

ПРАВОВЕ РЕГУЛЮВАННЯ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ В ЄВРОПЕЙСЬКОМУ СОЮЗІ

LEGAL REGULATION OF PERSONAL DATA PROTECTION WITHIN THE EUROPEAN UNION

Дяковський О.С., к.ю.н.,
докторант кафедри публічного права
Державний податковий університет

Кортукова Т.О., доктор філософії з міжнародного права,
доцент кафедри міжнародного, цивільного та комерційного права
Державний торговельно-економічний університет

У статті проаналізоване первинне та вторинне право Європейського Союзу у сфері захисту персональних даних. Визначено, що згідно з принципом передачі повноважень компетенція ЄС щодо захисту персональних даних визначена установчими договорами ЄС, а саме Договором про ЄС від 2007 року, Договором про функціонування ЄС від 2007 року та Хартією основних прав ЄС від 2000, яка з 2007 року була прирівняна до установчих договорів ЄС.

У 2016 році у ЄС було реформовано систему захисту персональних даних і було прийнято два нові законодавчі акти. На сьогодні, персональні дані захищаються Загальним регламентом захисту персональних даних 2016/679 та Директивою 2016/680 про захист персональних даних для поліції та органів кримінальної юстиції.

Серед нововведень у сфері захисту персональних даних фізичних осіб у ЄС, які були впроваджені Загальним регламентом захисту персональних даних 2016/679 були наступні: право отримувати чітку та зрозумілу інформацію про те, хто обробляє персональні дані, які дані обробляються та чому вони обробляються; право доступу до персональних даних, якими володіє суб'єкт даних про фізичну особу; право на забуття; суб'єкт даних у випадку крадіжки або втрати персональних даних повинен повідомити фізичну особу та відповідний орган нагляду за захистом даних, а у випадку невиконання цього положення суб'єкт даних може бути оштрафований; посилення захисту дітей в Інтернеті, тощо.

У статті також розмежовано відмінності між Загальним регламентом захисту персональних даних 2016/679 та Директивою 2016/680 про захист персональних даних для поліції та органів кримінальної юстиції. Відтак, для того, щоб Директива 2016/680 була застосовна, обробка персональних даних повинна здійснюватися компетентним органом з метою запобігання, розслідування, виявлення та переслідування кримінальних правопорушень або виконання кримінальних покарань, включаючи захист від загроз громадській безпеці і запобігання таким. Хоча на сьогодні все ще існує складність застосування компетентними органами двох різних правових режимів, що залежить від мети обробки персональних даних.

Ключові слова: захист персональних даних, Хартія основних прав ЄС, Регламент 2016/679, Директива 2016/680, право на забуття, правове регулювання, чутливі дані.

The article analyzes the primary and secondary law of the European Union in the field of personal data protection. It was determined that in accordance with the principle of transfer of powers, the competence of the EU regarding the protection of personal data is determined by the founding treaties of the EU, namely the Treaty on EU, 2007; the Treaty on the Functioning of the EU, 2007; and the EU Charter of Fundamental Rights of 2000, which since 2007 has been equated to founding treaties of the EU.

In 2016, the system of personal data protection was reformed in the EU and two new legislative acts were adopted. Currently, personal data is protected by the General Data Protection Regulation 2016/679 and Directive 2016/680 on the protection of personal data for the police and criminal justice authorities.

Among the innovations in the field of personal data protection of individuals in the EU, which were implemented by the General Data Protection Regulation 2016/679, were the following: the right to receive clear and understandable information about who processes personal data, what data is processed and why it is processed; the right of access to personal data held by the data subject about the person; the right to be forgotten; in case of theft or loss of personal data, the data subject must notify the natural person and the relevant data protection supervisory body, and in case of failure to comply with this provision, the data subject may be fined; strengthening the protection of children on the Internet, etc.

The article also delineates the differences between the General Data Protection Regulation 2016/679 and Directive 2016/680 on the protection of personal data for the police and criminal justice authorities. Therefore, in order for Directive 2016/680 to be applicable, the processing of personal data must be carried out by a competent authority for the purpose of preventing, investigating, detecting and prosecuting criminal offenses or carrying out criminal penalties, including the protection against and prevention of threats to public safety. Although today there is still the complexity of applying two different legal regimes by the competent authorities, which depends on the purpose of personal data processing.

Key words: personal data protection, EU Charter of Fundamental Rights, Regulation 2016/679, Directive 2016/680, right to be forgotten, legal regulation, sensitive data.

Постановка проблеми. Захист персональних даних в Європейському Союзі (далі – ЄС) є одним із ключових факторів дотримання прав людини. Оскільки порушення даного права може негативно впливати на суб'єкта персональних даних, належне збирання, зберігання, використання даних відіграє важливу роль [1, с. 38]. У світлі формування політики інформаційної безпеки та актуалізації питань гарантування конфіденційності особистого життя людини проблематика захисту персональних даних набуває неабиякого значення [2, с. 216]. Враховуючи євроінтеграційні прагнення України, закріплені на конституційному рівні, а також отримання Україною статусу кандидата на членство ЄС, досить важливим є аналіз та приведення у відповідність законодавства України до *acquis* ЄС, зокрема, у сфері захисту персональних даних.

Аналіз останніх досліджень. Аналіз правового регулювання персональних даних у ЄС знайшов своє відображення у чисельних наукових доробках вчених. Відтак, І. Сопілко [3, с. 75] вивчав міжнародно-правовий досвід захисту персональних даних. Проблематику відповідності законодавства України до законодавства ЄС у сфері захисту персональних даних досліджували М. Бем, І. Гордиський [4, с. 255], М. Різак [5, с. 72], О. Легка [6, с. 79] та інші. І. Брацук та І. Яворська аналізували практику суду ЄС щодо принципів захисту персональних даних в ЄС [7, с. 198]. Разом з тим, аналіз права на забуття, дослідження правового регулювання використання чутливих даних, особливості застосування вторинного законодавства ЄС у сфері захисту персональних даних вітчизняними та іноземними вченими не було достатньо досліджено.

Формулювання цілей статті. Метою дослідження є аналіз первинного та вторинного законодавства Європейського Союзу, а також практики Суду ЄС і доктринальних напрацювань у сфері правового регулювання захисту персональних даних у ЄС.

Виклад основного матеріалу. Правовою основою для захисту персональних даних в ЄС є положення первинного та вторинного законодавства ЄС. Враховуючи принцип передачі повноважень, згідно з яким, ЄС діє у межах повноважень, що надані йому установчими договорами ЄС, компетенція ЄС у сфері захисту персональних даних передбачена Договором про ЄС від 2007 року, Договором про функціонування ЄС від 2007 року та Хартією основних прав ЄС від 2000 року, яка з 2007 року була прирівняна до установчих договорів ЄС.

Слід зазначити, що хоча першочергово у ЄС захист прав людини не відносився до повноважень та завдань ЄС і був прерогативою Ради Європи, проте згодом, зокрема, згідно зі статтею 2 Договору про ЄС повага до прав людини, а відтак і право на захист персональних даних, вперше було визнано цінністю ЄС у 2007 році. Цінності об'єднують держави-члени ЄС, так як жодна держава, яка не визнала цінностей, не може належати до Союзу [8, с. 86].

Тому стандарти щодо захисту персональних даних у ЄС на сьогодні є уніфікованими.

Згідно зі статтею 16 Договору про функціонування ЄС фізичні особи мають захист під час обробки їхніх персональних даних установами, органами, службами та агентствами ЄС, а також державами-членами. Важливо відмітити, що коло осіб (*ratione personae*), на яких поширюється захист персональних даних у ЄС, згідно з формулюванням статті 16 Договору про функціонування ЄС не обмежується громадянством ЄС, а є універсальним правом, яке поширюється на усіх фізичних осіб.

У Хартії основних прав ЄС право на захист персональних даних закріплено у статті 8, що вказує на його основоположний характер. При цьому, у Хартії основних прав ЄС право на захист персональних даних має особливий характер і це право виділено в окрему статтю, що відрізняється від підходу закладеного Конвенцією про захист прав людини та основоположних свобод від 1950 року, згідно з якою захист персональних даних розглядається у контексті права на повагу до приватного і сімейного життя, а саме статті 8. Відтак, надаючи більшого значення праву на захист персональних даних, у Хартії основних прав ЄС розмежовуються статті щодо права на приватність (стаття 7) та права на захист персональних даних (стаття 8).

У межах вторинного законодавства, у 2016 році ЄС завершив довгоочікувані реформи захисту персональних даних і прийняв два нові законодавчі акти. На сьогодні, персональні дані захищаються Загальним регламентом захисту персональних даних 2016/679 та Директивою 2016/680 про захист персональних даних для поліції та органів кримінальної юстиції.

Відтак, правовим інструментом для уніфікації захисту персональних даних в усіх державах-членах ЄС, який посилив контроль за процесом збору, обробки і передавання персональних даних резидентів і громадян ЄС став Загальний регламент захисту персональних даних 2016/679, який має пряму дію та забезпечив однакове регулювання захисту персональних даних. Він спрямований на формування простору свободи, безпеки та справедливості, економічного союзу, підтримання добробуту громадян [9, с. 198].

Територіальна сфера дії (*ratione loci*) Загального регламенту захисту персональних даних 2016/679 виходить за межі ЄС, що спричиняє його екстериторіальний характер. Правила Загального регламенту захисту персональних даних 2016/679 застосовуються у випадках коли: контролер або оператор персональних даних знаходяться на

території ЄС, незалежно від місця обробки персональних даних; контролер або оператор персональних даних перебувають за межами території ЄС, а власники персональних даних (суб'єкти даних) перебувають на території ЄС: (а) при оплатному чи безоплатному постачанні товарів чи наданні послуг таким особам у межах ЄС або (б) при моніторингу поведінки власників персональних даних у межах ЄС; контролер або оператор персональних даних знаходяться за межами ЄС, але в місці, де застосовується законодавство держави-члена в силу публічного міжнародного права [10, с. 473].

Наприклад, у справі С-131/12 Суд ЄС постановив, що Google Spain є «осідком» компанії Google Inc., і що деякі з рекламних заходів, спрямовані на іспанську громадськість, здійснювалися в контексті діяльності іспанського «осідку», тому Google Inc. має відповідати законодавству ЄС [11]. Відтак, вільний потік інформації є важливим, але не настільки, як захист конфіденційності та персональних даних згідно з європейським режимом. Загальний регламент захисту персональних даних 2016/679 встановлює баланс між вільним потоком інформації та високий рівень захисту персональних даних.

Проте, навіть якщо компанія не має фізичної присутності в ЄС, Загальний регламент захисту персональних даних 2016/679 може застосовуватися. Наприклад, пропозиція громадянам ЄС товарів або послуг, навіть безкоштовних, може спричинити активізацію дії Загального регламенту захисту персональних даних 2016/679, якщо контролер або оператор планує пропонувати послуги суб'єктам даних в одній або кількох державах-членах Союзу. Тобто основна філософія полягає в тому, що коли організації поза межами ЄС свідомо обробляють персональні дані громадян ЄС, застосовуватиметься Загальний регламент захисту персональних даних 2016/679 [12].

Нововведеннями у сфері захисту персональних даних фізичних осіб у ЄС, які були закладені Загальним регламентом захисту персональних даних 2016/679 були наступні:

- право отримувати чітку та зрозумілу інформацію про те, хто обробляє персональні дані, які дані обробляються та чому вони обробляються (статті 12–14);
- право доступу до персональних даних, якими володіє суб'єкт даних про фізичну особу (стаття 15);
- право на забуття – фізична особа може вимагати видалення персональних даних, якщо вона не бажає їх подальшої обробки, а суб'єкт даних не має обґрунтованих причин зберегти їх (стаття 17);
- суб'єкт даних у випадку крадіжки або втрати персональних даних повинен повідомити фізичну особу та відповідний орган нагляду за захистом даних, а у випадку невиконання цього положення суб'єкт даних може бути оштрафований (статті 33 і 34);
- посилення захисту дітей в Інтернеті (стаття 8), тощо.

До того ж, Загальний регламент захисту персональних даних 2016/679 закріпив поняття спеціальної категорії персональних даних, а саме «чутливих даних», до яких належать персональні дані, що розкривають расове чи етнічне походження, політичні переконання, релігійні чи філософські переконання чи членство в профспілках, дані про стан здоров'я, дані щодо статевого життя чи сексуальної орієнтації фізичної особи, генетичні дані та обробка біометричних даних з метою ідентифікації фізичної особи. При цьому, Суд ЄС застосовує широке тлумачення «чутливих даних». Наприклад, коли хтось згадав на веб-сайті, що колега пошкодила ногу та працювала неповний робочий день за медичними показаннями, Суд ЄС у справі С-101/01 встановив, що це означало розголошення особистих даних щодо стану здоров'я [13].

З іншого боку, Загальний регламент захисту персональних даних 2016/679 встановлює ряд вимог, які застосовуються до суб'єктів даних, *inter alia*:

– Суб'єкти даних, які обробляють дані у великих масштабах або чиєю основною діяльністю є обробка спеціальної категорії персональних даних, наприклад, даних про здоров'я мають призначити особу, відповідальну за захист даних

– Суб'єктам даних доведеться проводити оцінку впливу, коли обробка даних може призвести до високого ризику для прав і свобод осіб.

– Пропонуються різні інструменти для передачі даних за межі ЄС, включаючи рішення щодо відповідності, прийняті Європейською комісією, коли країна, що не входить до ЄС, пропонує адекватний рівень захисту, попередньо схвалені (стандартні) договірні положення, обов'язкові корпоративні правила та кодекси поведінки [14].

На додаток до Загального регламенту захисту персональних даних 2016/679, реформи у сфері захисту персональних даних у ЄС також включали прийняття Директиви 2016/680 про захист персональних даних для поліції та органів кримінальної юстиції, яка регулює збір, обробку та зберігання персональної інформації в контексті поліцейської діяльності.

Оскільки інноваційні технології широко застосовуються правоохоронними органами для виявлення, розслідування та запобігання злочинам, негативний вплив порушень зберігання персональних даних може суттєво вплинути на безпеку громадян і діяльність поліції. Відтак, Директива 2016/680 про захист персональних даних для поліції та органів кримінальної юстиції вимагає від правоохоронних органів проводити оцінку впливу на захист даних, щоб проаналізувати можливі ризики.

Стаття 1 визначає сферу застосування Директиви 2016/680 про захист персональних даних для поліції та органів кримінальної юстиції, що є вирішальним для чіткого розмежування між Директивою та Загальним регламентом захисту персональних даних 2016/679. Для того, щоб Директива була застосовна, обробка персональних даних повинна здійснюватися компетентним органом з метою запобігання, розслідування, виявлення та переслідування кримінальних правопорушень або виконання кримінальних покарань, включаючи захист від загроз громадській безпеці і запобігання таким.

Щоразу, коли офіцер поліції обробляє дані для цілей, не пов'язаних із правоохоронними органами, і, як один із прикладів, кадрові дані або інформацію, яка підлягає архівації, застосовуватиметься Загальний регламент захисту персональних даних 2016/679.

Проте в деяких сферах, де правоохоронні органи мають право обробляти персональні дані, розмежування між Директивою 2016/680 про захист персональних даних для поліції та органів кримінальної юстиції та Загальним регламентом захисту персональних даних 2016/679 не є таким очевидним. Це може мати місце в ситуаціях, коли офіцери поліції обробляють персональні дані з метою ідентифікації або перевірки у сфері міграції та прикордонного контролю. Особа, яка незаконно перетинає кордони Шенгенського простору, може бути перевірена офіцерами поліції, і в тих державах-членах, де незаконний перетин кордонів кваліфікується як кримінальний злочин, офіцер поліції може змінити мету обробки персональних даних залежно від того, чи вона здійснюється для міграційних цілей або для кримінального переслідування. Однак, як

тільки нелегальний мігрант подає заяву про надання притулку, розгляд його заяви підпадає під дію Загального регламенту захисту персональних даних 2016/679, незважаючи на розпочате кримінальне провадження. Це демонструє складність застосування компетентними органами двох різних правових режимів залежно від мети обробки персональних даних [15].

Відтак, проблема захисту персональних даних, особливо, у кримінальних справах є надзвичайно релевантною. Неодноразово у контексті статті 8 Європейської конвенції про захист прав людини та основоположних свобод Європейський суд з прав людини виводив свої рішення. Як приклад, можна навести справу «S. та Марпер проти Сполученого Королівства». Зі змісту судового рішення вбачається, що заявники посилаючись на статтю 8 та статтю 14 Конвенції, скаржилися до Суду на те, що органи влади держави-відповідача продовжують зберігати їхні відбитки пальців, зразки клітин та профілі ДНК після того, як провадження за кримінальними справами стосовно них або завершилося винесенням виправдувального або закрито [16].

Під час розгляду даної справи національними судами заявників було вирішено відмовити у задоволенні позовних вимог про видалення відібраних персональних даних. Як наслідок Європейським судом з прав людини було встановлено порушення статті 8 Конвенції.

У свою чергу Директива 2016/680 про захист персональних даних для поліції та органів кримінальної юстиції не передбачає таких прав, які містяться в Загальному регламенті захисту персональних даних 2016/679, які в першу чергу були розроблені для здійснення комерційної діяльності, таких як право бути забутим або право на переносимість даних, що викликає також складність в реалізації норм вказаних двох джерел права у сфері персональних даних на практиці та утворює проблемні питання у даному напрямі.

Висновки. Таким чином, правове регулювання захисту персональних даних у Європейському Союзі має комплексний характер. Компетенція Європейського Союзу у сфері забезпечення права на захист персональних даних закріплена установчими договорами ЄС. При цьому, Хартия основних прав ЄС посилює захист цього права. У 2016 році у межах ЄС відбулась реформа захисту персональних даних, результатом якої стало прийняття та активізація Загального регламенту захисту персональних даних 2016/679 та Директиви 2016/680 про захист персональних даних для поліції та органів кримінальної юстиції. Хоча на сьогодні все ще існує складність застосування компетентними органами двох різних правових режимів, що залежить від мети обробки персональних даних та свідчить про необхідність внесення подальших змін в частині регулювання персональних даних для поліції та органів кримінальної юстиції до положень та прав котрі викладені в загальному регламенті з метою його подальшого функціонування та застосування за сферою дії.

Перспективи подальших досліджень. Збільшення чинників котрі впливають на збір, обробку, регулювання персональних даних та розширення прав суб'єктів персональних даних в Європейському Союзі свідчать про необхідність здійснення досліджень з урахуванням міжнародного вектора регулювання даної категорії прав.

ЛІТЕРАТУРА

1. Дяковський О.С. Правове регулювання захисту персональних даних в Європейському Союзі. *Актуальні питання розвитку науки та освіти*: матеріали VII міжнарод. Наук.–прак. конф. (Львів 9-10 січня 2023 р.). Львів, 2023. С. 38–39.
2. Правовий захист персональних даних: монографія / Т. О. Гуржій, А. Л. Петрицький. Київ: Київ. нац. торг.-екон. ун-т, 2019. 216 с.
3. Сопілко І. Міжнародно-правовий досвід захисту персональних даних. *Юридичний вісник*. 2014. № 4. С. 70–75.
4. Бем М., Городиський І. Відповідальність за порушення законодавства про захист персональних даних: проблеми відповідності законодавства України вимогам регламенту Європейського Союзу щодо захисту персональних даних (GDPR). *Право України*. 2019. № 2. С. 237–255.
5. Різак М. Практика країн Європейського Союзу та України у сфері судочинства щодо гарантування безпеки обігу та обробки персональних даних. *Підприємство, господарство і право*. 2017. № 7. С. 68–72.

6. Легка О. Актуальні питання захисту персональних даних: вітчизняний та міжнародний досвід. *Правова позиція*. 2021. № 2. С. 74–79.
7. Брацук І., Яворська І. Практика Суду ЄС щодо принципів захисту персональних даних в ЄС. *Вісник Львівського університету*. 2019. № 47. С. 192–198.
8. Кортюкова, Т. Особливості правового регулювання ЄС у сфері легальної міграції та інтеграції мігрантів. *Fundamental and applied researches in practice of leading scientific schools*. 2019. № 34 (4). С. 79–86.
9. Брацук І., Яворська І. Практика Суду Європейського Союзу щодо принципів захисту персональних даних в Європейському Союзі. *Вісник Львівського університету*. Серія «Міжнародні відносини». № 47. 2019. С. 192–198.
10. Берназ-Лукавецька О.М. Порівняльний аналіз правил GDPR з законодавством України щодо захисту персональних даних у соцмережах. *ВД «Гельветика»*. 2019, Т. 2. С. 471–473.
11. Case C-131/12, Google Spain, ECLI:EU:C:2014:317.
12. Hoofnagle, C. J., van der Sloot, B., & Zuiderveen Borgesius, F. (2019). The European Union General Data Protection Regulation: What It Is And What It Means. *Information & Communications Technology Law*. № 28. P. 65-98. <https://doi.org/10.1080/13600834.2019.1573501>, <https://doi.org/10.2139/ssrn.3254511>.
13. C-101/01 Bodil Lindqvist [2003] ECLI:EU:C:2003:596.
14. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) URL: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32016R0679>.
15. Sajfert, J., & Quintel, T.A. Data Protection Directive (EU) 2016/680 for Police and Criminal Justice Authorities. *SSRN Electronic Journal*. 2017.
16. S. та Марпер проти Сполученого Королівства URL: [https://hudoc.echr.coe.int/fre#{%22tabview%22:\[%22document%22\],%22itemid%22:\[%22001-117816%22\]}](https://hudoc.echr.coe.int/fre#{%22tabview%22:[%22document%22],%22itemid%22:[%22001-117816%22]}).