УДК 341.4

ПРАВОВА РЕГЛАМЕНТАЦІЯ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ У ДІЯЛЬНОСТІ ЄВРОПОЛУ

LEGAL REGULATION OF PERSONAL DATA PROTECTION IN THE ACTIVITIES OF EUROPOL

Хаврат М.С.,
аспірант кафедри міжнародного і європейського права
юридичного факультету
Харківського національного університету імені В.Н. Каразіна

У статті проаналізовано положення установчого акта Європолу щодо забезпечення захисту персональних даних; приділено увагу заходам забезпечення інформаційної безпеки; акцентовано увагу на існуючій проблематиці в цій сфері.
Ключові слова: заходи захисту, інформаційна безпека, міжнародна міжурядова організація, персональні дані, права людини.

В статье проанализированы положения учредительного акта Европола, касающиеся защиты персональных данных; уделено внимание мерам обеспечения информационной безопасности; акцентировано внимание на существующей проблематике в этой сфере.
Ключевые слова: меры защиты, информационная безопасность, международная межправительственная организация, персональные данные, права человека.

In this article it was analyzed the provisions of the constituent act of Europol for the protection of personal data; it was paid attention to information security measures; it was focused on the existing problems in this area.
Key words: protection measures, information security, international intergovernmental organization, personal data, human rights.

Постановка проблеми. Необхідність забезпечення належного рівня захисту персональних даних відіграє важливу роль у сучасному цифровому світі. Інформація дедалі частіше обробляється з використанням автоматизованих систем, що, у свою чергу, може мати наслідком можливість стороннього незаконного втручання до таких систем із метою заволодіння персональними даними, їх зміни або пошкодження. Збір та обробка даних є невід'ємними складовими діяльності більшості міжнародних міжурядових організацій, зокрема й Європейського поліцейського відомства (далі – Європол). З огляду на мету діяльності Європолу, яка полягає у наданні допомоги, спрямованої на запобігання та розслідування організованої злочинності, тероризму та інших тяжких злочинів, застосування найвищих стандартів захисту даних є обов'язковою умовою його належного функціонування.

Вищеозначене свідчить про актуальність обраної теми дослідження та її значимість для захисту прав людини, зокрема права на недоторканність приватного життя, оскільки високий рівень забезпечення інформаційної безпеки є невід'ємною частиною ефективного функціонування Європолу та дотримання прав осіб, персональні дані яких перебувають у його розпорядженні.

Стан опрацювання. Проблема забезпечення захисту персональних даних у діяльності Європолу досі залишалася поза межами наукових досліджень в українській науці міжнародного права. Наприклад, дослідженням окремих аспектів інформаційної безпеки в різний час займалися Я. Броунлі, М.В. Буроменський, О.О. Грицун, І.М. Забара, А.О. Кориневич, О.О. Мережко, А.В. Пазюк, Т.Л. Сироїд, Л.О. Фоміна та інші вчені. Однак ця тематика потребує подальшого детального дослідження.

Мета статті полягає у проведенні аналізу положень установчого акта Європолу щодо забезпечення захисту персональних даних, що перебувають у його розпорядженні.

Для досягнення мети поставлено такі **завдання:** дослідити положення установчого акта Європолу щодо забезпечення захисту персональних даних; проаналізувати заходи захисту персональних даних.

Виклад основного матеріалу. Діяльність Європолу, який функціонує з метою підтримання та зміцнення дій компетентних органів держав-членів та їх взаємного співробітництва в запобіганні та протидії серйозним злочинам, тероризму та іншим формам злочинності, що зачіпають загальний інтерес, безпосередньо пов'язана з опрацюванням персональної інформації. З цією метою в межах Європолу було створено інформаційну систему (далі – ІСЄ), яка являє собою центральну базу даних для обміну державами-членами розвідувальними даними та інформацією. ІСЄ містить інформацію про серйозні міжнародні злочини, підозрюваних і засуджених, злочинні структури та злочини й засоби, які використовуються для їх скоєння. ІСЄ може використовуватися для надання доступу до даних, що стосуються осіб, які є підозрюваними або яких було засуджено за скоєння кримінального правопорушення, що належить до компетенції Європолу; або осіб, факти щодо яких вказують на те, що вони готуються скоїти такі правопорушення [1, с. 166].

Однак функціонування такої системи вимагає застосування сучасних та ефективних заходів, спрямованих на запобігання та недопущення несанкціонованого доступу до неї. Наприклад, задля належного опрацювання персональних даних, які перебувають у розпорядженні Європолу, Регламентом (ЕС) 2016/794 було закріплено низку положень, якими врегульовано порядок збору, зберігання та використання таких відомостей. Зокрема, Регламентом (ЕС) 2016/794 визначено загальні принципи обробки персональних даних, серед яких – справедливість і законність, дотримання цільового призначення тощо (ст. 28). З метою захисту інформації передбачено проведення оцінювання надійності джерела інформації (ст. 29) [2].

Вищеозначеним Регламентом закріплено особливості опрацювання спеціальних категорій персональних даних, зокрема таких, що стосуються жертв і свідків злочинів, осіб, які не досягли 18 років, та інших. Обробка таких даних допускається у разі гострої потреби для запобігання або боротьби зі злочинністю, яка належить до завдань Європолу. Крім того, Регламентом передбачено заборону обробки персональних даних автоматизованими або іншими засобами, що містять інформацію про расове або етнічне походження, політичні погляди, релігійні або філософські переконання, членство у профспілках, а також обробку генетичних даних або даних, що стосуються здоров'я чи статевого життя людини, за винятком гострої потреби щодо запобігання або боротьби зі злочинністю, яка належить до завдань Європолу. Вибір конкретної групи осіб виключно на основі таких персональних даних забороняється. Правом доступу до такої інформації наділено лише обмежене число осіб, які визначаються виконавчим директором для

виконання їхніх завдань. Особисті дані, які перебувають у розпорядженні Європолу, не повинні передаватися державам-членам, союзним органам, третім державам або міжнародним організаціям, за винятком певних умов (ст. 30).

Наприклад, з огляду на ту обставину, що в розпорядженні Європолу перебуває значний масив інформації, зокрема чутливої, існує об'єктивна необхідність у здійсненні технічних та організаційних заходів із метою їх захисту від випадкового або незаконного знищення, втрати, несанкціонованого розкриття, зміни або доступу. Такі заходи мають бути спрямовані на контроль доступу до обладнання, яке використовується з метою опрацювання персональних даних; управління носіями даних (запобігання або недопущення несанкціонованого зчитування, копіювання, зміни, видалення); запобігання несанкціонованому вводу даних, їх модифікації; запобігання використанню автоматизованих систем обробки даних неавторизованими особами; забезпечення того, щоб уповноважені особи мали доступ тільки до тих даних, що охоплюються їхніми повноваженнями на доступ (контроль доступу до даних); забезпечення несанкціонованого зчитування, копіювання, зміни або видалення персональних даних під час передачі персональних даних або під час транспортування носіїв даних; створення умов для можливості невідкладного відновлення системи, яка використовується для зберігання інформації тощо (ст. 32) [2].

З метою захисту таких персональних даних також встановлено строки їх зберігання. За загальним правилом, інформація має зберігатися доти, доки це є необхідним для цілей, для яких вона обробляється. Однак у будь-якому разі Європол розглядає питання необхідності подовження зберігання таких відомостей не пізніше ніж через три роки після їх первинної обробки. У разі прийняття рішення про продовження строку зберігання даних мають бути зазначені обґрунтовані підстави. Якщо таке рішення не було прийнято, дані мають бути стерті автоматично через три роки. Особисті дані не стираються у тих випадках, коли це може завдати шкоди інтересам суб'єкта даних, який потребує захисту (у таких випадках дані повинні використовуватися тільки з явної та письмової згоди суб'єкта даних); їхня точність заперечується суб'єктом даних протягом періоду, що дає змогу державам-членам або Європолу перевіряти точність даних; вони повинні бути збережені як докази або для встановлення, реалізації чи захисту законних вимог; суб'єкт даних виступає проти їх стирання та замість цього вимагає обмеження їх використання (ст. 31).

У тому разі, якщо відбулося порушення цілісності персональних даних, Європол має повідомити Європейського інспектора із захисту даних, компетентні органи зацікавлених держав-членів, а також постачальника таких даних про це порушення без невиправданої затримки. Таке повідомлення має містити опис щодо характеру порушення персональних даних; категорій і кількості суб'єктів даних; опис ймовірних наслідків порушення; опис заходів, запропонованих або прийнятих Європолом для усунення порушень; рекомендації щодо пом'якшення можливих несприятливих наслідків унаслідок порушення особистих даних.

Інформація про будь-які порушення особистих даних, включно з фактами, які пов'язані з порушенням, наслідками та вжитими заходами щодо виправлення становища, має бути задокументована (ст. 34).

У тому разі, коли порушення особистих даних може мати серйозний і несприятливий вплив на права та свободи суб'єкта даних, Європол повинен повідомити таку особу про існуюче порушення без невиправданої затримки. Повідомлення має описувати характер порушення, містити необхідні рекомендації та контакті відомості співробітника з питань захисту даних. Якщо контактна інформація суб'єкта даних відсутня, Європол має направити запит провайдеру щодо повідомлення відповідного суб'єкта. Повідомлення суб'єкта про порушення персональних даних не вимагається, якщо Європол застосував необхідні заходи технологічного захисту, що роблять дані незрозумілими для будь-якої особи, яка не має доступу до них; вжив подальших заходів, які гарантують, що права та свободи суб'єкта даних більше не будуть піддані серйозному негативному впливу; або якщо таке повідомлення буде пов'язано з непропорційними зусиллями, зокрема, через число справ. У такому разі має бути здійснено публічне повідомлення або аналогічний захід (ст. 35).

Регламентом також закріплено право суб'єкта даних отримувати інформацію про те, чи обробляються його / її персональні дані. За таких обставин особа, яка бажає скористатися правом доступу до персональних даних, які її стосуються, може звернутися з відповідним проханням до компетентного органу держави-члена, який направляє відповідний запит Європолу. Надання інформації на запит може бути обмежено задля того, щоб дозволити Європолу виконувати свої завдання належним чином; забезпечити дотримання безпеки та суспільного порядку або запобігання скоєнню злочину; гарантувати, що будь-яке національне розслідування не буде поставлено під загрозу або з метою захисту прав і свобод третіх осіб (ст. 36). Суб'єкт даних має бути повідомлений у письмові формі про таку відмову, її причини, а також про право подати скаргу Європейському інспектору із захисту даних (ст. 36). У разі отримання скарги Європейський інспектор із захисту даних здійснює консультації з відповідними національними наглядовими органами держав-членів та бере до уваги їхню думку під час прийняття рішення (ст. ст. 47 92).

Регламентом також гарантується право суб'єкта даних на виправлення та стирання. У разі надходження такого запиту Європол має проінформувати особу про вчинені дії в письмовій формі протягом трьох місяців. Якщо було прийнято рішення про відмову у стиранні чи виправленні інформації, мають бути зазначені причини такої відмови та вказано щодо права особи на звернення зі скаргою до Європейського інспектора із захисту даних (ст. 37). У такому разі Європейський інспектор консультується з національними наглядовими органами держави-члена, які надали дані, та бере до уваги думку такого органу під час ухвалення свого рішення (ст. 47).

З метою перевірки законності опрацювання персональних даних, самоконтролю й забезпечення належної цілісності та безпеки даних Європол здійснює облік збору, зміни, доступу, розкриття, об'єднання або стирання персональних даних. Такі журнали або документація видаляються через три роки, якщо тільки дані, які вони містили, не потрібні для подальшого контролю. Внесення змін до таких журналів не допускається (ст. 40).

У межах Європолу також призначається співробітник із питань захисту даних, який є членом персоналу. Співробітник обирається на основі особистих і професійних якостей й, зокрема, експертних знань у сфері захисту даних. Строк повноважень становить 4 роки з правом повторного обрання. Під час виконання покладених обов'язків співробітник має діяти незалежно. З обійманої посади така особа може бути звільнена Правлінням лише за згодою Інспектора, якщо така особа більше не задовольняє вимоги, які до неї висуваються. До повноважень співробітника входять такі: забезпечення збереження запису про передачу й отримання персональних даних; забезпечення інформування суб'єктів даних про їхні права; проведення консультацій щодо обробки даних; співробітництво з Європейським інспектором із захисту даних; підготовка щорічного звіту й представлення його Правлінню та Європейському інспектору із захисту даних; ведення реєстру порушень обробки персональних даних тощо. Під час виконання своїх завдань співробітник із захисту даних повинен мати доступ до всіх даних, які опрацьовуються Європолом. У тому разі, коли співробітник вважає, що

опрацювання персональних даних було здійснено з порушеннями, він повідомляє про це виконавчого директора Європолу та просить його вирішити означену проблему протягом визначеного строку (ст. 41).

Крім того, кожна держава-член призначає національний наглядовий орган, який має контролювати відповідно до свого національного законодавства допустимість передачі персональних даних до Європолу. Такий орган здійснює нагляд за діяльністю національних підрозділів. Будь-яка особа має право просити національний наглядовий орган перевірити законність передачі даних Європолу, які стосуються такої особи. Таке право реалізується згідно з національним законодавством держави-члена, у якому здійснюється запит (ст. 42).

Регламентом передбачено положення щодо здійснення нагляду з боку Європейського інспектора із захисту даних. Наприклад, Інспектор несе відповідальність за моніторинг і забезпечення застосування положень Регламенту, що стосуються захисту основних прав і свобод фізичних осіб щодо обробки персональних даних у межах Європолу. Задля досягнення означеної мети Інспектор здійснює такі функції: заслуховує та розслідує скарги й інформує суб'єкта даних про результати розгляду; веде розслідування (за власною ініціативою або на підставі скарги) й інформує суб'єкта даних про підсумки; консультує Європол в усіх питаннях, що стосуються опрацювання персональних даних; веде реєстр нових видів операцій з обробки; проводить попередні консультації щодо опрацювання тощо. Крім того, Інспектор може доручити Європолу здійснити виправлення, обмеження, стирання або знищення персональних даних, які були оброблені з порушенням, і повідомити про такі дії третіх осіб, яким були розкриті дані; накласти тимчасову або остаточну заборону на обробку Європолом операцій, які порушують положення, що регулюють обробку персональних даних, тощо. За підсумками своєї роботи Інспектор, консультуючись із національними наглядовими органами, готує щорічний звіт, який повинен містити статистичну інформацію про скарги, розслідування, передачу персональних даних третім державам і міжнародним організаціям, випадки попередніх консультацій тощо (ст. 43) [2].

Варто також акцентувати увагу на тому, що з метою здійснення консультативних функцій Регламентом передбачено створення Ради зі співробітництва, до складу якої входять представники національних наглядових органів кожної держави-члена та Європейський інспектор із захисту даних. Рада здійснює обговорення загальної політики та стратегії нагляду за захистом даних Європолу; вивчає загальні проблеми, пов'язані зі здійсненням незалежного нагляду та реалізацією прав суб'єктів даних тощо. Рада зі співробітництва може приймати висновки, рекомендації та передову практику (ст. 45).

Висновки. Отже, зважаючи на означене, доходимо висновку, що забезпечення незалежної та ефективної діяльності Європолу вимагає застосування необхідних заходів інформаційної безпеки. Наприклад, Регламентом (ЕС) 2016/794 закріплено низку положень щодо загальних принципів опрацювання інформації, прав суб'єктів даних, особливостей опрацювання спеціальних категорій персональних даних і заходів захисту інформації.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. Посібник з європейського права у сфері захисту персональних даних. К.: K.I.C., 2015. 216 с. URL: https://rm.coe.int/168044e84e.
2. Regulation (EU) 2016/794 of the European Parliament and of the Council of 11 May 2016 on the European Union Agency for Law Enforcement Cooperation (Europol) and replacing and repealing Council Decisions 2009/371/JHA, 2009/934/JHA, 2009/935/JHA, 2009/936/JHA and 2009/968/JHA. URL: file:///C:/Users/Asus/Downloads/celex_32016r0794_en_txt%20(1).pdf.