язку, камер відеоспостереження на вулиці.

Щодо кваліфікації номеру телефону в якості ідентифікатора та визнання його персональними даними, то у кожному конкретному випадку необхідно визначати наявні можливості та необхідні ресурси, які мають бути додані контролером для ідентифікації суб'єкта за номером телефону. Якщо можливість є, або мета та контекст обробки передбачає ідентифікацію суб'єкта, номер телефону буде виступати в якості персональних даних. Дане правило має за аналогією застосуватися і до інших номерів.

Позиція WP29 дотримується ідеї, що за наявності контактних даних третьої особи може призвести до порушення його права, навіть якщо суб'єкт не може бути ідентифікований. Характерною властивістю номера телефону, яка відрізняє його від інших номерів речей, є можливість безпосереднього зв'язку із суб'єктом та істотного втручання у приватне життя, завдання шкоди здоров'ю. Конфіденційність цих даних забезпечує безпеку життя та здоров'я суб'єкта, його близьких, дозволяє контролювати свої зовнішні комунікації, знижує його доступність для зовнішнього світу, вибудовує особисті межі суб'єкта, оберігає його особистий простір, що дає суб'єкту комфорт та впевненість [4]. Загалом контактні дані (номер телефону, email, адреса і т.д.) надають можливість шахраям безпосередньо зв'язатися із суб'єктом даних, попри його волю, погрожуючи

його життю та безпеці, маніпулюючи, заважаючи роботі та особистому життю.

Позиція WP29 приймає до уваги те, що для визначення ступеня вірогідності та ймовірності того, що контролер або інша третя особа, яка заволоділа інформацією, спробує ідентифікувати суб'єкта за такими даними, слід приймати до уваги розумні зусилля контролера або будь-якої третьої особи, що мають докласти, щоб ідентифікувати конкретного суб'єкта: витрати грошових коштів та зусиль; людських ресурсів; існування технології, що дозволяє виконати ідентифікацію без додаткових зусиль та витрат; поставлену мету, а не декларовану; які переваги може отримати контролер або інша особа; тривалість зберігання даних та потенційний розвиток технологій для ідентифікації в означений проміжок часу.

Означений алгоритм обробки персональних даних ґрунтується на оцінці ризику ідентифікації, а не на можливості ідентифікації особи як такої. Таким чином, за даним підходом інформація, яка є персональною, може бути визнана не персональними даними у разі, якщо ідентифікація особи за її допомогою невігідна або недоцільна, оскільки потребує непропорційних вигоди та витрат [16]. За твердженням М. Фінк і Ф. Паллас, позиція Європейської ради з охорони даних допоміжного органу ЄС базується на визнанні неперсональними даними лише тієї інформації щодо суб'єктів даних, яка не дозволяє їх ідентифікувати [18].

Регламент ЄС 2016/679 регулює також псевдонімізовані дані, під якими розуміється обробка персональних даних таким чином, що вони не можуть бути віднесені до певного суб'єкта даних без використання додаткової інформації, за умови, що додаткова інформація зберігається окремо і підлягає технічним та організаційним заходам, що гарантують, що персональні дані не віднесені до ідентифікованої особи або особи, яка може бути конкретно ідентифікована. Анонімізованою інформацією визнається інформація, яка не дозволяє проводити ідентифікацію осіб та не охоплюється правовим регулюванням Регламентом ЄС 2016/679. Фундаментальна відмінність псевдонімізованих та анонімізованих даних полягає в тому, що дані, анонімізовані належним чином, навіть за наявності додаткової інформації не можуть стати персональними даними.

З урахуванням зазначеного слід констатувати, що тлумачення персональних даних та неперсональних даних у вітчизняній доктрині неминуче буде зазнавати змін з урахуванням положень законодавства ЄС та євроінтеграційних процесів.

Підходи, розроблені у законодавстві ЄС, характеризуються досить широким тлумаченням персональних даних та подекуди складністю відмежування персональних даних від інших даних, які є неперсональними. Означене ставить потребу подальшого дослідження аспектів, пов'язаних із персональними даними, для підвищення рівня правової визначеності та імплементації напрацювань у вітчизняне законодавство.

Література

1. Токарева В.О. Віртуальна ідентичність як проєкція фізичної особи у мережі Інтернет. *The European dimension of modern legal science : Scientific monograph*. Riga, Latvia : «Baltija Publishing», 2022. С. 406-418.
2. European protection in good health? / ed. by S. Gutwirth, R. Leenes, P. De Hert, Y. Poullet. Springer, 2012. P. 323.
3. Карадаш А.В. Інформація про особу та персональні данні: окремі аспекти співвідношення. *Форум права*. 2017. № 4. С. 87-92.
4. Концевой Р.С. До питання визначення поняття «персональні данні». *Інформація і право*. 2012. № 2. С. 23-28.
5. Бодров Р.И. Гражданско-правовые средства индивидуализации граждан (физических лиц): вопросы теории и практики : дисс. канд. юр. наук : 12.00.03. Москва, 2016. С. 35.
6. Opinion 4/2007 on the concept of personal data. Adopted on 20th June. WP 136. Working Party An independent European advisory body on data protection and privacy. URL: http://ec.europa.eu/justice_home/fsj/privacy/index_en.htm.
7. Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data // OJ L 281. 23.11.1995. P. 0031-0050.
8. ECtHR. Leander v. Sweden. Application no. 9258/81. Judgment of 26 March 1987. Series A. No. 116. Para. 48.
9. ECtHR. Mikulić v. Croatia. Application no. 53176/99. Judgment of 7 February 2002. Para. 53.
10. ECtHR. Bensaid v. United Kingdom. Application no. 44599/98. Judgment of 6 February 2001. Para. 47; Peck v. United Kingdom. Application no. 44647/98. Judgment of 28 January 2003. Para. 57; S. and Marper v. the United Kingdom [GC]. Applications nos. 30562/04 and 30566/04. Judgment of 4 December 2008. Para. 66.
11. ECtHR. Z v. Finland. Application no. 22009/93. Judgment of 25 February 1997. Paras. 70-71.

12. ECtHR. *Schüssel v. Austria*. Application no. 42409/98, Decision of 21 February 2002; *Von Hannover v. Germany*. Application no. 59320/00. Judgment of 24 June 2004. Paras. 50-53.

13. ECtHR. *PG и JH v. United Kingdom*. Application no 44787/98. Judgment of 25 September 2001. Paras. 59-60.

14. ECtHR. *S. and Marper v. United Kingdom [GC]*. Applications nos. 30562/04 and 30566/04. Judgment of 4 December 2008. Paras. 68-86.

15. Analytical report on EU law applicable to sharing of non-personal data // Support Centre for data sharing. DG Connect. Smart 2018/1009. 24 January 2020. V2.0. P. 13

16. Крылова М.С. Принципы обработки персональных данных в праве Европейского союза. *Актуальные проблемы российского права*. 2017. № 10. С. 17-181.

17. Воронкевич С. Семь шагов для подготовки к новому Европейскому регламенту защиты персональных данных 14 сентября 2017. URL: <https://devby.io/news/global-data-protection-regulation>.

18. Charter of Fundamental Rights of the European Union // OJ C 326. 26.10.2012. P. 391-407. Ст. 7, 8; Joined cases C-92/09 and C-93/09. *Volker und Markus Schecke GbR (C-92/09) and Hartmut Eifert (C-93/09) v Land Hessen*. *Judgment of the Court (Grand Chamber)* of 9 November 2010. П. 53, 54.

19. Чурилов А.Ю. Принципы общего Регламента Европейского союза о защите персональных данных (GDPR): проблемы и перспективы имплементации. *Сибирское юридическое обозрение*. 2019. № 1. С. 29-35.

20. Finck M., Pallas F. They who must not be identified – distinguishing personal from non-personal data under the GDPR. *International Data Privacy Law*. 2020. № 10. P. 1-47.

Токарева В. О.,
кандидат юридических наук,
доцент кафедры гражданского права
Национального университета
«Одесская юридическая академия»
ORCID: 0000-0002-8409-1477