ISSN 2078–4333. Вісник Львівського університету. Серія міжнародні відносини. 2019. Випуск 47 С. 192–198
Visnyk of the Lviv University. Series International Relations. 2019. Issue 47. P. 192–198

УДК 340.134 (477+061.1 ЄС): 351.822.009.6
DOI 10.30970/vir.2019.47.0.10988

ПРАКТИКА СУДУ ЄВРОПЕЙСЬКОГО СОЮЗУ ЩОДО ПРИНЦИПІВ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ В ЄВРОПЕЙСЬКОМУ СОЮЗІ

Іван Брацук, Ірина Яворська

Львівський національний університет імені Івана Франка,
вул. Університетська, 1, м. Львів, Україна, 79000, тел. (032)239-41-99,
e-mail: irynayavorska@hotmail.com

У контексті приведення законодавства України у відповідність до права Європейського Союзу видається актуальним дослідження практики Суду ЄС та Європейського суду з прав людини у сфері захисту персональних даних. Досліджено окремі рішення Суду Європейського Союзу у сфері захисту персональних даних, зокрема, практику Суду Європейського Союзу щодо принципів захисту персональних даних у Європейському Союзі.

Діяльність Суду Європейського Союзу щодо захисту персональних даних реалізується у формі висновків, які Суд ЄС надає з приводу преюдиційних звернень національних судів на запити осіб з приводу законності опрацювання персональних даних, строків доступу осіб з приводу законності опрацювання персональних даних, строків доступу осіб до інформації, що належить до персональних даних, забезпечення належної безпеки зберігання персональних даних, заборони зібрання надмірної кількості інформації про особу, а також щодо правильності запровадження у національне законодавство забезпечення вимог щодо «повної незалежності» наглядових органів, відповідальних за забезпечення запиту персональних даних. Усі вони спрямовані на недопущення «порушення захисту персональних даних» – порушення безпеки, що спричиняє випадкове чи незаконне знищення, втрату, зміну, несанкціоноване розкриття або доступ до персональних даних, які передано, збережено або іншим чином опрацьовано. Також необхідно зазначити, що «персональні дані» стосуються не лише приватного життя особи, а можуть застосовуватися і до професійної чи громадської діяльності особи.

Ключові слова: персональні дані; Європейський Союз; принципи захисту персональних даних в рамках Європейського Союзу.

Регламент Європейського Парламенту та Ради ЄС щодо захисту персональних даних набрав чинності 25 травня 2018 року. Персональні дані визначаються Регламентом як інформація, що стосується фізичної особи, яку ідентифіковано. До моменту набрання ним чинності діяли й інші нормативні акти, спрямовані на забезпечення захисту персональних особи в рамках ЄС.

Сформувалась чимала практика Суду ЄС щодо захисту прав осіб у сфері персональних даних. Зокрема, ще у ст. 2 Глави 1 Директиви ЄС № 94/46/ЄС закріплено, що персональні дані означають будь-яку інформацію, що стосується встановленої фізичної особи чи фізичної особи, яку можна встановити. Особою, яку можна встановити, є така, яка може бути встановленою прямо чи непрямо, окремо, за допомогою ідентифікаційного коду або одного чи більше чинників, притаманних її фізичним, фізіологічним, розумовим, економічним, культурним чи соціальним аспектам.

Прийняття Регламенту ґрунтується, як зазначено у ньому, на положеннях Хартії ЄС про основні права та положеннях Договору про функціонування Європейського Союзу, якими закріплено право особи на захист своїх персональних даних. Регламент спрямовано на формування простору свободи, безпеки та справедливості, економічного союзу, підтримання добробуту громадян. Метою прийняття регламенту є: гармонізація захисту фундаментальних прав і свобод під час опрацювання даних; забезпечення вільного руху персональних даних між державами-членами.

Важливим видається дослідження практики Суду ЄС та Європейського суду з прав людини з огляду на необхідність гармонізації законодавства України з правом ЄС у зазначеній сфері. Стратегію кібербезпеки України прийнято 2016 року з метою забезпечення кібербезпеки України як стану захищеності життєво важливих інтересів людини і громадянина, суспільства та держави у кіберпросторі, що досягається комплексним застосуванням сукупності правових, організаційних, інформаційних заходів. Стратегія має базуватись у тому числі й на принципах: верховенства права і поваги до прав та свобод людини і громадянина; забезпечення національних інтересів України; відкритості, доступності, стабільності та захищеності кіберпростору; державно-приватного партнерства, широкої співпраці з громадянським суспільством у сфері забезпечення кібербезпеки та кіберзахисту; пропорційності та адекватності заходів кіберзахисту реальним та потенційним ризикам та ін.

Закон України «Про основні засади забезпечення кібербезпеки України» набув чинності 2018 р. Як зазначено у публікації колективу авторів, підготованої в рамках проекту «Громадської синергії», головною суттю поглибленої та всеосяжної зони вільної торгівлі є одностороннє регуляторне наближення в обмін на економічну інтеграцію.

Цифровий ринок охоплює положення УА щодо електронної торгівлі, телекомунікаційних послуг, ІТ послуг, аудіовізуальних медіа, авторських та суміжних прав, захисту персональних даних. Як зазначають дослідники, Україна останніми роками зробила низку кроків для нормативно-правового наближення, однак прогрес недостатній і не встигає за темпами оновлення законодавства ЄС. Фахівці констатують також відсутність в Україні окремого органу державної влади у сфері цифрової економіки. Також видається необхідним покращення сфери державного фінансування Концепції розвитку цифрової економіки. Уряд підготував проект Стратегії інтеграції України до Єдиного цифрового ринку ЄС до 2023 року.

Діяльність Суду Європейського Союзу щодо захисту персональних даних реалізується у формі висновків, які Суд ЄС надає з приводу преюдиційних звернень національних судів на запити осіб з приводу законності опрацювання персональних даних, строків доступу осіб з приводу законності опрацювання персональних даних, дотримання строків доступу осіб до інформації, що належить до персональних даних, забезпечення належної безпеки зберігання персональних даних, заборони зібрання надмірної кількості інформації про особу, а також щодо правильності запровадження у національне законодавство забезпечення вимог щодо «повної незалежності» наглядових органів, відповідальних за забезпечення запиту персональних даних. Усі вони спрямовані на недопущення «порушення захисту персональних даних» – порушення безпеки, що спричиняє випадкове чи незаконне знищення, втрату, зміну, несанкціоноване розкриття або доступ до персональних даних, які передано, збережено або іншим чином опрацьовано. Також необхідно зазначити, що «персональні дані» стосуються не лише приватного життя особи, а можуть застосовуватися і до професійної чи громадської діяльності особи. Наприклад, у справі «Аманн проти Швейцарії» Європейський суд з прав людини визначив термін «персональні дані» як такий, що не обмежується питаннями приватної сфери особи [4].

До категорії таких справ належать справи «Європейська комісія проти Німеччини», справа «Губер проти Німеччини», справа «Рейкебур» [3, с. 179], справа «Національна асоціація кредитних фінансових установ (ASNEF) і Федерація електронної комерції і прямого маркетингу (FECEMO) та інші.

Відповідно до ст. 5 Регламенту ЄС щодо захисту персональних даних, принципами опрацювання персональних даних є: законність, застосування правомірного і прозорого способів щодо суб'єкта даних; збір для чітких і законних цілей; опрацювання достатньої не надмірної кількості даних («принцип мінімізації даних»); принцип закріплення точних даних, максимально швидке оновлення неточних персональних даних, збереження у формі, що дозволяє ідентифікацію суб'єктів даних не довше, ніж це є необхідним для цілей їхнього опрацювання, триваліше зберігання дозволяється винятково для досягнення цілей суспільних інтересів, для наукового чи історичного дослідження або статистичних цілей відповідно до статті 89(1) за умов вжиття відповідних технічних, організаційних заходів, передбачених Регламентом для гарантування прав і свобод суб'єкта даних; опрацювання у спосіб, що забезпечує належне зберігання даних; забезпечення перерозподілу персональних даних.

Зазначені вище принципи обробки співпадають зі стандартами, виробленими в практиці Європейського суду з прав людини. Зокрема, у своїх рішеннях Європейський суд з прав людини неодноразово наголошував, що обробка інформації щодо приватного життя особи входить до сфери ст. 8 Конвенції про захист прав людини та основних свобод.

Отже, практика розгляду справ Судом Європейського Союзу у сфері захисту персональних даних ґрунтується на засадах дотримання принципів захисту

персональних даних, викладених у Регламенті ЄС щодо захисту персональних даних та з урахуванням вимог права Ради Європи у сфері захисту персональних даних. Наведемо до прикладу кілька справ Суду ЄС, які торкаються питань принципів захисту персональних даних.

У справі «Бірюк проти Литви» заявниця вимагала від щоденної газети відшкодування збитків за публікацію у статті інформації про те, що вона було ВІЛ-позитивною. Цю інформацію нібито підтверджували лікарі місцевої лікарні. ЄСПЛ не вважає цю статтю такою, яка сприяє будь-яким публічним дискусіям, і підтвердив, що захист персональних даних, медичних зокрема, має принципове значення для задоволення прав особи на повагу до її приватного і сімейного життя, які гарантовані ст. 8 ЄКПЛ. Суд надає особливого значення тому факту, що, згідно з повідомленням у газеті, медичний персонал лікарні надав інформацію про ВІЛ-інфіковану заявницю, відкрито порушуючи обов'язок зберігати лікарську таємницю. Отже, держава не забезпечила право заявниці на повагу до її приватного життя. Суд дійшов висновку, що було порушено ст. 8.

Прикладом захисту Судом ЄС принципу законності щодо захисту персональних даних є його практика у справі «Фолькер і Маркус Шеке» і «Хартмут Айферт проти землі Гессен». Наступним важливим принципом у сфері захисту персональних даних також є принцип надання згоди на оприлюднення таких даних, ілюстрований у справі С-543/09 «Компанія «Deutsche Telekom».

Принцип законності обробки нечутливих персональних даних викладено у главі II «Загальні правила законності обробки персональних даних» Директиви 95/46, якою передбачено, що з урахуванням визначених ст. 13 винятків увесь процес обробки персональних даних повинен відповідати, насамперед, принципам якості персональних даних, викладеним у статті 6 Директиви про захист персональних даних і, по-друге, одному із критеріїв законності обробки персональних даних, передбачених ст. 7.130 (СЄС, об'єднані справи С-465/00, С-138/01 та С-139/01, «Рахункова палата проти австрійської телерадіокомпанії «Österreichischer Rundfunk» та інших і Нойком та Лауерманн проти австрійської телерадіокомпанії «Österreichischer Rundfunk» (Rechnungshof v. Osterreichischer Rundfunkand Others and Neukomm and Lauermann v. Osterreichischer Rundfunk) від 20 травня 2003 р., п. 65; СЄС, С-524/06, «Губер проти Німеччини» (Huber v. Germany) від 16 грудня 2008 р., п. 48; СЄС, об'єднані справи С-468/10 та С-469/10, «Національна асоціація кредитних фінансових установ (ASNEF) та Федерація електронної комерції і прямого маркетингу (FECEMD) проти Державної адміністрації» (Asociacion Nacional de Establecimientos Financieros de Credito (ASNEF) and Federacion de Comercio Electronico y Marketing Directo (FECEMD) v. Administracion del Estado) від 24 листопада 2011 р., п. 26.) [3, с. 88].

У справі «Губер проти Німеччини» [3, с. 133] громадянин Австрії, що проживає у Німеччині, звернувся до Федерального відомства з питань міграції та біженців з проханням видалити його дані з Центрального реєстру іноземців (AZR). Цей реєстр, у якому містяться персональні дані громадян держав-членів

ЄС, що проживають у Німеччині більше трьох місяців і не є її громадянами, використовують для цілей статистики, а також для цілей діяльності правоохоронних та судових органів під час розслідування та обвинувачення у злочинній діяльності або тій, яка загрожує громадській безпеці. Суд звернувся за роз'ясненням, чи відповідає здійснювана процедура обробки персональних даних у такому реєстрі, як Центральний реєстр іноземців, до якого також мають доступ інші державні органи, праву ЄС, враховуючи, що для громадян Німеччини такого реєстру немає. СЄС постановив, по-перше, що відповідно до статті 7(e) Директиви, персональні дані можуть законно обробляти тільки за умови, якщо це необхідно для виконання завдання, здійснюваного в суспільних інтересах чи при виконанні офіційних повноважень. На думку Суду, «враховуючи ціль забезпечення однакового захисту у всіх державах-членах, передбачене у статті 7(e) Директиви 95/46 поняття необхідності не може бути різним у державах-членах. Отож те, що ми розглядаємо – це поняття, яке має своє незалежне значення у праві Співтовариств і яке треба тлумачити у спосіб, який повністю відображає закладену в статті 1(1) ціль цієї Директиви. Суд зазначає, що здійснення права громадянина держави-члена ЄС щодо вільного пересування територією держави-члена, громадянином якої він чи вона не є, не є абсолютним і може бути предметом обмежень і умов, встановлених Договором та прийнятими на його виконання заходами. Отже, якщо у держави-члена є законні підстави для використання такого реєстру як AZR для допомоги органам, що відповідають за застосування законодавства про право на проживання, у такому реєстрі не повинно бути іншої інформації, окрім тієї, яка необхідна для досягнення цієї конкретної мети. Суд доходить висновку, що така система обробки персональних даних відповідає праву ЄС за умови, що містить тільки дані, які необхідні для використання такого закону, а централізований характер системи сприяє ефективнішому його застосуванню. Національний суд має встановити, чи є ці умови задовільними в даному конкретному випадку. Якщо ні, то збереження і обробку персональних даних у такому реєстрі, як AZR для статистичних цілей, не можна, за будь-яких підстав, вважати необхідними у розумінні статті 7(e) Директиви 95/46 /ЕС. Нарешті, стосовно питання використання даних реєстру для цілей боротьби зі злочинністю, Суд вважає, що до таких цілей «обов'язково включено мету щодо переслідування за скоєння злочинів та правопорушень, що не залежить від громадянства того, хто їх скоїв». У цьому реєстрі немає персональних даних про громадян цієї держави-члена, і це розходження у поводженні є дискримінацією, заборону якої передбачено ст. 18 ДФЄС. Отож тлумаченні Суду це положення «виключає створення державою-членом для цілей боротьби зі злочинністю системи обробки персональних даних для громадян держав-членів ЄС, які не є громадянами цієї держави-члена» [3, с. 133–136].

Висновки. Отже, персональними даними є будь-які відомості про особу, на основі яких її можна ідентифікувати. До набрання чинності Регламентом існувало безліч актів, які регулювали окремі аспекти захисту персональних даних особи. Сам Регламент прийнято на основі та з урахуванням зазначених

актів та положень Хартії Європейського Союз про основні права. Діяльність Суду Європейського Союзу щодо захисту персональних даних реалізується у формі висновків, які Суд ЄС надає з приводу преюдиційних звернень національних судів на запити осіб з приводу законності опрацювання персональних даних, дотримання строків доступу осіб до інформації, що належить до персональних даних, забезпечення належної безпеки зберігання персональних даних, заборони зібрання надмірної кількості інформації про особу. Інформація, що підпадає під визначення «персональні дані», стосується не лише приватного життя особи, а може стосуватися і професійної чи громадської діяльності особи.

Рішення Суду ЄС спрямовані на недопущення випадкового чи незаконного знищення, втрати, зміни, несанкціонованого розкриття або доступу до персональних даних, які передано, збережено або іншим чином опрацьовано.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Закон України «Про основні засади забезпечення кібербезпеки в Україні» // Голос України від 09.11.2017 р. № 208.

2. Інтеграція у рамках асоціації: динаміка виконання Угоди між Україною і ЄС. Аналітичний звіт. – Київ, 2019 р. [Електронний ресурс]. – Режим доступу : https://www.civic-synergy.org.ua/wp-content/uploads/2018/04/Integratsiya-u-ramkah-asotsiatsiyi-dynamika-vykonannya-Ugody-mizh-Ukrayinoyu-i-YES_ua.pdf.

3. Посібник з європейського права у сфері захисту персональних даних. – Київ : К.І.С., 2015. – 216 с.

4. Рішення Європейского суду з прав людини у справі «Аманн про Швейцарії» [Електронний ресурс]. – Режим доступу : http://eurocourt.in.ua/Article.asp?AIdx=308.

5. Стратегія кібербезпеки України // Урядовий кур'єр від 18.03.2016 р. № 52.

6. *Яворська І. М.* Захист персональних даних у праві Європейського Союзу / Яворська І. М., Микієвич М. М. // Вісник Львівського національного університету. – Серія «Міжнароні відносини». – 2019.

Стаття надійшла до редколегії 30.08.2019
Прийнята до друку 10.09.2019

BEST PRACTICE OF THE COURT OF THE EU IN ENSURING THE PRINCIPLES OF THE PERSONAL DATA PROTECTION

Ivan Bratsuk, Iryna Yavorska

Ivan Franko National University of Lviv,
1, Universytetska Str., Lviv, Ukraine, 79000, tel. (032)239-41-99,
e-mail: irynayavorska@hotmail.com

Research of the decisions of the European Court of Justice and of the European Court of Human Right is crucial in the process of approximation of Ukrainian legislation to the EU Law. This article subjects to analysis certain decisions of the Court of Justice of the EU in the area of Personal Data Protection, in particular, the main principles of protection.

Court of Justice of the EU forms its decisions on Personal Data Protection in the format of conclusions, provided by the Court in response to the pre-judicial requests from national courts in relation to enquiries from citizens on legality of processing of their personal data, on terms of response to such enquiries, on terms of access by citizens to information which is considered Personal Data, on ensuring

security of keeping Personal Data, on restrictions in collecting data, on the provisions in the national law on independence of bodies responsible for collecting and storing personal data.

These conclusions of the Court of Justice of the EU aim to prevent violations of the protection of personal data or of its security, which could lead to accidental or illegal destruction, loss, change, unauthorised access to data. It should be noted that the term Personal Data covers not only the private sphere of citizens but also their professional or civic activity.

Key words: personal data; EU; Court of Justice of the EU; EU principles of Personal Data Protection.