УДК 004.056:340.132.1+316.324.8

БРИЖКО В.М., *доктор філософії (Ph.D.), старший науковий співробітник*

СУЧАСНІ ОСНОВИ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ В ЄВРОПЕЙСЬКИХ ПРАВОВИХ АКТАХ(*

Анотація. *Про сучасний стан міжнародно-правових стандартів та перспективи захисту персональних даних в умовах розвитку інформаційного суспільства.*

Ключові слова: *захист персональних даних, цифрові технології, інформаційні відносини, інформаційне право, інформаційне суспільство.*

Аннотация. *О современном состоянии международно-правовых стандартов и перспективах защиты персональных данных в условиях развития информационного общества.*

Ключевые слова: *защита персональных данных, цифровые технологии, информационные отношения, информационное право, информационное общество.*

Summary. *About the modern state of international legal standards and prospects of personal data protection under the conditions of development of information society.*

Keywords: *personal data protection, digital technologies, informative relations, informative right, informative society.*

Постановка проблеми. Умови застосування інформаційно-цифрових технологій та засобів електронної комунікації в економічній, фінансовій, банківській, культурній, правоохоронній і інших формах сучасної міжнародної співпраці передбачають вільний рух та збільшення потоків інформаційних ресурсів щодо товарів, капіталів і послуг, які звичайно супроводжуються різними персональними даними. Вже відомо, що нові технології та мережі дозволяють “стискати” час та “скорочувати” відстані, отримувати політичні, економічні, технологічні та інші переваги як у плані досягнення інтересів окремих осіб, так і в масштабах груп людей, регіону та країни. З іншого боку, проблема неправомірних і несанкціонованих дій з отримання та використання персоніфікованої інформації про фізичних осіб продовжує існувати.

Аналіз досліджень. У країнах Заходу, пострадянського простору та в Україні дослідження нормативно-правового впорядкування інформаційних відносин сфери обробки та використання персональних даних здійснювало багато осіб, про результати робіт деяких з них йдеться, зокрема, у [1 – 6]. При цьому реальність свідчить про те, що не тільки “спостерігається певна тенденція щодо спроб нівелювати право людини розпоряджатися власними персональними даними” [7], але існують проблеми, які додатково ускладнюють захист персональних даних у зв’язку з застосуванням технологій Інтернет речей, про що у нас мова йшла у [8], та поступовим поширенням так званих “хмарних” (інформаційно-обчислювальних) технологій (послуг, сервісів) (див., до прикладу [9 – 11]).

* Робота є продовженням досліджень за темою НДР “Теоретико-правові основи формування та розвитку інформаційного суспільства” .

Метою статті є визначення стану міжнародно-правових стандартів та перспектив захисту персональних даних.

Виклад основного матеріалу. Враховуючи активність у використанні технологій та мереж і, одночасно, загрози несанкціонованої автоматизованої обробки персональних даних, європейські країни з кінця 1970 років почали приймати спеціалізовані закони та приєднуватися до Конвенції Ради Європи № 108 “Про захист осіб у зв’язку з автоматизованою обробкою персональних даних” від 28.01.81 р. [12; 13, с. 66-72]. Головною передумовою цього була зростаюча активність поширення автоматизованих баз даних, розвиток телекомунікацій та потреба у забезпеченні приватного життя людини згідно принципів Європейської Конвенції “Про захист прав людини та основоположних свобод” (Рим, 04.XI.1950 р.) [13, с. 35-45].

Через декілька років принципи Конвенції Ради Європи № 108 з точки зору економічних інтересів були деталізовані у Директиві 95/46/ЄС Європейського парламенту та Ради[**] “Про захист осіб у зв’язку з обробкою персональних даних та вільним обігом цих даних” від 24.10.95 р. [13, с. 273-293], а також у Директиві 97/66/ЄС Європейського парламенту та Ради “Про обробку персональних даних і захист прав осіб у телекомунікаційному секторі” від 15.12.97 р. [13, с. 337-344]. Ці міжнародні акти вважаються першими міжнародно-правовими стандартами, що визначають умови гармонізації національних законодавств у сфері захисту персональних даних як для європейських, так й інших країн світу. Вони сприяли трансформації європейського розуміння поняття “privacy” (“приватність” – право на недоторканість особистого та сімейного життя) у бік застосування заходів захисту права на інформаційний суверенітет особи, зокрема, права людини визначати ким, коли, з якою метою та яким чином інформація про неї буде використовуватися іншими особами.

Сьогодні існує більш ніж 100 міжнародно-правових актів – Конвенцій, Протоколів, Директив, Рекомендацій Ради Європи та Європейського Союзу, які прямо або побічно відносяться до правового регулювання захисту персональних даних (деякі з них див. у [13]). Разом з цим, проблема неправомірних і несанкціонованих дій у сфері персональних даних фізичних осіб залишається актуальною і однозначно не вирішеною, як в юридичному, так і практичному сенсі. Наприклад: 1) більшість баз персональних даних у функціонуванні не є автономними, що суперечить вимогам міжнародних правових стандартів; 2) передача персональних даних за кордон не має реального організаційно-правового механізму; 3) для будь-якого бізнесу персональні дані – зручне і необхідне доповнення до всього того, що надається через Інтернет; 4) на багатьох ринках має місце незаконна торгівля CD з персональними даними; 5) продовжує функціонувати відповідна система збирання і продажу адресних списків персональних даних тощо.

Загалом, інформацію про особисте чи сімейне життя, зміст розмов, майновий стан, медичні відомості, теле- чи відео- особисте меню, вибір книг, газет чи журналів, зміст файлів на комп’ютерах та на автовідповідачах – все це та багато іншого за бажанням можна поєднати, проаналізувати та інтерпретувати (навіть створити негативний “викривлений портрет” особи) так, що людина, модель її поведінки виглядатиме “прозорою”, в усіх своїх якостях та проявах.

[**] “Рада” – це Рада Європейського Союзу, тобто Рада міністрів від кожної країни ЄС – головний орган ухвалювання рішень в ЄС, який виконує роль консолідуючого органу співробітництва з економічних та монетарних політик (http//ue.eu.int). “Європейська Рада” – це регулярні зустрічі глав держав та урядів країн ЄС, та інституціями Ради Європи, яка виконує роль консолідуючого органу співробітництва з гуманітарних питань (див. [13, с.10-12]).

У останні роки Європейська Комісія намагається створити та запровадити нову міжнародну систему захисту персональних даних на базі не лише правил про те, як здійснювати діяльність (Директив), але й завдяки встановленню правил прямої дії (Регламенту), які визначають безпосередній порядок регулювання діяльності.

У травні місяці 2016 року Європейський Парламент і Рада затвердили постанову про нові правила і порядок захисту персональних даних (“Пакет захисту даних”), який передбачає створення умов забезпечення узгодженої нормативно-правової бази на європейському рівні, що включає наступні документи:

- Регламент (ЄС) 2016/679 від 27.04.16 р. “Про захист фізичних осіб у зв’язку з обробкою персональних даних та про вільне переміщення таких даних, а також про скасування Директиви 95/46/ЄС (Загальні Положення про захист даних)” [14];
- Директива (ЄС) 2016/680 Європейського Парламенту і Ради від 27.04.16 р. “Про захист фізичних осіб у зв’язку з обробкою персональних даних компетентними органами в цілях запобігання, розслідування, виявлення або переслідування злочинця злочину або виконання кримінальних покарань, а також про вільне переміщення таких даних, і скасування Рамкового рішення Ради 2008/977/ПВД” [15];
- Директива (ЄС) 2016/681 Європейського Парламенту і Ради від 27.04.16 р. “Про використання даних записів реєстрації пасажирів (PNR) для профілактики, виявлення, розслідування і судового переслідування злочинів терористичного характеру і тяжкого злочину” [16].

Регламент (ЄС) 2016/679 від 27.04.16 р. “Загальні Положення про захист даних” (Регламент “GDPR”) містить 39 пункту преамбули та 99 статей.

Як вже зазначалося у [8], Європейський Парламент і Рада прийняли рішення про скасування Директиви 95/46/ЄС Європейського Парламенту і Ради від 24.10.95 р. та введення в дію Регламенту (ЄС) 2016/679 від 27.04.16 року. В офіціальному прес-релізі ЄС це пояснюється таким чином: “Європейська комісія висунула свою реформу ЄС про захист даних для того, щоб зробити Європу придатною для життя в цифрову епоху. Більше 90 % європейців говорять, що вони хочуть ті ж права захисту даних як в країнах ЄС – і незалежно від того, де обробляються їх дані” [14].

Мета і принципи Регламенту “GDPR” залишаються співзвучними з положеннями Директиви 95/46/ЄС, дія якої передбачена до 2018 р. Разом з тим, економічна інтеграція і розвиток ринку ЄС в умовах активного застосування інформаційних технологій призвели до значного збільшення трансграничних потоків персональних даних, зокрема завдяки можливостям Інтернету. Нові технології і глобалізація принесли з собою нові проблеми для захисту персональних даних. Масштаби їх збору і використання значно зросли. Технології змінюють як економіку, так і соціальне життя. Одночасно, відмінності, що існують в підходах до застосування Директиви 95/46/ЄС до обробки і захисту персональних даних в державах-членах ЄС, перешкоджають вільному переміщенню персональних даних на всій європейській території.

Ефективний захист персональних даних на європейській території вимагає зміцнення і встановлення в деталях прав суб’єктів даних і обов’язків тих, хто обробляє і визначає обробку персональних даних, конкретність повноважень для моніторингу виконання правил із захисту персональних даних, а також еквівалентних санкцій за їх порушення в державах-членах ЄС. Це передбачає необхідність правової визначеності і прозорості для всіх малих і середніх підприємств, точності обов’язків і ефективної співпраці між уповноваженими органами держав-членів ЄС. Для забезпечення захисту фізичних осіб і усунення перешкод на шляху потоків персональних даних в рамках ЄС,

національні системи обробки та захисту персональних даних повинні бути еквівалентними (рівноцінними – *від авт.*) у всіх державах-членах ЄС. Тому Європейська Комісія пропонує здійснити реформу системи захисту даних для того, щоб зробити Європу придатною для життя в цифрову епоху.

Основне поняття у сфері захисту персональних даних – це “персональні дані”, визначення якого з часом поступово змінювалося.

Перше визначення було надано у Конвенції Ради Європи № 108 від 1981 р.: *“персональні дані означають будь-яку інформацію, яка стосується конкретно визначеної особи або особи, що може бути конкретно визначеною (суб’єкт даних)”* [12].

У 1995 р. Директивою 95/46/ЄС було надано таке визначення: *“персональні дані – це будь-яка інформація про особу – ідентифіковану або таку, що може бути ідентифікована; такою, що може бути ідентифікована, вважається будь-яка особа чия особистість може визначатися прямо чи не прямо, зокрема, через ідентифікаційний номер або один чи декілька специфічних елементів фізичної, фізіологічної, психічної, економічної, культурної або соціальної тотожності”* [17].

У 2011 р., згідно прийнятого Європейською Комісією рішення [18], *“персональні дані – будь-яка інформація, що відноситься до особистого, професійного або суспільного життя людини – ім’я (особисті реквізити), фотографії, адреси електронної пошти, банківські реквізити, повідомлення на сайтах соціальних мереж, медична інформація, IP-адреса комп’ютера та інше, що завгодно”*.

За визначенням 2016 р., яке сформульовано у Регламенті “GDPR”, – *“персональні дані означають будь-яку інформацію, що стосується ідентифікованої фізичної особи або фізичної особи, що ідентифікується (“суб’єкта даних”); фізична особа, що ідентифікується – це особа, яка може бути ототожнена прямо або опосередковано, зокрема, з ім’ям, ідентифікаційним номером, даними про місцеположення, он-лайн-ідентифікатором, з одним чи декількома специфічними чинниками для встановлення фізичної, фізіологічної, генетичної, психічної, економічної, культурної або соціальної ідентичності цієї фізичної особи”* [14].

По відношенню до встановленого в Директиві 95/46/ЄС Європейського Парламенту і Ради від 1995 р. визначенню персональних даних, у Регламенті “GDPR” воно має аналогічний, але не тотожний з нею зміст. У ньому більш конкретизовано поняття персональних даних та розширений обсяг обов’язків і повноважень відповідних суб’єктів. Генетичні відомості визначені як персональні дані, що відносяться до успадкованих або набутих генетичних характеристик фізичної особи, які є результатом аналізу біологічного зразка, зокрема аналізу хромосом, дезоксирибонуклеїнової (ДНК) або рібонуклеїнової (РНК) кислоти. До відомостей, які стосуються минулого, поточного або майбутнього стану фізичного або психічного здоров’я фізичної особи, додано інформацію щодо надання медичних послуг. Запропоновано визначення “біометричні дані”, яке означає особисті дані, одержані в результаті конкретної технічної обробки, пов’язаної з фізичними, фізіологічними або поведінковими характеристиками фізичної особи, що дозволяє підтвердити унікальну ідентифікацію цієї фізичної особи, такі як зображення особи або її дактилоскопічні дані.

Як наголошується у Регламенті “GDPR”, захист фізичних осіб у зв’язку з обробкою персональних даних є фундаментальним правом. При цьому, це право не є абсолютним. Воно повинне розглядатися у зв’язку з його функцією в суспільстві і бути збалансованим з іншими основними правами, відповідно до принципу пропорційності, який має бути визначений у базовому законі країни.

Основні принципи обробки персональних даних, які означені у документах “Пакета захисту даних”, визначають дотримання наступного:

- персональні дані повинні оброблятися законно, справедливо і в доступній формі по відношенню до суб’єкта даних (“законність, справедливість і прозорість”);
- збиратися для певної, конкретної і законної мети і не піддаватися додатковій обробці, яка несумісна з цією метою; подальша обробка для цілей архівації, з метою наукових, дослідницьких, історичних і статистичних цілей не може бути несумісною з початковою метою (“цільове обмеження”);
- бути адекватними і обмежуватися тими даними, які відповідають і необхідні для досягнення цілі, для яких вони обробляються (“зведення до мінімуму даних”);
- бути точними і, при необхідності, постійно підтримуватися в актуальному стані; неточні персональні дані, з урахуванням цілі, для якої вони обробляються, слід видаляти або виправляти без затримки (“точність”);
- зберігається у формі, що дозволяє ідентифікувати суб’єкта даних не довше, ніж це необхідно для цілі, для якої вони обробляються; персональні дані можуть зберігатися протягом тривалішого періоду виключно для цілей архівації, інтересів наукових, дослідницьких, історичних і статистичних цілей (“обмеження зберігання”);
- обробляються так, щоб забезпечити належний захист персональних даних, включаючи захист від несанкціонованої або незаконної обробки, випадкової втрати, знищення або пошкодження, з використанням відповідних технічних або організаційних заходів (“цілісність і конфіденційність”).

Нові правила застосовуються до обробки даних фізичних осіб у компаніях, підприємствах тощо, які розміщуються не тільки на європейській території, але і здійснюють свою діяльність за межами ЄС і пов’язані з обробкою персональних даних в рамках ЄС. Правила не поширюються на обробку даних про юридичних осіб, а також на дані, які відносяться до анонімної інформації і померлих осіб.

Правила Регламенту “GDPR” не застосовуються до обробки персональних даних фізичною особою в ході чисто особистої або побутової діяльності і, таким чином, без зв’язку з професійною або комерційною діяльністю. Особиста або побутова діяльність може включати, зокрема, листування, використання особистої адреси (е-пошта), здійснення он-лайн-діяльності у мережах та ін., у відзначеному контексті діяльності. Суб’єкт даних повинен мати можливість передавати свої персональні дані з однієї системи електронної обробки в іншу, без втручання інших осіб.

Регулювання згідно положень Регламенту “GDPR” не застосовується до обробки персональних даних для забезпечення національної безпеки і діяльності правоохоронних органів (для цілей попередження, розслідування), а також до обробки персональних даних державами-членами ЄС по відношенню до загальної зовнішньої політики і політики безпеки ЄС.

Персональні дані, які обробляються державними органами в цілях запобігання, розслідування, виявлення або судового переслідування злочинів або виконання покарань, зокрема по запобіганню загрозам суспільної безпеки і вільного переміщення таких даних, регулюються іншим правовим актом ЄС, а саме Директивою (ЄС) 2016/680 Європейського парламенту і Ради (див. далі).

Кожна держава-член ЄС зобов’язана мати незалежний наглядовий орган для розслідування скарг і застосування адміністративних санкцій відносно правопорушень, а також співробітничати з незалежними наглядовими органами інших держав, забезпечуючи взаємну допомогу, організацію сумісних операцій, виявлення і судове переслідування порушень і виконання покарань.

Регламент “GDPR” вводить поняття “контролер” и “процесор”, які забезпечують засоби обробки персональних даних. “Контролер” означає фізичну або юридичну особу, державний орган, установу або інший орган, який, поодинці або спільно з іншими, визначає цілі і засоби обробки персональних даних, згідно законодавства. “Процесор” означає фізичну або юридичну особу, державний орган, установу або інший орган, який обробляє персональні дані за дорученням контролера. Також, в компаніях, підприємствах тощо мають бути призначені спеціалісти по захисту даних.

Регламент “GDPR” передбачає наступні санкції, які можуть бути накладені, зокрема: штраф в розмірі від 10.000.000 (або до 2 % від річного обігу за попередній фінансовий рік) до 20.000.000 євро (або до 4 % від річного обігу попереднього фінансового року).

Безпосереднє застосування Регламенту “GDPR” передбачено з 25 травня 2018 року для всіх держав-членів ЄС, які до вказаного терміну повинні привести свої національні законодавства в повну відповідність з положеннями нових правил.

Директива (ЄС) 2016/680 Європейського Парламенту і Ради від 27.04.16 р. “Про захист фізичних осіб у зв’язку з обробкою персональних даних компетентними органами в цілях запобігання, розслідування, виявлення або переслідування злочинця злочину або виконання кримінальних покарань, а також про вільне переміщення таких даних, і скасування Рамкового рішення Ради 2008/977/ПВД” (Директива “Поліція і органи юстиції”) містить 107 пункту преамбули та 64 статті.

Метою цієї Директиви є створення сильної, узгодженої і вищого рівня основи для ефективної судової і поліцейської співпраці по кримінальних справах в ЄС по відношенню до процесів обробки і захисту персональних даних компетентними органами і обміну даними між компетентними органами держав-членів для запобігання, розслідування, виявлення або судового переслідування кримінальних злочинів та виконання кримінальних покарань, зокрема запобігання загрозам суспільної безпеки.

Компетентними органами можуть бути не тільки державні органи, такі як судові органи, поліція або інші правоохоронні органи, але і будь-який інший орган або юридична особа, якій державою-членом довірено право здійснювати державну владу і суспільні повноваження для цілей цієї Директиви. Якщо такий орган або організація обробляє персональні дані для цілей, відмінних від цілей цієї Директиви, застосовується Регламент “GDPR”. Дозволено надавати персональні дані іншим компетентним органам тільки в конкретних випадках і відповідно до законодавства держави-члена.

Будь-яка обробка персональних даних повинна здійснюватися законно, бути справедливою і прозорою для суб’єктів даних, і виконуватися тільки згідно конкретно встановленої мети. Це саме по собі не перешкоджає правоохоронним органам у проведенні заходів, таких як таємні розслідування або відеоспостереження. Така діяльність може здійснюватися в цілях запобігання, розслідування, виявлення або судового переслідування кримінальних злочинів або виконання кримінальних покарань, зокрема по охороні проти і запобігання загрозам суспільної безпеки, тією мірою, яка встановлена законом і є необхідною, і відповідною мірою в демократичному суспільстві, з урахуванням законних інтересів фізичної особи, зацікавленої.

Захист фізичних осіб застосовується до обробки персональних даних за допомогою автоматизованих засобів, а також для ручної обробки. Файли або набори файлів, а також їх титульні сторінки, які не структуровані відповідно до певних критеріїв, під дію цієї Директиви не підпадають.

Директивою визначається, що рівень захисту прав і свобод фізичних осіб відносно обробки персональних даних компетентними органами в цілях запобігання,

розслідування, виявлення або судового переслідування кримінальних злочинів або виконання кримінальних покарань, зокрема гарантування запобігання загрозам суспільної безпеки, повинен бути еквівалентним у всіх державах-членах. Сьогодні для вищевказаних цілей застосовується Рамкове рішення Ради ЄС 2008/977/ПВД “Про захист персональних даних у зв’язку з їх обробкою в рамках поліцейської і судової співпраці по кримінальних справах” [19], чинність якої скасовується у 2018 р., згідно з цією Директивою.

Закон держави-члена, яка здійснює обробку персональних даних в рамках цієї Директиви, повинен визначати, які особисті дані підлягають обробці, мету обробки і процедури для збереження цілісності і конфіденційності персональних даних, а також процедури їх знищення, забезпечуючи тим самим достатні гарантії проти ризику зловживань і свавілля. При реалізації Директиви в національному законодавстві, держави-члени повинні вказати, які правила, що викладені в Регламенті “GDPR”, застосовуються.

Державам-членам, відносно обробки персональних даних, надана можливість забезпечити вищий рівень гарантій захисту, ніж той, який встановлений Директивою “Поліція і органи юстиції”. Можна звернути увагу на те, що ще у 1981 р. у ст. 11 Конвенції Ради Європи № 108 “Про захист осіб у зв’язку з автоматизованою обробкою персональних даних” було визначено: *“Жодне з положень цієї глави не тлумачиться як таке, що обмежує або іншим чином перешкоджає можливості Сторони забезпечувати суб’єктам даних більший ступінь захисту, ніж передбачено цією Конвенцією”* [12].

Директива “Поліція і органи юстиції” не застосовується до обробки персональних даних в ході діяльності установ або підрозділів, що займаються питаннями національної безпеки, яка підпадають під дію розділу V Договору про Європейський Союз. Обробка персональних даних повинна бути спрямована на зміцнення співпраці держав-членів в боротьбі з тероризмом та іншими серйозними злочинами у всіх країнах ЄС.

Директива не перешкоджає дотриманню принципу доступу до офіційних документів. Відповідно до Регламенту “GDPR” персональні дані, які зазначені у офіційних документах державних або приватних органів для виконання задач, що проводиться на користь суспільства, можуть бути розкриті відповідно до законодавства ЄС або національного законодавства.

Директива для органів поліції і юстиції спрямована на гармонізацію законів в державах-членах відносно обробки і обміну персональних даних між поліцією і судовими органами. З метою врахування різних правових традицій держав-членів, вона надає свободу дій в певних областях, зокрема, вказівки державам-членам на обов’язковість виконання конкретних операцій і процедур в національних правилах по кримінальних справах відносно обробки персональних даних судовими органами не передбачено.

Директива (ЄС) 2016/681 Європейського Парламенту і Ради від 27.04.16 р. “Про використання даних записів реєстрації пасажирів (PNR) для профілактики, виявлення, розслідування і судового переслідування злочинів терористичного характеру і тяжкого злочину” (Директива PNR)” містить 39 пунктів преамбули та 99 статей.

Метою Директиви PNR є забезпечення безпеки і захисту життя людей, а також створення правової основи для захисту персональних даних авіапасажирів міжнародних рейсів. Її положення спрямовані на запобігання, виявлення, розслідування і судове переслідування терористичних злочинів та серйозних злочинів шляхом регулювання передачі даних PNR від авіакомпаній державам-членам ЄС, а також обробку даних PNR компетентними органами в державах-членах ЄС.

Зібрані дані PNR можуть бути оброблені тільки для профілактики, виявлення, розслідування і судового переслідування терористичних і серйозних злочинів. Вони включають: ім’я пасажира, дату поїздки, маршрут проходження, відомості про квитки, контактні дані з турагентом, через якого політ був замовлений, використовувані засоби платежу, номер місця, відомості про багаж.

Директива PNR передбачає необхідність створення і застосування критеріїв оцінки терористичних і серйозних злочинів, які повинні зводити до мінімуму помилковість ідентифікаційних систем.

Авіаперевізники вже давно збирають і обробляють дані PNR в комерційних цілях. Директива PNR не накладає на них зобов’язань збору і збереження додаткових даних.

Нові правила визначають стандарт ЄС для обробки і використання даних PNR та включають положення, що відносяться до:

- мети, з якою дані PNR будуть оброблені в контексті правоохоронної діяльності (використання в розслідуваннях і судових переслідуваннях конкретних осіб);
- зберігання даних PNR (протягом 4.5 років), із суворою процедурою доступу до повної інформації (перелік даних, які збираються авіаперевізниками, представлений в Додатку 1 до Директиви PNR);
- обміну даними PNR між державами-членами ЄС та між державами-членами ЄС і третіми країнами. Обмін даними здійснюється за допомогою мереж обміну (електронних засобів), за умов забезпечення їх сумісності для форматів даних PNR і відповідних протоколів. Забезпечення створення однакових умов сумісності, застосовних до передачі (електронної передачі) даних від авіаперевізників, покладено на Комісію ЄС. Ці повноваження мають здійснюватися відповідно до Регламенту (ЄС) № 182/2011 Європейського парламенту і Ради “Про правила і загальні принципи механізму контролю державами-членами ЄС та здійснення Комісією ЄС виконавчих повноважень” [20];
- посилення гарантій захисту приватного життя та персональних даних, зокрема шляхом підвищення ролі національних наглядових органів і обов’язкового призначення співробітника по захисту даних PNR у відповідних організаціях;
- визначення в кожній державі-члені ЄС компетентного органу для профілактики, виявлення, розслідування або судового переслідування терористичних і серйозних злочинів для забезпечення виконання положень Директиви PNR. Національний контролюючий орган (Національний орган нагляду) кожної держави-члена відповідає за консультування і моніторинг застосування на своїй території прийнятих національних нормативних положень, згідно Директиви PNR;
- призначення в кожному органі реєстрації авіапасажирів (ОРА) співробітника по захисту даних, відповідального за контроль обробки даних PNR і реалізацію правових гарантій. ОРА зобов’язаний вести облік наступних операцій обробки: збір, консультації, розкриття інформації та її стирання. Протоколи консультацій і розкриття інформації повинні містити, зокрема, мету, дату і час проведення таких операцій і вказувати, наскільки це можливо, відомості про особу людини, яка консультувалася. Записи мають бути використані виключно для цілей перевірки, самоконтролю, забезпечення цілісності і безпеки даних або аудиту. ОРА повинен надавати записи по запиту Національного наглядового органу;
- встановлення правил відносно санкцій, зокрема фінансових, до авіаперевізників, які не передають дані.

Визначення “терористичні злочини”, що застосовується в Директиві PNR, відповідає визначенню встановленому рамковим рішенням Ради ЄС 2002/475/ПВД від

13.06.02 р. “Про боротьбу з тероризмом” [21]. Визначення “серйозний злочин” охоплює категорії правопорушень, що наведено в Додатку 2 до Директиви PNR.

Пропозиції Європейської Комісії про нові правила і порядок захисту персональних даних в контексті “Пакету захисту даних” викликали багато дискусій, суперечок і внесення значної кількості поправок. Ось деякі з них:

- вимоги мати в кожній компанії, підприємстві тощо штатного співробітника по захисту даних є новим для багатьох країн ЄС і піддається критиці у зв’язку з потребами додаткових фінансових витрат;
- реалізація нових правил ЄС по обробці і захисту персональних даних потребує всеосяжних змін ділової практики для всіх компаній (особливо неєвропейських) і додаткових адміністративними витрат;
- регламент розроблений з акцентом на соціальні мережі і провайдерів, але не достатньою мірою визначає вимоги до обробки даних співробітниками по захисту даних в компаніях (організаціях);
- передача (“переносимість”) даних не розглядається як один з ключових аспектів для захисту даних в контексті важливості і необхідності визначення вимог для функціонування соціальних мереж і провайдерів;
- слід чекати конфліктів в тлумаченні положень Регламенту ЄС 2016/679 і практики регулювання відносин з іншими неєвропейськими державами, що мають свої закони, правила і практику.

Разом з зазначеним вище слід звернути увагу на наступне.

По-перше. На сьогодні законодавство про захист персональних даних практично у жодній країні світу не досягло своєї зрілості, навіть на термінологічному рівні. Повна адекватність національних законодавств про захист персональних даних європейським правовим стандартам також не досягнута. На це є об’єктивні й суб’єктивні причини.

Основною дилемою упорядкування інформаційних відносин у сфері захисту персональних даних є протиріччя між прагненням максимального застосування персональних даних у державних (міждержавних), політичних, комерційних та особистих інтересах, й, одночасно, спрямованість у бажаннях та деклараціях захистити права на недоторканність приватного життя людини. Хоча ідея захисту персональних даних виходить з необхідності захисту індивідуума і гарантій верховенства його інтересів над “суспільними інтересами”, деякі інтереси можуть виконувати волю однієї особи (чи групи) із силою і невідворотністю натовпу. Проте, давно відомо, що будь-яке насильство повинне застосовуватися процедурно, за чинними у суспільстві правовими приписами та етичними принципами у окремому колективі.

З іншого боку, з погляду державних інтересів, обмеження прав на персональні дані має здійснюватися лише за законом. Це може пояснюватися тим, що без отримання персональних даних, без, так званого, каналу зворотного зв’язку в управлінні, держава існувати не може. Іншими словами, проблема дотримання інтересів усіх сторін – людини, суспільства і держави, на основі збалансованості їх прав та обов’язків продовжує існувати та потребує подальшої уваги.

По-друге. Запровадження запропонованого Європейською Комісією нового порядку захисту даних сьогодні, звісно, може викликати критичні зауваження стосовно того, що введення його в дію ускладнює старі проблеми та можливості їх вирішення на практиці. Головне у тому, що реалізація відповідних положень нового європейського порядку захисту персональних даних потребує нових ресурсів, нових підходів та всеосяжних змін ділової практики не тільки для всіх держав-членів ЄС, але і для всіх

неєвропейських країн, в більшості яких рівень захисту персональних даних і раніше не завжди відповідав положенням європейських правових стандартів.

Об’єктивна необхідність подальшого вдосконалення захисту прав людини в значною мірою визначається традиційно поширеним чинником неправомірних і несанкціонованих дій з персональними даними фізичних осіб, які продовжують мати місце, як на міжнародному, так і на національному рівнях. Більш того, враховуючи сучасні реалії активного застосування мереж та вдосконалення електронно-цифрових технологій, зокрема щодо активного поширення у західних країнах використання “хмарних” (інформаційно-обчислювальних) технологій [9 – 11], рішення проблеми захисту персональних даних значно ускладнилися. На сьогодні ці технології вважають перспективними, але вони не мають достатнього рівня захисту даних та опрацьованих правових формул у його забезпеченні. Це вимагає, хочеться того чи ні, додаткових ресурсів і пошуку нових ідей у підвищенні правової ефективності захисту персональних даних.

Саме ці обставини вимагають створення умов узгодженості і адаптації національних законодавств – рівень захисту прав і свобод фізичних осіб відносно обробки персональних даних повинен бути еквівалентним у всіх державах-членах ЄС, а також у державах, що мають соціальні та економічні з ними відносини.

По-третє. Як вважаємо, можлива спрямованість на максимальну деталізацію національного нормативно-правового упорядкування інформаційних відносин в сфері захисту персональних даних повинна враховувати те, що, по-перше, ідеальну нормативну модель захисту уявити та створити на папері можна, однак реалізувати її практично дуже складно та, на жаль, не завжди можливо, оскільки абсолютного захисту не існує – з появою нових технологій захисту виникають нові способи порушення інформаційної безпеки. По-друге, зайва деталізація правового упорядкування у цій сфері може ускладнювати розробку нових інформаційно-комп’ютерних технологій. Зазначене обумовлює відповідну мотивацію для “бізнес-софт-індустрії”, яка буде менш звертати увагу та пропонувати менше технологій, здатних забезпечити сильний захист даних. Й це особливо стосується “хмарних технологій”, про які було згадано раніше.

Висновки.

1. Персональні дані, як найбільш чутлива, делікатна і пріоритетно важлива для людини інформація, посідає особливе місце в інформаційних відносинах. Проблема їх захисту та поширення все життя супроводжує людину та пронизує будь-які сфери діяльності суспільства і держави. Від розуміння важливості й необхідності створення системи ефективного захисту персональних даних залежить спокій та благополуччя як окремої людини, так і держави.

2. Узагальнення основних принципів захисту персональних даних, які відображаються у положеннях всіх міжнародних стандартів, передбачає обов’язкове дотримання конкретних умов застосування персональних даних для будь-яких суб’єктів інформаційних відносин, при яких персональні дані повинні:

- бути доступними для суб’єкта даних;
- бути точними і оновлюватися;
- бути отримані законним способом;
- оброблятися з конкретною метою та за згодою на це суб’єкта даних і в кількості мінімально необхідній для визначеної мети;
- використовуватися тільки згідно визначеної мети;
- бути захищеними від несанкціонованого доступу та незаконної обробки.

Суб’єкт персональних даних має право на те, щоб не приймалося рішення, яке ґрунтується виключно на автоматизованій обробці його даних.

Таким чином, будь-яка обробка персональних даних повинна здійснюватися законно, бути справедливою і прозорою для суб’єктів даних, та виконуватися тільки згідно конкретно визначеної мети.

3. Узагальнення нових правил організаційно-правового забезпечення захисту персональних даних у Європейському Союзі передбачає наступне.

За Регламентом ЄС 2016/679 від 27.04.16 р. (“Загальні Положення про захист даних”) створюється Рада Європи по захисту даних, як окремий орган Європейського Союзу, який є юридичною особою. Склад Ради складається з представників контролюючих (наглядових) органів кожної держави-члена ЄС, Європейського супервайзера (Європейський інспектор) по захисту даних та Європейської Комісії (призначає голову Ради).

Згідно положень Конвенції № 108 Ради Європи від 1981 р. та “Пакету захисту даних” Європейського Союзу від 2016 р. у всіх європейських країнах та країнах, які пов’язані економічними відносинами с державами-членами ЄС, мають бути спеціальні державні інститути (один або декілька) по нагляду і контролю за дотриманням прав у сфері захисту персональних даних. Організаційно-правове та методологічне забезпечення мають здійснювати національні уповноважені органи нагляду (Омбудсмен чи Уповноважений) із захисту персональних даних, які є незалежними та підпорядкованими закону, підзвітними парламенту, у організаційних питаннях можуть бути підконтрольними уряду. Національні уповноважені органи призначають контролерів, які визначають цілі і засоби обробки персональних даних, яка здійснюється фізичною або юридичною особою, державним органом, установою або іншим органом (“процесором”), що обробляє персональні дані за його дорученням. Кожен контролер та процесор на підприємствах або в організаціях з чисельністю працівників більше 250 чоловік повинен вести облік діяльності по обробці персональних даних.

У корпораціях, підприємствах, організаціях тощо або їх об’єднаннях усіх форм власності має бути призначений спеціаліст по захисту даних. Він може бути штатним співробітником контролера або процесора, або виконувати задачі на підставі договору.

Держави-члени, національні наглядові органи повинні заохочувати розробку кодексів поведінки у сфері захисту персональних даних та створення механізмів сертифікації захисту даних, з урахуванням специфіки галузей діяльності і конкретних потреб різних корпорацій, підприємств тощо, а також здійснювати моніторинг їх виконання.

4. Законодавство про захист персональних даних має значний масив багатогранних та різнопланових документів, освоїти який не просто. На сьогоднішній день у цій області населення має слабке уявлення про свої права і їх застосуванні на практиці, фахівців дуже мало і нові вимоги можуть погіршити ситуацію. Тому є необхідність у введенні в систему освіти за напрямом “інформаційне право” окремої спеціалізації по юридичним та техніко-технологічним аспектам захисту персональних даних в цифрову епоху. Це може бути одним з важливих чинників на шляху професіоналізації зазначеної діяльності та приведення інформаційних відносин у відповідність з потребами рішення завдання захисту прав людини згідно європейських правових стандартів та одночасно дотримання інтересів держави у сфері персональних даних.

Використана література

1. Защита персональных данных / [А. Баранов, В. Брыжко, Ю. Базанов]. – К. : Національне агентство по інформатизації при Президентові України, ВАТ КП ОТІ, 1998. – 128 с. ;

Права человека и защита персональных данных / [А. Баранов. В. Брыжко, Ю. Базанов]. – Харьков : Фолио, 2000. – 280 с. – (Финансовая помощь и содействие в издании Харковской правозащитной группы и Национального фонда поддержки демократии (США).

2. Правовий механізм захисту персональних даних : монографія / В. Брижко ; за ред. М. Швеця та Р. Калюжного. – К. : Парлам. вид-во, 2003. – 120 с.

3. Інформаційне право та правова інформатика в сфері захисту персональних даних / [В. Брижко, М. Швець та ін.] ; за ред. М. Швеця. – К. : ТОВ “ПанТот”, 2005. – 451 с.

4. е-майбутнє та інформаційне право / В. Брижко, Ю. Базанов [та ін.] ; за ред. д.е.н., проф. М. Швеця. – [2-е вид., доп.]. – К. : ТОВ “ПанТот”, 2006. – 234 с.

5. Порівняльне-правове дослідження відповідності законодавства України законодавству ЄС у сфері персональних даних / [В. Брижко, А. Радянська, М. Швець]. – К. : Тріумф, 2006. – 256 с.

6. Електронний банкінг у контексті захисту персональних даних / В. Брижко, Ю. Базанов [та ін.] : за ред. чл.-кореспондента АПрН України М. Швеця. – К. : ТОВ “ПанТот”, 2008. – 141 с.

7. Пилипчук В.Г. Актуальні питання захисту прав, свобод і безпеки людини в сучасному інформаційному суспільстві : зб. матеріалів виступів на наук.-практ. конференції [“Проблеми захисту прав людини в інформаційному суспільстві”], (Київ, 1 липня 2016 р.) / НДІІП НАПрН України, НІСД, Секретаріат Уповноваженого Верховної Ради України з прав людини, НТУУ “КПІ” ; упорядн. Фурашев В.М., Петряев С.Ю. – К. : Вид-во “Політехніка”, 2016. – С. 6-8.

8. Захист персональних даних в сфері Інтернет речей / О. Баранов, В. Брижко // Інформація і право. – № 2(17)/2015. – 75-81.

9. Cloud computering : основные концепции и тенденции развития / З.С. Сейдаметова, В.А. Темненко // Ученые записки Крымского инженерно-педагогического университета. – Вып. 28. – Симферополь : НИЦ КИПУ, 2011. – С. 43-48.

10. Cloud computering и облачная модель представления ИТ-услуг / В.И. Гриценко, А.А. Урсатьев // Кибернетика и вычислительная техника. – 2013. – Вып. 171. – С. 5-19.

11. Гнатюк С.Л. Актуальні питання захисту персональних даних у віртуальному середовищі (на прикладі технологій та сервісів “хмарного” обчислення) : аналітична записка. – Режим доступу : http://www.niss.gov.ua/articles/1090

12. Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data : Amendment to Convention ETS No. 108 allowing the European Communities to accede. – Strasbourg, 28.1.1981. – Режим доступу : http://www.convention.coe.int/treaty/en/Treaties/Html/108.htm

13. Системна інформатизація правоохоронної діяльності : європейські нормативно-правові акти та підходи до упорядкування інформаційних відносин у зв’язку з автоматизованою обробкою даних : посіб. / В. Брижко, М. Швець [та ін.]. – Кн. 2. – К. : ТОВ “ПанТот”, 2006. – 509 с.

14. 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) : Reglament (EU) 2016/679 of the European Parlament and of the Council, of 27 April 2016. – Режим доступу : http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016 R0679&from= EN

15. On the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data and repealing Council Framework Decision 2008/977/JHA : Directive (EU) 2016/680 of the European Parliament and of the Council, of 27 April 2016. – Режим доступу : https:///eur-lex.europa.eu/legal-cont ent/en/TXT/%3Furi%3DCELEX%253A32016L0680 &p rev=search

16. On the use of passenger name record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime : Directive (EU) 2016/681 of the European Parliament and of the Council, of 27 April 2016. – Режим доступу : https://consilium.europa.eu/en/press/press-releases/2016/04/21-council-adopts-eu-pnr-directive/&prev=search

17. On the Protection of Individuals with regard to the of Personal Data and on the free movement of such Data : Directiva 95/46/EC of the European Parliament and of the Council. – Режим доступу : // www.evropa.eu.int/ISPO/legal/en/dataprot /directiv/directiv.html

18. On the application of patients' rights in cross-border healthcare : Directive 2011/24/EU of the European Parliament and of the Council, of 9 March 2011. – Режим доступу : http://eur-lex. europa. eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2011.088.01.0045.01.ENG&toc=OJ:L:2011:088:TOC

19. On the protection of personal data processed in the framework of police and judicial cooperation in criminal matters : Council scope decision 2008/977/JHA, of 27 November 2008. – Режим доступу : http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2008.350.01.0060.01.ENG&toc=OJ:L:2008:350:TOC

20. On laying down the rules and general principles concerning mechanisms for controlby Member States of the Commission's exercise of implementing powers : Regulation (EU) No 182/2011 of the European Parliament and of the Council, of 16 February 2011. – Режим доступу : http://eur-lex. europa. eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2011.055.01.0001.01.ENG&toc=OJ:L:2011:055:TOC

21. On combating terrorism : Council Framework Decision, of 13 June 2002 . – Режим доступу : http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2002.164.01.0003.01.ENG&toc=OJ:L:2002:164:TOC

~~~~~~~~~~~~~ * * * ~~~~~~~~~~~~~
~~~~~~~~~~~~~