ПРАВО ЕВРОПЕЙСКОГО СОЮЗА

УДК 342.721

ІНСТИТУЦІЙНО-ПРАВОВИЙ ЗАХИСТ ПЕРСОНАЛЬНИХ ДАНИХ В ЄВРОПЕЙСЬКОМУ СОЮЗІ

Костянтин МЕЛЬНИК,
здобувач наукового ступеня кандидата юридичних наук
Науково-дослідного інституту інформатики і права
Національної академії правових наук України,
начальник управління юридичного забезпечення
Державної служби України з питань захисту персональних даних

SUMMARY

Control of compliance with legal requirements of the European Union on processing of personal data, which carried out at the level of supranational bodies of the European Union and at the level of national institutions, is a priority of the European Union in the context of the functioning of an effective system of personal data protection. The comprehensive analysis of institutional legal mechanisms on personal data protection in the European Union, recent trends in the legal reform in the European Union at this sphere, are investigated in the article. Research in this paper may be useful in seeking and reasoning of the optimal national institutional model of personal data protection.

Key words: personal data, personal data protection, institutional legal mechanisms, European Union.

АНОТАЦІЯ

Контроль над відповідністю законодавчим вимогам Європейського Союзу процесів обробки персональних даних, що здійснюється як на рівні наддержавних органів Європейського Союзу, так і на рівні національних установ, є пріоритетним напрямом діяльності Європейського Союзу в контексті функціонування дієвої системи захисту персональних даних. В статті проведено комплексний аналіз інституційно-правових механізмів захисту персональних даних в Європейському Союзі, досліджено останні тенденції правових реформ в Європейському Союзі в цій сфері. Дослідження, проведене в даній статті, може стати в нагоді під час пошуку та обґрунтуванні оптимальної національної інституційної моделі захисту персональних даних.

Ключові слова: персональні дані, захист персональних даних, інституційно-правові механізми, Європейський Союз.

Постановка проблеми. Одним з основних напрямів діяльності Європейського Союзу (ЄС) у сфері захисту персональних даних є здійснення контролю над відповідністю процесів обробки персональних даних, що здійснюється як на рівні наддержавних органів ЄС, так і державних (муніципальних) установ, приватних структур, вимогам законодавства ЄС. Європейським Союзом на сьогодні створено досить розгалужений інституційний механізм із захисту персональних даних як на наддержавному рівні, так і безпосередньо в державах-членах ЄС.

Так, відповідно до статті 286 Договору про заснування Європейської Спільноти з 1 січня 1999 року акти ЄС про захист інтересів особи щодо опрацьовування персональних даних та вільного руху таких даних належить застосовувати до інституцій та органів, створених цим Договором чи на його підставі. До дати, зазначеної в частині першій, Раді, діючи згідно з процедурою, зазначеною в статті 251 цього Договору, належить створити *незалежний наглядовий орган,* уповноважений здійснювати нагляд за застосуванням цих актів ЄС до інституцій та органів ЄС, та ухвалювати будь-які потрібні дотичні заходи, що є доцільними [1].

Метою статті є комплексний аналіз інституційно-правового захисту персональних даних в Європейському Союзі як на наднаціональному, так і на національному рівнях. Дослідженню окремих питань цієї проблематики в різні часи приділяли увагу такі українські фахівці та вчені, як В. Брижко, М. Різак, А. Пазюк, Ю. Базанов, М. Швець, А. Радянська. Розгляд цього питання здійснюється і зарубіжними вченими: І. Вельдер, М. Важорова, Л. Брейдейс, С. Уоррен, Р. Валєєв та інші. Наукові пошуки з даного питання знаходяться на стадії свого розвитку, який, в свою чергу, потребує подальших досліджень.

Методологічну основу даного дослідження становлять організаційно-правовий, порівняльний та діалектичний методи.

Виклад основного матеріалу дослідження. Базовим документом, який запроваджує інституційний механізм із захисту даних на рівні інституцій ЄС, є Регламент Європейського Парламенту та Ради № 45/2001

від 18.12.2000 про захист фізичних осіб у зв'язку з обробкою персональних даних установами і органами Європейської Спільноти і щодо вільного переміщення таких даних (далі – Регламент № 45/2001) [2]. Установи і органи, створені Договорами про заснування Європейських Спільнот, повинні відповідно до цього Регламенту і на виконання Директиви Європейського Парламенту і Ради № 95/46/ЄС про захист фізичних осіб під час обробки персональних даних і про вільне переміщення таких даних (далі – Директива № 95/46/ЄС) [3] гарантувати захист основних прав і свобод фізичних осіб, і зокрема, їх право на приватне життя, які стосуються обробки персональних даних, і не повинні ні обмежувати, ні забороняти вільну передачу персональних даних між собою або одержувачами, підпорядкованими національному праву держав-членів ЄС.

Відповідно до статті 41 Регламенту № 45/2001 засновується посада незалежного контролюючого інституту влади – *Європейського уповноваженого із захисту даних (далі – Уповноважений)*. У питаннях обробки персональних даних Уповноважений повинен слідкувати за повагою з боку установ і органів ЄС до фундаментальних прав і свобод фізичних осіб, зокрема, до їх права на приватне життя, гарантувати і наглядати за застосуванням положень цього Регламенту і будь-якого іншого акту ЄС, пов'язаного із захистом фундаментальних прав і свобод фізичних осіб щодо обробки персональних даних установою чи органом ЄС, а також він повинен висловлювати свою думку установам і органам ЄС та заінтересованим особам щодо всіх питань, пов'язаних з обробкою персональних даних [2].

Призначення Уповноваженого на посаду здійснюється за результатами публічного конкурсу кандидатів. Європейський Парламент і Рада ЄС за спільною згодою призначають Уповноваженого на термін до п'яти років на основі списку, розробленого Європейською Комісією в результаті відкритого скликання кандидатів. Разом із Уповноваженим на аналогічний термін за цією ж процедурою призначається і його заступник. Окрім цього, Уповноважений може бути переобраний на цю посаду. Крім періодичного переобрання або заміщення з причини смерті, мандат Уповноваженого може бути зупинений у випадку подання про відставку або звільнення [4, с. 73-74].

Одним із головних принципів діяльності Уповноваженого є його незалежність, яка забезпечується за допомоги цілого ряду заходів, передбачених Регламентом № 45/2001, серед яких існує необхідність виокремити наступні:

1) кандидат на цю посаду може бути обраний з числа осіб, чия незалежність не викликає сумнівів і хто володіє досвідом і навичками, необхідними для роботи на зазначеній посаді, наприклад, в силу їх попередньої участі в роботі національних органів із захисту персональних даних держав-членів ЄС (стаття 42 (2) Регламенту № 45/2001);

2) Уповноважений може бути звільнений або позбавлений привілеїв тільки за рішенням Суду ЄС на вимогу Європейського Парламенту, Ради ЄС або Європейської Комісії, в разі невідповідності вимогам, необхідним для виконання його обов'язків, або у випадку вчинення посадового злочину;

3) Уповноважений користується всіма привілеями та імунітетами, передбаченими для суддів Суду ЄС згідно Протоколу привілеїв та імунітетів ЄС;

4) Уповноважений та його заступник під час виконання своїх обов'язків діють абсолютно незалежно і не звертаються за вказівками, так само як і не отримують будь-яких вказівок від будь-кого.

В період дії їх мандату вони не можуть займатися діяльністю, несумісною з їх посадовими обов'язками незалежно від того, чи є вона прибутковою чи ні. Крім того, після завершення свого мандата вони повинні з особливою розсудливістю вибирати подальший вид своєї роботи;

5) на Уповноваженого та його штат як в період їх роботи, так і після його завершення поширюється правило про збереження конфіденційності всієї інформації, що стала їм доступною у зв'язку з виконанням своїх посадових обов'язків [5, с. 620-621].

Російський науковець І. Вєльдер зазначає, що Уповноважений відіграє значну роль в політиці щодо захисту персональних даних за допомогою надання своїх консультаційних роз'яснень як за власною ініціативою, так і у відповідь на звернення зацікавлених органів. Зокрема, мова йде про підготовку рішень або власних норм, пов'язаних з обробкою персональних даних, про що інституції ЄС повинні інформувати Уповноваженого. Консультативна функція на вищому рівні проявляється в співпраці з Європейською Комісією з питань прийняття нормативних актів стосовно захисту прав фізичних осіб під час обробки їх персональних даних [4, с. 80].

Окрім вищезазначених повноважень, Уповноважений заслуховує та розслідує скарги, а також інформує осіб, що звернулися зі скаргою (фізичних осіб, про яких або від яких збираються або щодо яких обробляються дані), про своє рішення протягом «розумного» строку. Зазначене повноваження кореспондує праву кожного суб'єкта персональних даних звертатися до Уповноваженого зі скаргою про порушення права на захист персональних даних, передбачене статтею 286 Договору про заснування Європейської Спільноти, будь-якою інституцією ЄС. У випадку, якщо Уповноважений не надасть відповіді протягом шести місяців з моменту подачі скарги, скарга вважається відхиленою (стаття 46 (2) Регламенту № 45/2001) [2].

Слід зазначити, що Регламент № 45/2001 передбачає 2 особливих види скарг Уповноваженому:

1) права суб'єктів персональних даних можуть бути обмежені в силу попередження або розслідування злочинів, або в силу особливих економічних інтересів

держав-учасниць ЄС, або іншого публічного інтересу. У цьому випадку фізична особа, чиї права обмежені, повинна бути інформована про своє право звернутися зі скаргою до Уповноваженого (стаття 20 Регламенту № 45/2001);

2) стаття 33 Регламенту № 45/2001 передбачає право будь-якої фізичної особи, найнятої на роботу інституцією ЄС, подати скаргу Уповноваженому за наявності підозри щодо порушення норм Регламенту, причому скарга може бути подана в обхід офіційних каналів. При цьому ніхто не може бути підданий переслідуванню за подачу подібної скарги [2].

Можна припустити, що у зв'язку з величезним обсягом обробки персональних даних, і особливо «чутливих» даних (про стан здоров'я, релігійні переконання, членство в політичних партіях), дана категорія скарг може складати значний обсяг роботи апарату Уповноваженого.

При наявності певних правових і технічних гарантій Уповноважений має право санкціонувати обробку персональних даних у статистичних цілях або у випадку, коли це необхідно в інтересах історичного чи наукового дослідження, причому без інформування суб'єктів персональних даних про цілі та способи обробки даних про них, як це передбачено практично у всіх інших випадках обробки персональних даних. Уповноважений також може схвалити обробку даних про телефонні розмови – дані трафіку – для цілей планування телекомунікаційного бюджету передавальної компанії або для цілей управління трафіком [5, с. 623].

Діяльність Уповноваженого носить також характер взаємодії, що здійснюється у двох основних площинах: у площині національних органів (обмін інформацією, вимога виконання своїх зобов'язань із захисту персональних даних, розгляд спірних питань) та у площині наглядових органів ЄС (співробітництво з Європолом, органами Шенгенської угоди та Євроюстом) [6, с. 116].

Враховуючи норми Директиви № 95/46/ЄС, Регламент № 45/2001 встановив правило про обов'язкове повідомлення контролерами даних (володільцями персональних даних) про операції з обробки персональних даних. Відповідно до статті 24 Регламенту № 45/2001 кожен орган ЄС призначає спеціально уповноважену особу – *Офіцера із захисту персональних даних (далі – Офіцери),* завданнями якого є забезпечення суб'єктів персональних даних інформацією про їхні права, дотримання норм Регламенту № 45/2001 на конкретному інституційному рівні, сприяння Уповноваженому у розслідуванні скарг, повідомлення останнього про ризиковані операції з обробки персональних даних тощо. Офіцери працюють в Європейському Парламенті, Раді ЄС, Європейській Комісії, Суді ЄС, Суді Аудиторів, Європейському економічному та соціальному комітеті, Європейському медичному агентстві тощо. Офіцер також виконує й функцію реєстратора операцій з обробки даних, саме його контролери даних повинні завчасно повідомляти про подібні операції. Так, офіцер повинен бути поінформований про найменування контролера, мету обробки персональних даних, про категорії суб'єктів даних, правові підстави обробки даних, про категорії одержувачів даних тощо. В свою чергу, Уповноважений має право прямо чи опосередковано перевіряти реєстри операцій [7, с. 43].

На думку європейських законодавців, обробка даних про здоров'я громадян, про підозру у скоєнні злочину, про наявність звинувачень та застосування запобіжних заходів, а також здійснення операцій, спрямованих на оцінку здібностей, поведінки громадян або на обмеження їх прав, у тому числі за договором, являє собою певну загрозу захисту прав і свобод громадян за своєю природою або в силу мети обробки даних. Усі подібні операції підлягають попередній перевірці Уповноваженим з повідомленням Офіцера [6, с. 101].

Європейське законодавство про захист персональних даних накладає суттєві обмеження на передачу персональних даних у треті країни, де не існує адекватного режиму їх захисту. Винятки можливі у випадку, якщо, наприклад, передача даних за кордон необхідна для захисту життєво важливих інтересів суб'єкта персональних даних або коли суб'єкт сам дав на це однозначну згоду. Однак Уповноважений може схвалити передачу персональних даних у інші держави (окрім держав-членів ЄС) або інші міжнародні організації, якщо визнає, що рівень захисту даних, а отже, і прав їхніх суб'єктів відповідає необхідним правовим параметрам. Адекватний рівень захисту може випливати із зобов'язань у сфері захисту персональних даних, прийнятих, наприклад, на основі двох- і багатосторонніх міжнародних договорів [8, с. 527].

Вищезазначені інституції з питань захисту персональних даних є основними в Європейському Союзі, діяльність та спеціалізація яких направлена на захист персональних даних на наднаціональному рівні ЄС у практичному вимірі. Так, функції інституту Європейського уповноваженого із захисту даних подібні до функцій Омбудсмена з прав людини, але більш вузько спеціалізовані в межах захисту персональних даних.

Водночас, окрім контрольно-наглядових механізмів із захисту персональних даних на рівні ЄС існують й інші. Так, Європейська Комісія, як вже зазначалось, створила досить дієвий інститут консультацій та правової підтримки в сфері захисту персональних даних. Першим практичним втіленням цього напряму діяльності ЄС є створення в 1996 році так званої «Робочої групи статті 29» – *Робочої групи із захисту даних (далі – Робоча група),* утвореної відповідно до статті 29 Директиви 95/46/ЄС, діяльність якої направлена на гармонізацію європейського права у сфері захисту персональних даних та полегшення застосування для європейських країн, втілених у Директиві принципів [9, с. 28].

Робоча група має консультативний статус і діє незалежно. Вона складається з представників національних наглядових органів держав-членів ЄС, представника органів, створених установами та органами ЄС, і представника Європейської Комісії. Робоча група виконує дослідницьку, експертну і консультативну функції. Згідно зі статтею 30 Директиви № 95/46/ЄС, вона досліджує питання щодо застосування національних положень, надає висновки про рівень захисту персональних даних як всередині ЄС, так і в третіх країнах, а також про відповідність кодексів поведінки, прийнятих на рівні ЄС, вимогам Директиви № 95/46/ЄС. Робоча група надає також консультації Європейській Комісії щодо подальших змін цієї Директиви та можливих додаткових чи спеціальних заходів для забезпечення прав і свобод осіб стосовно обробки персональних даних.

Діяльність та ефективність Робочої групи можна прослідкувати за наступними напрямами:

• Обґрунтування доцільності віднесення *права на захист персональних даних* до європейського «каталогу фундаментальних прав». На своєму засіданні 4 липня 1999 року у Кельні (Німеччина) Рада ЄС ухвалила рішення про підготовку проекту Хартії основних прав Європейського Союзу. У зв'язку з цим Робоча група, підтримуючи рішення Ради ЄС, ухвалила 7 вересня 1999 року рекомендацію, якою запропонувала включити *право на захист персональних даних до* європейського «каталогу фундаментальних прав». При цьому Робоча група обґрунтувала свою позицію тим, що у своїх висновках і рішеннях Європейська Комісія і Суд ЄС розвинули і визначили фундаментальне право як таке, що основане на різних правах людини, яке стосується захисту персональних даних [10].

• Надання численних рекомендацій та висновків щодо застосування законодавства про захист персональних даних, зокрема стосовно тлумачення термінів «персональні дані», «згода суб'єкта персональних даних»; конфіденційності персональних даних в мережі Інтернет; обробки персональних даних у контексті працевлаштування; обробки персональних даних, одержаних шляхом відеоспостереження; електронного урядування; застосування правил ЄС в контексті захисту даних у процесі боротьби з хабарництвом, банківськими та фінансовими злочинами тощо. З детальним переліком та текстами українською мовою зазначених рекомендацій та висновків можна ознайомитись у монографії за редакцією О. Мервінського «Захист персональних даних: міжнародні стандарти. Збірник нормативно-правових документів» [2].

• Активна участь у виробленні правової позиції ЄС щодо кодексів поведінки у сфері захисту персональних та інших механізмів саморегуляції, яка полягала в тому, що запропонована різними приватними компаніями модель саморегуляції, в цілому, не може розглядатися як альтернативна до законодавчого регулювання питання захисту персональних даних. Низький рівень захисту і неможливість забезпечення проголошених корпоративних стандартів є слабкими місцями цієї регулятивної моделі. У документі, який був підготовлений Робочою групою під назвою «Засуджуючи індустріальну саморегуляцію», експерти ЄС дійшли висновку, що інструмент саморегуляції може розглядатися як дієва складова «адекватного захисту» за таких умов: він буде обов'язковим до виконання для всіх членів, яким дані передаються, і забезпечувати адекватні гарантії у разі передачі даних третім особам; прозорим і містити основний зміст принципів захисту даних; мати механізм для забезпечення достатнього рівня його додержання в цілому через систему превентивних санкцій і покарання, а також обов'язковий безсторонній аудит; надавати підтримку і допомогу суб'єктам даних, які зіткнулися з проблемами; мати легкодоступний, неупереджений і незалежний орган для розгляду заяв суб'єктів даних і прийняття рішень у разі порушень кодексу; гарантувати у випадках його порушення відповідну компенсацію для суб'єкта персональних даних [11].

• Розробка рекомендацій у галузі транскордонної передачі персональних даних. Зазначені рекомендації знайшли своє відображення у документі «Попередній погляд на застосування договірних положень у контексті передачі персональних даних до третіх країн», прийнятий 22 квітня 1998 року Робочою групою. В цьому документі, зокрема, наголошується, що оцінювати ефективність контрактної форми захисту персональних даних слід за такими критеріями: 1) досягнення належного рівня дотримання встановлених правил; 2) надання підтримки і допомоги суб'єктам даних у реалізації їх прав; 3) забезпечення відповідного відшкодування і поновлення прав у разі їх порушення. З метою посилення відповідних контрактних положень щодо надання відшкодування і поновлення прав суб'єктів даних експертами Робочої групи пропонується укладення додаткової окремої угоди між «експортером» даних і суб'єктом персональних даних під час одержання даних безпосередньо від суб'єкта та покладення на «експортера» даних відповідальності за можливі порушення прав суб'єкта подальшими одержувачами персональних даних. В цьому випадку суб'єкт персональних даних одержує від «експортера» даних відшкодування за можливі порушення одержувачем даних, а «експортер» даних, у свою чергу, може вимагати в подальшому відповідної компенсації за збитки від одержувача персональних даних [12, с. 121-122].

У пропозиціях, оприлюднених Європейською Комісією у 2012 році, щодо реформування законодавства у сфері захисту персональних даних містяться нововведення в контексті реформування діяльності Робочої групи. Так, відповідно до статті 64 проекту Загального регламенту із захисту даних пропонується створити *Європейську раду з захисту даних* у складі

керівників органів нагляду всіх держав-членів ЄС та Європейського уповноваженого із захисту даних. Європейська рада з захисту даних має на меті замінити собою Робочу групу. Статті 65 та 66 підкреслюють та уточнюють незалежність Європейської ради з захисту даних, а також визначають завдання Європейської ради з захисту даних на основі частини 1 статті 30 Директиви № 95/46/ЄС, додаткові елементи, що віддзеркалюють збільшення обсягу діяльності Європейської ради з захисту даних в межах ЄС та поза ним. Для забезпечення можливості реагування за критичних ситуацій стаття надає Європейській Комісії можливість звертатися з проханням про надання рекомендацій та правового висновку в певний строк [13].

Вищезазначені адміністративно-правові механізми ЄС у сфері захисту персональних даних діють на наднаціональному рівні. Разом з цим у кожній державі-члені ЄС існують відповідні національні інституційні механізми захисту персональних даних. Моделі відповідних інституційних механізмів є досить різними та залежать від того, до якої правової системи належить та чи інша держава.

Важливим для розуміння вимог ЄС щодо побудови дієвої інституційної системи захисту персональних даних *на національному рівні,* зокрема, забезпечення незалежності національного уповноваженого органу з питань захисту персональних даних, є вимоги статті 28 Директиви № 95/46/ЄС. Відповідно до статті 28 згаданої Директиви:

• Кожна держава-член передбачає, що один чи більше державних органів відповідають за моніторинг застосування в межах її території положень, прийнятих державами-членами відповідно до даної Директиви. Ці органи діють у повній незалежності при здійсненні функцій, якими вони наділені.

• Кожен державний орган, зокрема, має бути наділений:

– такими слідчими повноваженнями, як право доступу до даних, що є предметом операцій із обробки, і право збирати всю інформацію, необхідну для виконання його обов'язків із здійснення нагляду,

– ефективними повноваженнями на втручання, якот: надання висновків до здійснення операцій із обробки відповідно до статті 20 Директиви, і забезпечення відповідного опублікування таких висновків, видання розпоряджень про блокування, стирання чи знищення даних, накладення тимчасової чи остаточної заборони на обробку даних, попередження чи винесення догани контролеру даних, або повноваження звертатися до національних парламентів чи інших політичних інститутів,

– правом брати участь у судочинстві, якщо були порушені національні положення, прийняті відповідно до даної Директиви, чи довести ці порушення до відома судових органів.

• Рішення наглядового органу, що викликали скарги, можуть бути оскаржені в суді.

• Кожен наглядовий орган розглядає запити, зроблені будь-якою особою чи об'єднанням, що представляє інтереси цієї особи, про захист її прав і свобод під час обробки персональних даних. Особа, якої це стосується, повинна бути поінформована про результати розгляду запиту.

• Кожен наглядовий орган, зокрема, розглядає запити про перевірку законності обробки даних, зроблені будь-якою особою, у випадках, коли застосовуються національні положення, прийняті у відповідності до статті 13 даної Директиви. Така особа повинна в будь-якому випадку бути поінформована про те, що перевірка мала місце.

• Кожен наглядовий орган регулярно складає звіт про свою діяльність. Звіт повинен оприлюднюватись.

• Кожен наглядовий орган має право, незалежно від того, яке національне законодавство застосовується до відповідної обробки, виконувати на території власної держави-члена повноваження, якими він наділений. Кожен орган може отримати прохання про виконання його повноважень від органу іншої держави-члена.

• Наглядові органи співпрацюють один з одним у тій мірі, наскільки це необхідно для виконання їхніх обов'язків, зокрема, шляхом обміну всією корисною інформацією.

Держави-члени ЄС передбачають, що навіть після звільнення на посадових осіб і персонал наглядового органу поширюється обов'язок зберігати професійну таємницю відносно конфіденційної інформації, до якої вони мають доступ [3].

Досвід низки європейських держав свідчить про те, що національний уповноважений орган з питань захисту персональних даних – це державна структура, що підпорядковується парламенту та має спеціальні повноваження, які визначені саме парламентом, що здійснюють нагляд і контроль у сфері захисту персональних даних, несе відповідальність за вирішення питань щодо виконання вимог законодавства про захист персональних даних.

Висновки. Аналіз інституційно-правових механізмів захисту персональних даних в Європейському Союзі дозволяє зробити важливі висновки.

В Європейському Союзі склалась усталена система адміністративних, правозастосовних, наглядових та консультативних органів як на наднаціональному, так і на національному рівнях, які забезпечують дотримання прав на захист персональних даних в приватній та публічній сферах. Відмінна риса правового статусу вказаних органів – *незалежність* як основний принцип їх діяльності.

Центральне місце на наднаціональному рівні ЄС в цій системі посідає *Європейський уповноважений із захисту даних,* основним завданням якого є забез-

печення поваги до права на недоторканість приватного життя всіма органами та установами ЄС. Робоча група, утворена відповідно до статті 29 Директиви № 95/46/ЄС, з початку своєї роботи відгравала ключову в процесі гармонізації законодавства ЄС у сфері захисту персональних даних, у діяльності з приведення національних законодавств у цій сфері відповідно до стандартів Директиви № 95/46/ЄС. Зазначена Робоча група являє собою один з найбільш ефективних та сучасних консультаційних органів при Європейській Комісії.

Безумовно, ефективне виконання норм у сфері захисту персональних даних, закріплених Директивою № 95/46/ЄС, в європейському законодавстві було б неможливим без створення національних механізмів з надзору та захисту прав і законних інтересів фізичних осіб в державах-членах ЄС. У всіх державах ЄС на даний момент створені відповідні незалежні наглядові органи.

Глобальна реформа ЄС у сфері захисту персональних даних, що триває з 2010 року й понині, має на меті удосконалити існуючі прогалини у ефективній діяльності адміністративно-правового механізму у цій сфері. Так, планується ще більше посилити роль та незалежність наглядових органів як на наднаціональному, так і на національному рівнях ЄС, реформувати консультаційно-правовий механізм.

Аналіз та дослідження, проведені в цій статті, стануть в нагоді під час пошуку та обґрунтування оптимальної інституційної моделі захисту персональних даних як в Україні, так і в інших державах, які прагнуть вступити до Європейського Союзу.

Список використаної літератури

1. Договір про заснування Європейської Спільноти [Електронний ресурс]. – Режим доступу : http://zakon2.rada.gov.ua/laws/show/994_017/print1383746845020769.

2. Мервінський О.І., Козак В.Ф., Мельник К.С. Захист персональних даних: міжнародні стандарти : Збірник нормативно-правових документів. – К. : Видавництво Подоліна І.В., 2013.

3. Директива Європейського Парламенту і Ради № 95/46/ЄС про захист фізичних осіб при обробці персональних даних і про вільне переміщення таких даних [Електронний ресурс]. – Режим доступу : http://zakon.rada.gov.ua/laws/show/994_242.

4. Вельдер И.А. Система правовой защиты персональных данных в Европейском Союзе : дис. ... канд. юрид. наук : спец. 12.00.10. – Казань, 2006.

5. Різак М.В. Правовий статус уповноваженого органу з питань захисту персональних даних: досвід зарубіжних країн / М.В. Різак // Форум права. – 2012. – № 3. – С. 619–625.

6. Кашкин С.Ю. Право Европейского Союза / С.Ю. Кашкин. – М. : Проспект, 2005.

7. Капустин А.Я. Европейский Союз: интеграция и право / А.Я. Капустин. – М. : Издательство РУДН. – 2000.

8. Задорожний А.В., Пазюк А.В. Международное информационное право. – К., 2013.

9. Ищенко Е.А. Защита персональных данных в праве Европейского Союза / Е.А. Ищенко // Российское право в Интернете. – 2009. – № 1. – С. 23–31.

10. Recommendation 4/99 on the inclusion of the fundamental right to data protection in the European catalogue of fundamental rights adopted on 7 September 1999. – The Working Party on the Protection of Individuals with regard to the Processing of Personal Data. – Brussels, 1999. – [Електронний ресурс]. – Режим доступу : http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/1999/wp26_en.pdf.

11. Judging industry self-regulation: when does it make a meaningful contribution to the level of data protection in a third country? – Working Document. – Brussels : Data Protection Working Party, 1999. – [Електронний ресурс]. - Режим доступу : http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/1998/wp7_en.pdf.

12. Брижко В.М. Організаційно-правові питання захисту персональних даних : дис. … канд. юрид. наук : спец. 12.00.07 / В.М. Брижко. – К., 2004.

13. Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) [Електронний ресурс]. – Режим доступу : http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf.