МІЖНАРОДНЕ ПРАВО. ПОРІВНЯЛЬНЕ ПРАВОЗНАВСТВО

УДК 340
DOI https://doi.org/10.32782/2521-6473.2023-4.7

О. В. Легка, доктор юридичних наук,
професор, кафедри міжнародного права
Університету митної справи та фінансів

ЗАСТОСУВАННЯ ПРАКТИКИ ЄСПЛ ПРИ ЗАБЕЗПЕЧЕННІ ПРАВА НА ЗАХИСТ ІНФОРМАЦІЇ

Статтю присвячено дослідженню міжнародного досвіду та практики ЄСПЛ щодо захисту порушених прав людини у контексті захисту персональних даних. Здійснено аналіз ключових міжнародних нормативно-правових актів, які регламентують діяльність у даному напрямі. Констатовано, що вони спрямовані на гарантування як стабільності правовідносин шляхом забезпечення надійного балансу між правом людини на конфіденційність особистого життя, так і суспільними інтересами в інформаційній сфері. З'ясовано, що на сьогодні на міжнародному рівні досягнуто певної узгодженості щодо основоположних принципів та стандартів захисту інформації і відповідних основних процесуальних гарантій, які необхідно включити до національних законодавств. Проаналізовано ст. 52 Хартії Європейського Союзу про основоположні права щодо обмежень у частині щодо забезпечення гарантованих прав і свобод, а також основні міжнародні принципи та стандарти у контексті забезпечення права на захист інформації. Розглянуто рішення Європейського суду з прав людини у справах «Volker und Markus Schecke GbR та Хартмут Ейферт проти землі Гессен», «Заїченко проти України» (№ 2), «Ельсхольц проти Німеччини», «Кемпбелл проти Сполученого Королівства», «Леандер проти Швеції», «І проти Фінляндії» та рішення Європейського Суду «Гугл проти Маріо Костехі Гонсалеса». Проаналізовано Рекомендації Уповноваженого Верховної Ради України з прав людини щодо забезпечення захисту персональних даних під час укладення Україною міжнародних договорів, які передбачають транскордонний обмін даними. Теоретично обґрунтовано необхідність: удосконалення вітчизняного законодавства у частині, що стосується транскордонного обміну даними; доопрацювання окремих норм Закону України «Про державну реєстрацію геномної інформації людини» щодо дотримання права на захист інформації. Зроблено висновок, що практика ЄСПЛ у даному напрямі йде шляхом пріоритетності права на захист інформації над потенційним інтересом суб'єкта господарювання, котрому така інформація потрібна з метою надання послуг, що свідчить про доцільність врахування практики ЄСПЛ для закріплення її в нормативній площині України.

Ключові слова: *міжнародний досвід, законодавство, практика ЄСПЛ, право на захист інформації, GDPR.*

O. V. Lehka. Application of the practice of the EUHR in security rights to protection of information

The article is devoted to the study of the international experience and practice of the EUHR regarding the protection of violated human rights in the context of personal data protection. An analysis of key international legal acts regulating activities in this direction was carried out. It was established that they are aimed at guaranteeing both the stability of legal relations by ensuring a reliable balance between a person's right to privacy of personal life and public interests in the information sphere. It has been found that today at the international level, a certain agreement has been reached regarding the fundamental principles and standards of information protection and the relevant basic procedural guarantees, which must be included in national legislation. Article was analyzed. 52 of the Charter of the European Union on fundamental rights regarding restrictions in terms of ensuring guaranteed rights and freedoms, as well as basic international principles and standards in the context of ensuring the right to information protection. The decision of the European Court of Human Rights was considered in the cases "Volker und Markus Schecke GbR and Hartmut Eifert v. Land of Hesse", "Zaichenko v. Ukraine" (No. 2), "Elsholz v. Germany", "Campbell v. United Kingdom", "Leander v. Sweden", "And against Finland" and the decision of the European Court "Google against Mario Costehi Gonzalez". The Recommendations of the Commissioner for Human Rights of the Verkhovna Rada of Ukraine on ensuring the protection of personal data during Ukraine's conclusion of international agreements, which provide for cross-border data exchange, have been analyzed. The need for: improvement of domestic legislation in the part related to cross-border data exchange is theoretically substantiated; finalization of certain norms of the Law of Ukraine "On State Registration of Human Genomic Information" regarding compliance with the right to information protection. It was concluded that the practice of the EUHR in this direction follows the path of prioritizing the right to protect information over the potential interest of the economic entity, which needs such information for the purpose of providing services, which indicates the expediency of taking into account the practice of the EUHR in order to consolidate it in the regulatory plane of Ukraine.

Key words: *international experience, legislation, EUHR practice, right to information protection, GDPR.*

Постановка проблеми. У міжнародному праві норми, які регулюють питання забезпечення права на захист інформації, поділяють на норми «так званого» м'якого права, які мають рекомендаційний характер (Рекомендації Кабінету міністрів Ради Європи (№ R (87) 15 щодо використання персональних даних у сфері діяльності правоохоронних органів, Рекомендація № R (97) 5 щодо захисту медичних даних та ін.) та обов'язкові норми (Конвенція про захист прав і основоположних свобод людини, Конвенція Ради Європи про захист осіб у зв'язку з автоматизованою обробкою їх персональних даних (№ 108), Загальний регламент захисту персональних даних № 2016/679, Директива Європейського парламенту та Ради ЄС «Про захист фізичних осіб щодо обробки персональних даних компетентними органами з метою запобігання, розслідування кримінальних злочинів, ведення розшукових чи судових дій або виконання кримінальних покарань, а також за вільне переміщення таких даних…» № 2016/680). Обов'язковими для держав-членів ЄС є також норми Хартії Європейського Союзу про основоположні права, ст. 8 якої передбачено право на захист персональних даних. Зазначені міжнародно-правові акти спрямовані на гарантування як стабільності правовідносин шляхом забезпечення надійного балансу між правом людини на конфіденційність особистого життя, так і суспільними інтересами в інформаційній сфері.

Основним міжнародним документом, який регламентує право на захист інформації є Загальний регламент захисту персональних даних № 2016/679 (далі – GDPR), який має не лише пряму регулятивну дію в рамках національного права держав-членів Європейського Союзу (далі – ЄС), але й пріоритет у разі «конфлікту» між національним правом та регламентом. Вартим уваги є те, що GDPR заборонено здійснення будь-яких операцій з даними резидентів ЄС у країнах, де рівень захищеності персональних даних нижчий, ніж у ЄС.

Зазначене вище свідчить про те, що проведені останнім часом реформи у сфері забезпечення права на захист інформації доволі успішні та широкомасштабні. Зважаючи на те, що вітчизняне законодавство та судова практика у досліджуваному контексті на сьогодні перебувають на стадії активного розвитку, а також з урахуванням реалізації прагнень до європейської інтеграції, питання щодо вивчення позитивного міжнародного досвіду та практики ЄСПЛ у напрямі забезпечення права на захист інформації є досить актуальним.

Аналіз останніх досліджень та публікацій. Деякі питання європейського правозастосування та оцінки його ефективності у частині, що стосується захисту персональних даних досліджували А. Біла-Кисельова, П. Гуйван, О. Калітенко, B. Custers, Р. Майданик, П. Макушев, О. Оніщенко, П. Рабінович, М. Різак, В. Токарева, С. Шевчук та інші. Разом з тим, питання міжнародного досвіду та практики ЄСПЛ щодо захисту порушених прав людини у контексті захисту персональних даних, з урахуванням суттєвих законодавчих змін у даному напрямі, залишається практично поза увагою та потребує додаткового вивчення.

Метою є дослідження особливостей застосування практики ЄСПЛ при забезпеченні права на захист інформації та окреслення основних міжнародних принципів та стандартів.

Результати дослідження. Конвенцією про захист прав і основоположних свобод людини 1950 року (далі – Конвенція) запроваджено новий механізм вирішення спорів, які виникають у «царині охорони людських прав і свобод» спеціальним правозастосовним органом – Європейським судом із прав людини (далі – ЄСПЛ), який розпочав діяльність у 1959 році у Страсбурзі. Повноваженнями ЄСПЛ передбачено не лише право «винесення вердикту щодо конкретної справи, але й прийняття прецедентного рішення, обов'язкового до застосування на теренах усіх держав-членів, здійснювати так зване судове правотворення» [1].

На сьогодні на міжнародному рівні досягнуто певної узгодженості щодо основоположних принципів та стандартів захисту інформації і відповідних основних процесуальних гарантій, які необхідно включити до національних законодавств. Що стосується обмежень у частині щодо забезпечення гарантованих ст. 52 Хартії Європейського Союзу про основоположні права прав і свобод, а також забезпечення права на захист інформації, то вони допускаються у разі, якщо: передбачені законом; забезпечують дотримання суті права на захист інформації; є необхідними, відповідають принципу пропорційності; відповідають цілям загального інтересу, що визнаний Європейським Союзом, або є необхідними для захисту прав і свобод інших осіб [2].

До основних міжнародних принципів захисту інформації віднесено: принципи законності, чесності та прозорості; принцип обмеження мети; принцип мінімізації даних; принцип точності даних; принцип обмеження періоду зберігання даних; принцип безпеки даних; принцип підзвітності.

У першу чергу обробка приватної інформації має здійснюватися на засадах адекватності, відповідності та ненадмірності (переваги від обмеження прав мають переважати шкоду, яке воно спричиняє для реалізації відповідних основоположних прав). Це так званий принцип пропорційності, відповідно до якого обробка інформації повинна мати законні підстави. Розглянемо, як приклад, рішення ЄСПЛ у справі «Volker und Markus Schecke GbR та Хартмут Ейферт проти землі Гессен», який за результатами розгляду справи дійшов висновку, що «зобов'язавши опубліковувати персональні дані кожної фізичної особи, яка отримала допомогу з сільськогосподарських фондів, без розрізнення за відповідними критеріями, наприклад періодами, коли ці особи отримали таку допомогу, частотою отримання такої допомоги або її характеру та сум, Рада та Комісія вийшли за межі принципу пропорційності» [3].

У справі «Заїченко проти України» (№ 2) В.Г. Заїченко поскаржився на примусове поміщення його до психіатричної лікарні та збір органами міліції про нього даних (збирання органами внутрішніх справ відомостей про нього на підставі вказівок Красногвардійського суду порушило його право на повагу до

його приватного життя за ст. 8 Конвенції) [4]. За результатами розгляду справи Суд дійшов висновку, що дії працівників міліції щодо збору доказів для судово-психіатричної експертизи у відношенні громадянина Заїченка у даному випадку є незаконними, а отже, наявне порушення ст. 8 Конвенції.

Пунктом 118 рішення ЄСПЛ у зазначеній справі визначено, що поняття «згідно із законом» вимагає, щоб оскаржуваний захід не тільки мав підґрунтя у національному законодавстві, але також був сумісний з принципом верховенства права, який прямо зазначається у преамбулі Конвенції і є невід'ємною частиною мети і завдання ст. 8 Конвенції. Закон має бути доступним і передбачуваним, тобто сформульованим достатньо чітко [4]. Також п. 45 рішення ЄСПЛ у справі «Ельсхольц проти Німеччини» передбачено, що «склад та зміст персональних даних, що обробляються володільцем, а також спосіб їх обробки мають відповідати легітимній задачі, обробка є необхідною у демократичному суспільстві задля досягнення цієї цілі» [5, п. 45]. «Якщо хоча б один із вказаних чинників не дотримано, наголошується у п. 34 справи «Кемпбелл проти Сполученого Королівства» [6] та п. 36 справи «Петра проти Румунії» [7], втручання у персональні дані визнається неправомірним з огляду на його непропорційність».

Варто звернути увагу і на те, що будь-які операції (збір, обробка, захист) з приватними даними особи мають бути підпорядковані конкретним визначеним цілям. За інших умов вони є незаконними. Так, наприклад, за результатом розгляду справи «Леандер проти Швеції» ЄСПЛ дійшов висновку про відсутність порушення ст. 10 Конвенції, так як «**секретна перевірка осіб, які подають документи для працевлаштування на посади,** важливі з точки зору національної безпеки, не суперечить вимогам, які *є необхідними у демократичному суспільстві»* [8].

За відсутності підстав, передбачених законодавством, виключається також можливість доступу до персональних даних іншими особами (особливо медичної інформації). Знаковою у даному контексті є справа «І проти Фінляндії». Громадянка Республіки Фінляндія подала до ЄСПЛ заяву за фактом порушення її права на захист «чутливої» інформації. «Окружний заклад охорони здоров'я не зміг виконати свої обов'язки щодо створення реєстру, в якому б її конфіденційна інформація як пацієнта була захищена від розкриття» [9] (заявниця працювала на посаді медсестри в поліклініці захворювань ока при державній лікарні та певний період часу регулярно відвідувала поліклініку інфекційних захворювань у тій же лікарні, у зв'язку із діагнозом «ВІЛ-інфекція». Через деякий час заявниця зрозуміла, що її діагноз у лікарні не є таємницею, тим більше зважаючи на те, що у той час персонал лікарні мав вільний доступ до ідентифікаційного списку пацієнтів, в якому була інформація про діагнози пацієнтів і лікарів, які проводили лікування. Після повідомлення про свої підозри головному лікарю, ідентифікаційний список клієнтів було змінено таким чином, що до медичних карток пацієнтів мав доступ лише персонал установи (клініки), яка проводила лікування. Заявницю було внесено до ідентифікаційного списку клієнтів під вигаданим іменем. Як вбачається, пізніше вона ще раз змінила свої ідентифікаційні дані та отримала новий номер соціального страхування [9]. За результатами розгляду справи, Суд дійшов висновку про порушення ст. 8 Конвенції.

Будь-які операції з конфіденційною інформацією особи мають тривати не довше, ніж це передбачено цілями обробки персональних даних або іншої конфіденційної інформації особи з дотриманням права бути забутим. Слушно у даному контексті зазначає О.М. Калітенко «право бути забутим знаходиться на межі таких двох особистих немайнових прав, як права на інформацію, яке проявляється у безперешкодному доступі до неї, права на вираження власної думку (ст. 19 Всесвітньої декларації прав людини), з іншого боку – на право фізичної особи на приватність, недоторканість та повагу до свого приватного та сімейного життя, захист персональних даних (ст. 7, 8 Хартії Європейського Союзу про основні права та ст. 12 Всесвітньої декларації прав людини) [10; 11, с.44].

Розглянемо, як приклад, рішення у справі «Гугл проти Маріо Костехі Гонсалеса». К. Гонсалес подав до Іспанського агентства із захисту персональних даних (далі – Агентство) скаргу на компанію Google Spain. Заявник зазначив, що під час пошуку його ім'я у Google видаються посилання на газети (датовані 1998 роком), у публікаціях яких присутні його персональні дані у зв'язку із тим, що його будинок було продано на торгах через несплату податків, що є порушенням ст. 8 Конвенції [12]. Агентство підтримало скаргу К. Гонсалеса, і, відповідно, зобов'язало Google видалити відповідні посилання. Компанія Гугл, у свою чергу, вирішила оскаржити рішення у Верховному суді Іспанії, а останній звернувся до Європейського Суду. За результатами розгляду Суд ЄС дійшов висновку, що «право вимагати видалення посилань з результатів пошукової системи ґрунтується на положеннях Директиви 95/46/ЄС (втратила чинність у 2018 році у зв'язку із прийняттям Загального регламенту захисту персональних даних № 2016/679), яка передбачає право суб'єкта персональних даних вимагати від контролера уточнення або видалення даних (ст. 12) та права заперечувати проти обробки його даних (ст. 14) [12]. Разом з тим, дана справа спричинила «запеклі» громадські дискусії щодо встановлення права на забуття як міжнародно-правової норми. «Були висловлені побоювання, що право на забуття суперечить таким правам людини, як свобода слова і свобода доступу до інформації» [13].

Даної точки зору притримується Б. Кастерс, який критично трактує ст. 17 Загального регламенту захисту персональних даних № 2016/679, так як «вона повною мірою не забезпечує реалізацію права на видалення та права особи почати життя з нової сторінки, адже допускає лише можливість видалення персональних даних за дотриманням визначених умов та певних ситуацій» [14].

Варто також звернути увагу на те, що останнім часом, особливо з введенням в Україні правового режиму воєнного стану, суттєво зросла потреба у транскордонному обміні даними, особливо що стосується обміну геномною інформацією. Геномна інформація відноситься до категорії так званих «чутливих» персональних даних, обробка яких забороняється. Статтею 6 Конвенції Ради Європи № 108 про захист осіб у зв'язку з автоматизованою обробкою персональних даних передбачено, що персональні дані не можуть піддаватися автоматизованій обробці, якщо внутрішнє законодавство не забезпечує відповідних гарантій. Разом з тим, окремі норми Закону України «Про державну реєстрацію геномної інформації людини», який набув чинності у лютому 2023 року, мають певні правові невизначеності щодо відповідності її міжнародним стандартам у частині, що стосується дотримання права на захист інформації. «Міжнародний досвід транскордонного обміну геномною інформацією свідчить про доцільність створення єдиної бази даних ДНК, адже за таким принципом успішно ведуться бази даних ДНК в США, Великобританії, Польщі, Німеччині, Італії, Іспанії, Франції» [15]. Однак, функціонування таких баз даних ДНК автоматично передбачає надійний технічний захист та відповідну сертифікацію.

Загальним регламентом захисту персональних даних № 2016/679 визначено дієві механізми та правові підстави для транскордонної передачі персональних даних. Зокрема, статтями 44-50 передбачено, що транскордонні передачі даних можливі: до юрисдикцій в межах ЄЕЗ; до юрисдикцій щодо яких Європейська комісія схвалила рішення про адекватність (зазначимо, що країни, які отримали рішенням про адекватність, підлягають систематичному моніторингу з боку EDPB. Кожне з рішень про адекватність, винесене з набуттям чинності GDPR, включає механізм періодичного перегляду); одержувачу в третій країні на умовах належних гарантій (наприклад, типові договірні положення, обов'язкові корпоративні правила, сертифікація) або на конкретних правових підставах (наприклад, безумовна згода поінформованого суб'єкта персональних даних, виконання правочину між суб'єктом персональних даних та володільцем даних, захист життєвих інтересів суб'єкта персональних даних, публічні інтереси тощо. Проте зазначені підстави застосовуються виключно в індивідуальних випадках і не підходять для щоденного транскордонного обміну масивами HR-даних) [16]. Зазначимо, що за 20 років дії Директиви 95/46/ЄС лише 10 країн були визнані Єврокомісією як такі, що забезпечують «адекватний» рівень захисту інформації.

Рекомендаціями Уповноваженого Верховної Ради України з прав людини щодо забезпечення захисту персональних даних під час укладення Україною міжнародних договорів, які передбачають транскордонний обмін даними визначено, що «центральним органам виконавчої влади, що виконують правоохоронну функцію, рекомендується ініціювати розроблення та укладення Україною окремих міжнародних договорів про захист персональних даних, якими обмінюються з правоохоронною метою, із кожною країною, що не є учасницею Європейського економічного простору та/або не підписала Конвенцію 108. Так, наприклад, між ЄС та США укладено низку договорів щодо співробітництва між правоохоронними органами держав-членів Союзу і США. При цьому питання забезпечення належного рівня захисту персональних даних при реалізації цих договорів гарантовано окремим Рамковим договором ЄС-США про захист персональних даних (передбачено перелік чітких гарантій для забезпечення захисту персональних даних у контексті їх транскордонної передачі в рамках співробітництва між правоохоронними органами), якими обмінюються для правоохоронних цілей [17, с. 8].

Висновки. Підсумовуючи, зазначимо, що подальша інформатизація суспільства, а це зростання обміну інформацією між публічними та приватними суб'єктами, між публічними суб'єктами в органах державної влади вимагають у першу чергу узгодженості дій між суб'єктами забезпечення інформаційної безпеки у частині, що стосується забезпечення права на захист інформації.

Аналіз основних норм міжнародного законодавства та практики Європейського Союзу з прав людини свідчить про необхідність приведення вітчизняного законодавства у відповідність до основних принципів та стандартів, визначених Загальним регламентом захисту персональних даних № 2016/679. Що стосується практики ЄСПЛ у даному напрямі, то, як показує практика, вона йде шляхом пріоритетності права на захист інформації над потенційним інтересом суб'єкта господарювання, котрому така інформація потрібна з метою надання послуг, що свідчить про доцільність врахування практики ЄСПЛ для закріплення її в нормативній площині України.

Список використаних джерел:

1. Посібник з європейського права у сфері захисту персональних даних. 2018. URL: chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/fra-coe-edps-2018-handbook-data-protection_ukr.pdf

2. Хартія основних прав Європейського Союзу. Ніццький договір та розширення Європейського Союзу. К., 2001. 124 с.

3. Рішення ЄСПЛ у справі «Volker und Markus Schecke GbR та Хартмут Ейферт проти землі Гессен» від 17.06.2010. URL: https://eur-lex.europa.eu/legal-content/GA/TXT/?uri=CELEX:62009CC0092

4. Рішення ЄЄСПЛ у справі «Заїченко проти України» (№ 2) (заява № 45797/09) від 26.02.2015. URL: https://zakon.rada.gov.ua/laws/show/974_a87#Text

5. Рішення ЄСПЛ у справі «Ельсхольц проти Німеччини» (заява № 25735/94) від 13.07.2000. URL: http://www.c-g.org.uk/camp/hr/elsholz.htm

6. Рішення ЄСПЛ у справі «Кемпбелл проти Сполученого Королівства» (заява № 13590/88) від 25.03.1992. URL: https://hudoc.echr.coe.int/eng

7. Рішення ЄСПЛ у справі «Петра проти Румунії» (заява №27273/95) від 23.09.1998. URL: http://echr.ketse.com/doc/27273.95-en-19980923

8. Рішення ЄСПЛ у справі «Леандер проти Швеції» (заява № 9248/81) від 26.03.1987. URL: https://dostup.pravda.com.ua/digest/publications/laifkhaky-vid-tsedem-iak-vyhraty-v-yespl-spravu-z-dostupu-do-informatsii

9. Рішення ЄСПЛ у справі «І проти Фінляндії» (заява № 20511/03) від 17.07.2008. URL: efaidnbmnnnibpcajpcglclefindmkaj/https://rm.coe.int/168059920d

10. Калітенко О. М. Право на забуття: здобуток європейський чи глобальний? Римське приватне право: здобутки європейські та глобальні : матеріали міжнар. колокв. (м. Одеса, 27 жовт. 2018 р.). Одеса : Фенікс, 2018. С. 84–86.

11. Токарева В. О. Окремі питання реалізації права на видалення. *Актуальні проблеми вітчизняної юриспруденції.* 2022. № 4. С. 42–47.

12. Рішення Суд ЄС у справі «Mario Costeja González» від 13.05.2014. URL: http://curia.europa.eu/juris/document/document_print.jsf?doclang=EN&docid=152 065

13. Право на забуття. Матеріали з Вікіпедії. URL: https://uk.wikipedia.org/wiki/Право_на_забуття

14. Custers B., Calders T., Schermer B., Zarsky T. What is data mining and how does it work? *Discrimination and Privacy in the Information Society.* 2013.

15. Парламент прийняв Закон «Про державну реєстрацію геномної інформації людини». URL: https://www.kmu.gov.ua/news/parlament-pryiniav-zakon-pro-derzhavnu-reiestratsiiu-henomnoi-informatsii-liudyny

16. Загальний регламент із захисту персональних даних № 2018/1725. URL: http://aphd.ua/gdpr-ofitsiinyi-ukranskyi-pereklad

17. Рекомендації Уповноваженого Верховної Ради України з прав людини щодо забезпечення захисту персональних даних під час укладення Україною міжнародних договорів, які передбачають транскордонний обмін даними. Київ, 2021. URL: chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www.ombudsman.gov.ua/storage/app/media/transkordonna-peredacha-personalnyh-danyh.pdf