

*Різак М. В.,**кандидат юридичних наук,**Харківський національний університет внутрішніх справ*

КЛАСИФІКАЦІЯ ПЕРСОНАЛЬНИХ ДАНИХ ЯК НЕОБХІДНИЙ ЕЛЕМЕНТ ВВЕДЕННЯ ЕФЕКТИВНОЇ КОМУНІКАЦІЇ В СУСПІЛЬСТВІ

Анотація. Статтю присвячено висвітленню окремих особливостей правового регулювання персональних даних як специфічного інституту інформаційного права України. Здійснено аналіз досліджень ряду вчених, а також нормативно-правового масиву України у питанні класифікації персональних даних. Запропоновано класифікувати персональні дані на такі види: 1) загальні персональні дані; 2) спеціальні персональні дані; 3) вразливі персональні дані. Сформульовано пропозицію щодо вдосконалення понятійного апарату Закону України «Про захист персональних даних».

Ключові слова: інформація, інформаційне право, персональні дані, класифікація персональних даних, вразливі персональні дані, загальні персональні дані, спеціальні персональні дані.

Постановка проблеми. У сучасних умовах зміцнення й підвищення ролі інформаційно-телекомунікаційних технологій у суспільстві в усіх соціально-політичних, соціально-економічних та інших процесах, що відбуваються у світі, надзвичайно важливими стають проблеми створення ефективного механізму реалізації громадянами своїх прав та свобод, здійснення яких забезпечується, серед іншого, і якісним правовим регулюванням відносин щодо персональних даних.

Актуальність теми дослідження зумовлена активною законотворчою діяльністю в напрямку побудови інформаційного суспільства. Так, 09.01.2007 р. прийнято Закон України «Про Основні засади розвитку інформаційного суспільства в Україні на 2007–2015 рр.», 01.06.2010 р. – Закон України «Про захист персональних даних», 06.07.2010 р. – Закон України «Про ратифікацію Конвенції про захист осіб у зв'язку з автоматизованою обробкою персональних даних та Додаткового протоколу до Конвенції про захист осіб у зв'язку з автоматизованою обробкою персональних даних щодо органів нагляду та трансграничних потоків даних», 20.11.2013 р. – Закон України «Про Єдиний державний демографічний реєстр», 02.2013 р. – зареєстровано три законопроекти про удосконалення інституційної системи захисту персональних даних (реєстраційні номери 2282, 2282-1 та 2282-2).

Аналіз наукових джерел. Проблема реалізації права на інформацію неодноразово ставала предметом дискусій як науковців, законотворців, політиків, так і споживачів інформації. Зокрема, загальнотеоретичні питання класифікації персональних даних розглядають В. Брижко, Т. Єфременко, В. Іщєйнов, А. Кучеренко, А. Лушніков, М. Лушнікова, Н. Петрикiна та інші.

Разом із тим, незважаючи на існуючі наукові праці в напрямку дослідження, відсутність комплексних досліджень окресленого питання в українській правовій науці

ускладнює процес пошуку адекватної моделі національного механізму класифікації персональних даних, яка б узгоджувалася з міжнародно-правовими стандартами та гарантувала ефективний захист прав і свобод громадян України. З огляду на це, метою даного дослідження є аналіз наукових робіт і нормативно-правових актів щодо класифікації персональних даних та на підставі цього аналізу висловлення пропозицій щодо введення в обіг нових понять у сфері персональних даних.

Виклад основного матеріалу дослідження. Персональні дані винятково різноманітні та різнорізні. Їх можна розглядати в різних аспектах та об'єднувати в різні групи залежно від ознак і цілей класифікації. При цьому будь-яка класифікація буде досить умовною, позаяк деякі відомості можуть однаковою мірою стосуватися відразу декількох груп. Тому правове регулювання такого складного інституту як інститут персональних даних повинне бути гнучким і багатоваріантним [1, с. 45].

У чинному українському законодавстві на сьогодні відсутня чітка класифікація персональних даних. Натомість зарубіжний досвід свідчить про доцільність розподілу відповідної інформації на дві групи: дані загального характеру та особлива категорія персональних даних, до якої належить інформація про расове походження, політичні погляди, конфесійну належність, стан здоров'я тощо. Персональні дані цієї групи повинні мати особливий режим захисту та вищий рівень конфіденційності. Збір, обробка та використання таких даних повинні здійснюватися тільки за необхідності [2, с. 21].

У міжнародному законодавстві визнається умовний поділ персональних даних на дві групи: дані «загального змісту» та особливі категорії відомостей, що визначаються як дані «вразливі». До останніх відносять відомості про расове походження, політичні, релігійні чи інші вірування, а також щодо здоров'я чи сексуального життя. Для зазначеної категорії встановлюють додаткові заходи забезпечення їх безпеки. Так, згідно зі ст. 6 Конвенції № 108 Ради Європи ці відомості не повинні оброблятися автоматично, якщо в національному законодавстві не передбачаються достатні гарантії їх захисту. Положення Ради Європи встановлюють, що ст. 6 не містить повного переліку персональних даних, що розглядаються як «вразливі». Справа кожної держави – встановлювати обмеження щодо збору, реєстрації, накопичення, зберігання та поширення зазначених відомостей у національному законодавстві. Загальне правило зводиться до того, що персональні дані не повинні обробляти винятково з метою виявлення фактів, що характеризують фізичну особу лише негативно.

Обробка даних можлива з метою надання людині особливої допомоги або для спеціального дослідження. Системи, за допомогою яких здійснюються дії з персональними «вразливими» даними, повинні мати техніко-технологічні засоби їх захисту [3].

Російські науковці А. Лушніков і М. Лушнікова, спіраючись на загальноправові класифікації інформації, виокремлюють наступні її види: 1) за ступенем організованості (документована та інша інформація); 2) за ступенем доступу (загальнодоступна (відкрита) інформація та інформація з обмеженим доступом) [2, с. 24].

Відкрита інформація залежно від характеру доступу, у свою чергу, може поділятися на інформацію, яку суб'єкти зобов'язані довести до відома іншої сторони (наприклад, роботодавець зобов'язаний ознайомити працівників зі змістом локальних нормативно-правових актів, безпосередньо пов'язаних з їх трудовою діяльністю); яку суб'єкти зобов'язані надати у відповідь на запит (наприклад, роботодавець зобов'язаний у тижневий термін після отримання вимог про усунення виявлених порушень повідомити відповідний орган профспілкової організації про результати розгляду вимог та прийнятих заходів); яку суб'єкти зобов'язані надати для загального відома (наприклад, органи федеральної інспекції праці інформують громадськість про виявлені порушення трудового законодавства) [2, с. 43].

Залежно від наявності суб'єктивного фактора персональні дані можна поділити на два види: 1) фактичні дані, які не підлягають суб'єктивній оцінці (наприклад, про набути після закінчення навчального закладу спеціальність, службу у Збройних Силах України, інших військових формуваннях тощо); 2) персональні дані оціночного характеру, які можуть міститися у виробничій (службовій) характеристиці, висновку атестаційної комісії тощо.

На сьогодні залишається невирішеним і питання щодо статусу зображення людини: чи правомірно відносити його до персональних даних, адже саме зображення служить часто одним із основних ідентифікаторів особистості (так, наприклад, за зображенням людини можна отримати інформацію про її біометричні дані, національність, релігійну приналежність тощо). Зокрема фотографії громадян можуть використовуватися при неможливості пред'явлення особи до впізнання та при направленні запиту про видачу особи, яка перебуває на території іноземної держави; нотаріус має право засвідчувати тотожність особи громадянина з особою, зображеною на поданій громадянином фотокартці; іноземний громадянин, винний у порушенні законодавства України, підлягає обліку, у тому числі фотографуванню, тощо. Таким чином, ідентифікаційне призначення зображення громадянина, у тому числі фотографічної копії, є очевидним. При цьому безсумнівно залишається факт порушення прав людини (зокрема права на недоторканність приватного життя) при несанкціонованій обробці фотографічних та інших зображень.

Таким чином, питання віднесення зображення особи до числа персональних даних сьогодні залишається відкритим у межах українського праворозуміння та правозастосування. Видається, що оптимальним у даному випадку було б звернення до положень Директиви 95/46/ЄС Європейського парламенту та Ради Європейського Союзу від 24 жовтня 1995 р. «Про захист прав приватних осіб

щодо обробки персональних даних та про вільний рух таких даних», що розглядає відео- й аудіодані як персональні дані в безумовному порядку шляхом прямого закріплення в законі зображення в якості джерела персональних даних [4].

Поряд із загальними, так званими номінативними, персональними даними конвенція спеціально обумовлює необхідність гарантування вищого рівня безпеки низки персональних даних, автоматизована обробка яких може призвести до істотного ущемлення прав та інтересів деяких категорій осіб. Такі персональні дані, як ми вже відзначали вище, прийнято називати «вразливими». Дії з цими персональними даними без належних гарантій забезпечення прав суб'єкта можуть нанести йому додаткових збитків. Закон України «Про захист персональних даних» також містить перелік подібних персональних даних: «Забороняється обробка персональних даних про расове або етнічне походження, політичні, релігійні або світоглядні переконання, членство в політичних партіях та професійних спілках, звинувачення у скоєнні злочину або засудження до кримінального покарання, а також даних, що стосуються здоров'я чи статевого життя» (ч. 1 ст. 7) [5].

Згідно з конвенцією спеціальні персональні дані не можуть піддаватися автоматизованій обробці, якщо національне законодавство не встановлює відповідних гарантій. Однак ч. 2 ст. 7 Закону «Про захист персональних даних» передбачаються умови, за яких обробка зазначених категорій даних можлива:

1) здійснюється за умови надання суб'єктом персональних даних однозначної згоди на обробку таких даних;
2) необхідна для здійснення прав та виконання обов'язків у сфері трудових правовідносин відповідно до закону;
3) необхідна для захисту інтересів суб'єкта персональних даних або іншої особи у разі невідповідності або обмеження цивільної дієздатності суб'єкта персональних даних;

4) здійснюється 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;

5) необхідна для обґрунтування, задоволення або захисту правової вимоги;

6) необхідна в цілях охорони здоров'я, для забезпечення піклування чи лікування за умови, що такі дані обробляються медичним працівником або іншою особою закладу охорони здоров'я, на якого покладено обов'язки щодо забезпечення захисту персональних даних;

7) стосується обвинувачень у вчиненні злочинів, вироків суду, здійснення державним органом повноважень, визначених законом, щодо виконання завдань оперативно-розшукової чи контррозвідувальної діяльності, боротьби з тероризмом;

8) стосується даних, які були оприлюднені суб'єктом персональних даних [5].

Основною гарантією, наданою законом суб'єктам подібних персональних даних, є обов'язковість негайного

припинення їх обробки у випадку усунення причин, внаслідок яких вона здійснювалася. Здається, це положення не відповідає вимогам конвенції. Насамперед це пов'язано з тим, що персональні дані як інформація, на відміну від інших видів об'єктів, будучи навіть одноразово введені в обіг, не можуть бути вилучені з нього у традиційному розумінні. При здійсненні з ними будь-якої з операцій, які відповідають змісту поняття «обробка персональних даних», до них автоматично отримує доступ певне коло осіб, тобто, по суті, вони втрачають властивість, котра є особливо цінною для їх суб'єкта, – невідомість третім особам [6, с. 130].

При класифікації персональних даних слід приділити особливу увагу також біометричним (антропометричним) даним, тобто даним про фізіологічні особливості людини, на основі яких можна її ідентифікувати (зріст, вага, колір волосся, група крові, голос, почерк, відбитки пальців, результати аналізу ДНК, цифровий образ особи, сітківка ока тощо). Саме біометрична ідентифікація може дати абсолютно точну картину ідентифікації громадянина через унікальність біологічних параметрів: не існує двох людей із тотожними біометричними ознаками. Останнє забезпечує біометричним технологіям істотну перевагу перед розробленими раніше та широко запровадженими сьогодні системами контролю обмеженого доступу (наприклад, PIN-коди, пластикові картки з магнітною стрічкою, криптографічні коди тощо), щодо яких є ймовірність втрати, пошкодження, копіювання або незаконного використання третіми особами.

Потреба в надійній ідентифікації, досягнутий рівень біометрики, а також прагнення України до спрощення візового режиму з державами ЄС сьогодні призвели до прийняття 20 листопада 2012 р. Закону України «Про Єдиний державний демографічний реєстр та документи, що підтверджують громадянство України, посвідчують особу чи її спеціальний статус».

Перелік біометричних даних особи у Законі України «Про захист персональних даних» відсутній, проте дії щодо них, як правило, мають спеціальне правове регулювання, зокрема такі дані мають особливий статус у сфері оперативно-процесуальної діяльності. На сьогоднішній день взаємодія норм законодавства про оперативно-розшукову діяльність та про персональні дані носить проблемний характер через ряд питань, зокрема, з приводу застосування біометричної інформації, отриманої оперативними підрозділами негласно. Як підкреслюють окремі автори, викликає серйозні побоювання й сама можливість потрапляння у так звані «недружні» лабораторії біоматеріалів людей, які працюють у силових відомствах і на оборонних підприємствах [7].

Ще одним аспектом неузгодженості законодавства в цьому відношенні є вказівки Інструкції про призначення та проведення судових експертиз та Науково-методичних рекомендацій із питань підготовки та призначення судових експертиз та експертних досліджень [8] на те, що державні органи, які забезпечують збереження відомостей, зобов'язані зберігати та використовувати персональні дані.

Разом із тим, на біометричні дані в повному обсязі поширюються всі принципи обробки звичайних персональних даних, за винятком спеціально встановлених

вимог. Це означає, насамперед, ідентичність санкцій за незаконне отримання або використання біометричних даних і за аналогічні дії щодо інших категорій персональних даних.

А. Кучеренко вважає, що розподіл усіх персональних даних на три категорії – загальні, спеціальні та біометричні – є логічним, проте носить, швидше, теоретичний характер і чітко законом не закріплений [9, с. 184]. У свою чергу Н. Петрикін в якості альтернативи пропонує легальний розподіл персональних даних залежно від ступеня оборотоздатності на чотири категорії: 1) персональні дані, що можуть бути у вільному обігу (П.І.Б., адреса, номер телефону, електронна пошта тощо); 2) персональні дані, що обмежуються в обігу (реєстраційні номери, дата народження, освіта, сімейний стан, наявність дітей, стан здоров'я тощо); 3) персональні дані, що можуть бути в обігу лише в спеціальних цілях (дані про усиновлення (удочеріння), біометрична інформація, тощо); 4) заборонені для обігу персональні дані (спеціальні персональні дані) [1, с. 78].

Безумовно, запропонувати уніфікований підхід до класифікації персональних даних досить складно з огляду на те, що одна й та сама інформація про особу часто може набувати різних правових титулів, перебувати у вільному обігу, бути забороненою для обігу тощо. Однак беручи до уваги той факт, що головною особою, зацікавленою у збереженні обмеженого доступу до персональних даних, є їх суб'єкт (а об'єктом охорони є не самі дані, а права їх суб'єкта), цілком закономірним є припущення про наявність у нього права вибору – надати доступ до них будь-яким особам, обмеженому колу осіб або взагалі вилучити їх із обігу.

Слід зазначити, що окремими дослідниками пропонується й інші варіанти класифікації персональних даних. Так, наприклад, В. Іщейнов пропонує поділ їх на такі категорії: 1) фізичні та фізіологічні персональні дані; 2) співвідносні персональні дані. При цьому перелік даних людини, які традиційно відносять до біометричних, значно розширюється автором, зокрема він відносить до числа фізичних і фізіологічних персональних даних наступні: стать, вік, зріст, маса тіла, склад крові, склад ДНК, будова сітківки очей, цифровий образ особи, наявність (відсутність) пластичних операцій, відбитки пальців, відбитки долонь, сексуальна орієнтація, аперцепція, стан нервової системи, хронічні захворювання, відсутність будь-яких органів або частин тіла, наявність патологічних змін, індивідуальні особливості (гіпноз, телепатія тощо) [10, с. 89].

Слід зазначити, що окремі з названих В. Іщейновим видів інформації взагалі не мають правового змісту. Наприклад, аперцепція є філософським терміном, що означає свідоме сприйняття відомого чуттєвого враження, перехід від враження до пізнання; індивідуальні особливості людини, типу здібності до телепатії та гіпнозу, тим більше лежать поза правовою площиною. Крім того, запропонована вказаним автором класифікація жодним чином не сприяє вирішенню проблем правового регулювання обігу персональних даних, а лише ускладнює потенційне закріплення особливостей правового режиму окремих видів персональної інформації в нормах права [11, с. 60].

Різні класифікації персональних даних містяться й у національному законодавстві європейських країн. Наприклад, Закон Франції «Про інформацію, картотеки та свободи» виділяє в окрему категорію медичну інформацію про особу (за винятком даних, що накопичуються з метою терапевтичного або медичного контролю за пацієнтом і для дослідницьких цілей) і в спеціальному розділі виділяє порядок збору та обігу такої інформації. В окрему категорію виділені також дані про здоров'я, що накопичуються й обробляються з метою розвитку профілактичної та лікувальної діяльності [12, с. 99].

Згідно з угорським законом «Про захист персональних даних та публікацію даних, що представляють суспільний інтерес» в окрему категорію публічних персональних даних виділені відомості про імена та посади фізичних осіб, котрі обрані/призначені до центральних та місцевих органів влади [12, с. 119].

У Законі «Про персональні дані» Іспанії особливими положеннями регулюється обробка таких категорій персональних даних: а) ті, що визначаються законодавством про вибори; б) ті, що мають на меті збереження відомостей, які містяться в особистих звітах про рівень кваліфікації, про які йде мова в законах про військову службу; в) картотеки зображень і звуків, отриманих за допомогою використання відеокамер органами безпеки, згідно з відповідним законодавством [12, с. 109].

Три категорії персональних даних виділені законодавцем і в Законі Російської Федерації «Про персональні дані»: 1) загальнодоступні персональні дані; 2) спеціальні категорії персональних даних; 3) біометричні персональні дані – об'єднані в групи, виходячи з особливостей режиму їх обігу [12, с. 55].

Нині Закон України «Про захист персональних даних» не має чіткої класифікації персональних даних, однак слід констатувати, що перша редакція Закону закріплювала обов'язкову письмову згоду суб'єкта персональних даних на обробку інформації щодо нього, що створило реальну загрозу ефективної комунікації в суспільстві шляхом блокування обігу контактної інформації особи, що спричинило виникнення додаткового бар'єра інформаційним потоком. У процесі будівництва інформаційного суспільства така ситуація була неприпустимою, унаслідок чого законотворець виклав у новій редакції поняття «згода суб'єкта персональних даних», однак питання залишається актуальним і, на нашу думку, може бути вирішене виключно у разі запровадження класифікації персональних даних на законодавчому рівні.

Висновки. Основною проблемою у процесі запровадження класифікації персональних даних, котра вимагає адекватного правового вирішення, є те, що часто одні й ті ж персональні дані можуть бути одночасно віднесені до декількох видів. Через відсутність на законодавчому рівні класифікації персональних даних у розпорядника та володільця бази персональних даних виникають проблеми у виборі алгоритму дій щодо наявної в базі персональної інформації.

На підставі вищевикладеного, аналізуючи наукову літературу, законодавство України та зарубіжних держав, а також практику його застосування, вважаємо за доцільне:

1. Запропонувати класифікацію персональних даних на такі види: 1) загальні персональні дані; 2) спеціальні персональні дані; 3) вразливі персональні дані.

2. Ст. 2 Закону України про захист персональних даних доповнити новими термінами:

А) «*загальні персональні дані* – прізвище, ім'я та по батькові, дата народження, а також інші персональні дані, які за згодою суб'єкта цих даних розміщені в загальнодоступних базах персональних даних та які на момент їх обігу та/або обробки не були вилучені або знищені з цих баз»;

Б) «*вразливі персональні дані* – відомості про расове або етнічне походження, політичні, релігійні або світоглядні переконання, членство в політичних партіях та професійних спілках, звинувачення у скоєнні злочину або засудження до кримінального покарання, а також дані, що стосуються здоров'я чи статевого життя»;

В) «*спеціальні персональні дані* – персональні дані, які не входять до вразливих чи загальних персональних даних, межі обігу яких визначаються суб'єктом цих даних».

Крім того, вважаємо, що введення нових понять дасть можливість зменшити надмірне регулювання у сфері персональних даних та покращить комунікацію в суспільстві.

Література:

1. Петрыкина Н.И. Правовое регулирование оборота персональных данных в России и странах ЕС [Электронный ресурс] : Сравнительно-правовое исследование : Дисс. канд. юрид. наук : 12.00.14. / Н.И. Петрыкина. – Москва: РГБ, 2007. – (Из фондов Российской Государственной Библиотеки). – 188 с.
2. Лушников М.В., Лушников А.М. Право на информацию субъектов трудового права / М.В. Лушников, А.М. Лушников // Государство и право. – 2004. – № 6. – С. 42-48.
3. Брижко В.М. Права людини і захист персональних даних / В.М. Брижко. – Дк-зв'язок: Держкомзв'язку та інформатизації України. – 2000, 23 листопада.
4. Директива 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 [Електронний ресурс]. – Режим доступу : http://zakon2.rada.gov.ua/laws/show/994_242.
5. Про захист персональних даних : Закон України від 01 черв. 2010 р. / Верховна Рада України. – Офіц. вид. – К. : Парлам. вид-во, 2010. – 34 с. – (Бібліотека офіційних видань).
6. Кучеренко А.В. Классификация персональных данных : теоретико-правовой аспект / А.В. Кучеренко // Политика и право. Ученые записки. – Вып. 9. – Благовещенск : УКЦ «Юрист», 2009. – С. 127-133.
7. Ефременко Т. Биоматериалам дадут пропуск / Т. Ефременко // Российская газета. – 2007. – 7 июня.
8. Про затвердження Інструкції про призначення та проведення судових експертиз та Науково-методичних рекомендацій з питань підготовки та призначення судових експертиз та експертних досліджень : Наказ Міністерства юстиції України № 53/5 від 08 лист. 1998 // Офіційний вісник України від 03.12.1998.
9. Кучеренко А.В. Персональные данные как институт становления информационного общества в Российской Федерации / А.В. Кучеренко // Экономика, социология, философия, право : пути созидания и развития : Материалы междунар. научно-практич. конференции (21 декабря 2009 г.). – Ч. 2. – Саратов : ООО Издательство «КУБиК», 2010. – С. 183-185.
10. Ишейнов В.Я. Персональные данные в законодательных и нормативных документах Российской Федерации и информационных системах / В.Я. Ишейнов // Делопроектирование. – 2006. – № 3. – С. 90-94.
11. Кучеренко А.В. Особенности правового режима биометрических персональных данных / А.В. Кучеренко // Юридические науки и современность. Всероссийская научно-практическая конференция : сборник статей / МНИЦ ПГСХА. – Пенза : РИО ПГСХА, 2009. – С. 59-62.
12. Защита персональных данных. Опыт правового регулирования. – М., 2001. – 221 с.

Ризак М. В. Классификация персональных данных как необходимый элемент введение эффективной коммуникации в обществе

Аннотация. Статья посвящена освещению отдельных особенностей правового регулирования персональных данных как специфического института информационного права Украины. Осуществлен анализ исследований ряда ученых, а также нормативно-правового массива Украины в вопросе классификации персональных данных. Предложено классифицировать персональные данные на такие виды: 1) общие персональные данные, 2) специальные персональные данные 3) уязвимые персональные данные. Сформулировано предложение по совершенствованию понятийного аппарата Закона Украины «О защите персональных данных».

Ключевые слова: информация, информационное право, персональные данные, классификация персональ-

ных данных, уязвимые персональные данные, общие персональные данные, специальные персональные данные.

Rizak M. Classification of personal data as a necessary element of the introduction of effective communication in society

Summary. Article is devoted to some peculiarities of legal regulation of personal data as a specific institution of information law in Ukraine. Made the analysis a series of research scientists and regulatory array of Ukraine in the classification of personal data. Asked to classify personal data on: 1) general personal data, 2) special personal data 3) sensitive personal data. Formulated a proposal to improve the conceptual apparatus of the Law of Ukraine «On Protection of Personal Data».

Key words: information, information law, personal data, classification of personal data, sensitive personal data, general personal data, specific personal data.