УДК 342.9
DOI https://doi.org/10.32782/2524-0374/2024-10/144

# ЗАХИСТ ПЕРСОНАЛЬНИХ ДАНИХ ЄВРОПЕЙСЬКИМ СУДОМ З ПРАВ ЛЮДИНИ

# PROTECTION OF PERSONAL DATA BY THE EUROPEAN COURT OF HUMAN RIGHTS

**Пашинський В.Й., д.ю.н., доцент,**
**доцент кафедри адміністративного права та процесу**
*Навчально-науковий інститут права Київського національного університету імені Тараса Шевченка*

**Цьоменко А.В., PhD,**
**асистент кафедри адміністративного права та процесу**
*Навчально-науковий інститут права Київського національного університету імені Тараса Шевченка*

Розбудова України як європейської, демократичної, правової держави, де найвищою цінністю є людина і її права, вимагає створення та ефективного функціонування інститутів публічної влади, які забезпечують реалізацію та захист основних прав та свобод громадян. Провідне місце у системі таких прав наразі належить правам пов'язаним з забезпеченням захисту персональних даних громадян, без чого неможлива реалізація конституційних прав і свобод громадян України суб'єктами публічної влади в повному обсязі. Радикальні інновації у сфері інформаційних технологій призводять до поглиблення різноманітних аспектів захисту прав і свобод людини, невід'ємною складовою, яких є обробка і захист персональних даних, що обумовлює необхідність дослідження європейського досвіду в зазначеній сфері. Актуальність теми пов'язана із швидким запровадженням інформаційних технологій та процесів у всіх сферах публічного адміністрування через створення різноманітних баз даних та доступу органів публічної влади до персональних даних громадян і необхідністю забезпечення їх захисту. Активна розбудова електронного врядування та процеси цифрової трансформації управлінської діяльності в Україні та світі загалом, визначають завдання щодо формування «держави в смартфоні», здійснення «цифровізації економіки» та проведення «цифрових трансформацій» в органах публічної влади. Вище зазначене вимагає створення правових механізмів забезпечення захисту персональних даних громадян. Відтак, стаття присвячена аналізу практики Європейського суду з прав людини (далі – ЄСПЛ) щодо захисту персональних даних та дослідженню основних рішенньь Суду, що стосуються прав громадян на захист їхньої приватності та особистої інформації, а також вплив цих рішень на розвиток міжнародної правової доктрини в сфері захисту персональних даних. Автори розглядають ключові аспекти правозастосування, а також роль ЄСПЛ у встановленні стандартів та механізмів забезпечення прав людини у контексті сучасних викликів, зокрема у цифровому середовищі. На основі проведеного аналізу зроблено висновок про необхідність удосконалення національних правових систем у сфері захисту персональних даних з урахуванням практики ЄСПЛ для ефективної реалізації прав людини в умовах глобалізації та цифровізації інформаційного простору.

**Ключові слова:** права фізичних осіб, захист прав людини, адміністративно-правове забезпечення захисту персональних даних, персональні дані, Європейський суд з прав людини, Уповноважений Верховної Ради України з прав людини.

The development of Ukraine as a European, democratic, legal state, where the highest value is the person and his rights, requires the creation and effective functioning of public authorities that ensure the implementation and protection of fundamental rights and freedoms of citizens. The leading place in the system of such rights currently belongs to the rights related to ensuring the protection of personal data of citizens, without which the full implementation of the constitutional rights and freedoms of citizens of Ukraine by public authorities is impossible. Radical innovations in the field of information technologies lead to the deepening of various aspects of the protection of human rights and freedoms, an integral part of which is the processing and protection of personal data, which necessitates the study of European experience in this area. The relevance of the topic is associated with the rapid introduction of information technologies and processes in all areas of public administration through the creation of various databases and access of public authorities to the personal data of citizens and the need to ensure their protection. The active development of e-governance and the processes of digital transformation of administrative activities in Ukraine and the world in general determine the tasks of forming a "state in a smartphone", implementing "digitalization of the economy" and conducting "digital transformations" in public authorities. The above requires the creation of legal mechanisms to ensure the protection of citizens' personal data. Therefore, the article is devoted to the analysis of the practice of the European Court of Human Rights (hereinafter referred to as the ECHR) on the protection of personal data and the study of the main decisions of the Court concerning the rights of citizens to the protection of their privacy and personal information, as well as the impact of these decisions on the development of international legal doctrine in the field of personal data protection. The authors consider key aspects of law enforcement, as well as the role of the ECHR in establishing standards and mechanisms for ensuring human rights in the context of modern challenges, in particular in the digital environment. Based on the analysis, a conclusion is drawn about the need to improve national legal systems in the field of personal data protection, taking into account the practice of the ECHR for the effective implementation of human rights in the context of globalization and digitalization of the information space.

**Key words:** rights of individuals, protection of human rights, administrative and legal support for the protection of personal data, personal data, European Court of Human Rights, Commissioner for Human Rights of the Verkhovna Rada of Ukraine.

У сучасних умовах швидкого розвитку цифрових технологій, що застосовуються у всіх сферах суспільного життя, особливо в сфері публічного управління, що призводить до стрімкого зростання обсягу обробки персональних даних суб'єктами публічної адміністрації, питання забезпечення належного захисту таких даних набуває особливої актуальності. Інтернет-платформи, електронні сервіси, бази даних та інші інструменти, які активно використовуються суб'єктами публічної адміністрації для збирання, зберігання та обробки персональних даних, створюють нові виклики для правової системи. У цьому контексті одним із важливих аспектів є забезпечення не лише захисту персональних даних громадян, але й ефективного контролю та регулювання обробки персональних даних, що є окремим правом, закріпленим міжнародними стандартами.

Наразі Україна вживає необхідних заходів щодо адаптації європейських стандартів щодо захисту персональних даних в національне законодавство, як держава-кандидат на вступ до Європейського Союзу (далі – ЄС). З цього приводу В. І. Теремецький та Д. В. Цвірюк наголошують про те, що незважаючи на успішне створення сучасної та адекватної нормативно-правової бази для розвитку системи захисту персональних даних в Україні за останні роки, на даний момент в країні напрацьовані лише основи законодавства у зазначеній сфері. Також вчені правники зазначають, що законодавство в цілому відповідає міжнародним стандартам, проте потребує подальшої роботи з систематизації, розробки виконавчих актів, національних стандартів та чіткого визначення термінів, понять і категорій [1, с. 81].

Вирішення питання ефективного публічно-правового механізму забезпечення персональних даних грома-

дян є також частиною вимог щодо майбутнього вступу України до ЄС та знаходить своє відображення у відповідних програмних документах.

Так, зокрема, у тексті Доповіді Європейської комісії «Ukraine 2023 Report Accompanying the document Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions Brussels, 8.11.2023 SWD(2023) 699 final» («Звіт про Україну 2023, що супроводжує документ Повідомлення Комісії до Європейського парламенту, Ради, Європейського економічного та соціального комітету та Комітету регіонів Брюссель, 8.11.2023 SWD(2023) 699») йдеться поміж іншого про те, що Україна зобов'язана прийняти закон про захист персональних даних, узгоджений із acquis ЄС [2; 3, с. 6]. Також, у Доповіді Європейської комісії йдеться про те, що у сфері захисту персональних даних, Україна має продовжити роботу над приведенням у відповідність із acquis ЄС. Нинішнім ключовим законодавчим актом, який регулює захист даних, є Закон про захист персональних даних від 2010 року (Law on personal data protection of 2010), який є недостатньо деталізований і має проблеми в застосуванні. Також, Україна ратифікувала Конвенцію 108 про захист осіб щодо автоматизованої обробки персональних даних (ILO Convention 108 on the Protection of Individuals with regard to Automatic Processing of Personal Data). Уповноважений Верховної Ради України з прав людини є органом, відповідальним за перевірку дотримання законодавства про захист персональних даних, але він не має відповідних ресурсів, щоб робити це ефективно. Законопроект про захист персональних даних було внесено до Верховної Ради 7 вересня 2022 року» [3, с. 42], саме із зазначених вище причин набуває своєї актуальності аналіз практики ЄСПЛ у сфері забезпечення захисту персональних даних.

В першу чергу, необхідно зазначити, що уповноважені незалежні органи, які здійснюють регулювання захисту персональних даних у Європейському Союзі здійснюється спеціальними уповноваженими органамита та судовими органами, що встановлено Директивою (ЄС) 2016/680 [4].

Натомість, в Україні, наразі контроль за дотриманням зазначених прав здійснює Уповноважений Верховної Ради України з прав людини та суди. Однак, виконання ефективного контролю в цій сфері відповідно до всіх міжнародних стандартів стає неможливим в межах повноважень Омбудсмена. Об'єднання функцій контролю за вказаними правами з мандатом Омбудсмена загрожує ефективності реалізації як першого, так і другого [5].

Як слушно зазначає О.А. Заярний, для забезпечення здійснення публічного моніторингу та виконання міжнародних зобов'язань, що випливають з актів Ради Європи та GDPR, в Україні розглядається важливим створення інформаційного омбудсмена. Такий омбудсмен буде незалежним, колегіальним центральним органом виконавчої влади, який матиме спеціальний статус. Він буде нести відповідальність перед Президентом України та підконтрольний і підзвітний Верховній Раді України [6].

В цьому аспекті необхідно зазначити, що нині Україна є одним із лідерів щодо запровадження інформаційних технологій в діяльність органів публічного управління, а також створення системи електронного урядування, та здійснює широкий доступ до застосування, в тому числі програм штучного інтелекту. Втім, на нашу думку, таке зростання використання інформаційно-телекомунікаційних технологій та технологій штучного інтелекту в публічному управлінні викликає потребу у відповідних нормативно-правових механізмах, які гарантуватимуть ефективне забезпечення захист прав та свобод громадян, включаючи захист персональних даних відповідно до стандартів ЄС, що доводять необхідність вже зараз розпочати розробку комплексу правових та організаційно-управлінських заходів забезпечення захисту персональних даних громадян у контексті використання штучного інтелекту. Відтак, основними завданнями щодо подальшого вдосконалення правового регулювання захисту персональних даних є здійснення заходів щодо: а) приведення національного законодавства щодо захисту персональних даних до стандартів ЄС, як невід'ємна складова європейської інтеграції України; б) визначення на законодавчому рівні системи органів публічного контролю за забезпеченням захисту персональних даних, яке відповідає законодавству ЄС. З огляду на це є необхідність доповнити національне законодавство нормами відповідно до яких органам державної влади та органам місцевого самоврядування буде надано повноваження щодо забезпечення захисту персональних даних [7, с. 155–157].

Відтак, наразі забезпечення захисту персональних даних фізичних осіб у контексті стрімкого використання та поширення інформаційно-телекомунікаційних систем та розвитку штучного інтелекту стає важливим завданням для органів публічного управління і повинно бути врегульоване на законодавчому рівні. Потреба у створенні ефективних механізмів захисту особистих даних обумовлена також широким використанням інноваційних проектів, таких як «цифрове урядування» та «смарт-міста», що ґрунтуються на створенні обширних баз даних користувачів. Необхідно регулювати питання стосовно використання та обробки персональних даних у процесі «навчання» штучного інтелекту [8].

В цьому аспекті, необхідно звернутись до європейського досвіду у згаданій сфері, який ,на нашу думку, є особливо актуальним, оскільки ЄСПЛ вже давно став важливим інструментом захисту прав людини, зокрема у контексті гарантування безпеки і захисту персональних даних. Принципи та рішення ЄСПЛ щодо обробки персональних даних сприяють формуванню чітких норм та стандартів у цій галузі, що дозволяють забезпечити належний рівень захисту персональної інформації на міжнародному рівні та в діяльності національних органів, які здійснюють збирання, оброку та зберігання персональних даних. Практика ЄСПЛ, зокрема, надає конкретні орієнтири для національних судів і суб'єктів публічної адміністрації щодо забезпечення балансу між інтересами національної безпеки та правом громадян на ефективний захист персональних даних. На нашу думку, для досягнення такого балансу важливими є такі чинники, як чітке нормативне регулювання, ефективний контроль за обробкою персональних даних, дотримання принципів пропорційності та необхідності, а також забезпечення дієвих механізмів судового та адміністративного захисту.

В першу чергу, необхідно наголосити, що право на персональні дані безпосередньо не згадується в Конвенції про захист прав людини і основоположних свобод, підпадає під її дію, що неодноразово підтверджувалось в практиці ЄСПЛ.

Так, у 1987 році ЄСПЛ у справі Leander проти Швеції [9] визнав, що інформація з секретного поліцейського реєстру, що містила дані про особисте життя пана Леандера, а також відмова у наданні можливості йому спростувати ці дані, порушували його право на повагу до приватного життя, яке гарантується статтею 8 Конвенції про захист прав людини [9]. Суд надав визначення терміну «персональні дані» як будь-яку інформацію, яка стосується конкретно визначеної особи або особи, яка може бути конкретно визначеною. Зазначене поняття охоплює не лише відомості про «приватне життя», що розуміється ширше, адже воно включає право на встановлення та розвиток відносин з іншими людьми, а також інформацію про професійну та ділову діяльність. [9]. Більше того, публічна інформація може вважатися «приватним життям», якщо вона систематично збирається та зберігається в базах даних, якими володіють органи публічної влади [8].

У своїх рішеннях ЄСПЛ послідовно формує підходи до захисту прав суб'єкта персональних даних, визначаючи баланс між правом особи на доступ до власної інформації та необхідністю захисту суспільних інтересів. Суд наголошує на тому, що право на доступ до персональних даних є невід'ємною частиною права на приватність і має гарантувати не лише можливість ознайомлення з інформацією, що зберігається державними органами, а й отримання її у доступній та зрозумілій формі [9]. Особливу увагу Суд приділяє питанням ефективності реалізації цього права, підкреслюючи, що національні органи повинні створювати дієві механізми доступу до персональних даних [10] . Важливим критерієм ефективності Суд визначає своєчасність надання інформації, можливість отримання копій відповідних документів та обґрунтованість будь-яких обмежень у доступі [11]. Водночас Суд визнає допустимість певних обмежень цього права, якщо вони виправдані легітимними цілями, такими як забезпечення національної безпеки [9] або захист прав і конфіденційної інформації третіх осіб [13]. Відтак, зазначена практика ЄСПЛ встановлює стандарти, які повинні враховувати держави у процесі розробки та застосування законодавства про захист персональних даних, забезпечуючи рівновагу між інтересами держави та правами людини.

На нашу думку, особливу увагу також слід приділити забезпеченню безпеки персональних даних, що вимагає від держави позитивного зобов’язання забезпечувати повагу до приватного життя осіб, що передбачає впровадження системи правил та гарантій для захисту даних. Така система має бути практичною та ефективною, перш за все, забезпечуючи виключення будь-якого несанкціонованого доступу до персональних даних. Згідно з позицією ЄСПЛ, право на корекцію або видалення своїх персональних даних означає, що відмова у можливості спростувати неточні персональні дані становить порушення права на повагу до приватного життя, яке гарантується статтею 8 Конвенції [14].

В аспекті нашого дослідження також є необхідність звернути увагу і на протележну позицію ЄСПЛ стосовно збору персональних даних. У справі Breyer v. Germany (заява № 50001/12), ухваленій ЄСПЛ від 30 січня 2020 року, Суд розглянув питання щодо правомірності збору та зберігання персональних даних в контексті Телекомунікаційного акта Німеччини. Справа стосувалась обов'язку постачальників телекомунікаційних послуг збирати та зберігати певні персональні дані потенційних абонентів, які планують придбати SIM-карту на умовах попередньої оплати [15].

Згідно з чинним на той момент законодавством Німеччини, поправки до Закону про телекомунікації, внесені в червні 2004 року, зобов'язували постачальників мобільних послуг збирати та зберігати персональні дані своїх клієнтів навіть у випадках, коли ці дані не були необхідні для здійснення розрахунків або виконання договору. Зазначене стосувалося, зокрема, абонентів, які придбали SIM-карту на умовах попередньої оплати, для яких збір таких даних (включаючи ім’я, адресу, дату народження та номер телефону) був обов'язковим [15].

ЄСПЛ зазначив, що за своєю природою зберігання даних, які стосуються приватного життя особи, є втручанням у право на приватність, гарантоване статтею 8 Європейської конвенції з прав людини. Водночас Суд підкреслив, що це втручання не є автоматично незаконним, а має бути оцінене з точки зору пропорційності та відповідності законодавчим вимогам. Важливим елементом аналізу стало питання, чи є це втручання необхідним у демократичному суспільстві та чи відповідає воно умовам, передбаченим статтею 8, зокрема, чи є воно «необхідним у демократичному суспільстві», чи відповідно до закону та пропорційним [15].

Суд визнав, що обов'язок зберігати персональні дані абонентів, який був передбачений національним законодавством, не суперечить вимогам статті 8 Конвенції. Зазначене рішення стало значущим в контексті відсутності єдиного підходу до цього питання серед держав-членів Ради Європи, оскільки в різних країнах існують різні підходи до регулювання збору та зберігання персональних даних у телекомунікаційному секторі. Втім, у рішенні по справі Breyer v. Germany ЄСПЛ не обмежувався лише правовим аналізом, а врахував також і суспільний контекст. Важливим було те, що оскаржуване зберігання даних стосувалося лише обмеженого набору інформації, який не містив надмірної особистої інформації, не дозволяв створювати профілі осіб або відстежувати їх переміщення. Крім того, не зберігалися дані про індивідуальні комунікації між абонентами [15].

Таким чином, Суд зробив розрізнення між цим рівнем втручання та попередніми справами, де йшлося про збір більш чутливих даних або випадки, коли реєстрація в певній базі даних супроводжувалася частими перевірками або додатковим збором приватної інформації. Зрештою, Суд дійшов висновку, що втручання було обмеженим за своїм характером.

Висновок ЄСПЛ був підтриманий, зокрема, тим, що німецьке законодавство забезпечує належний рівень захисту прав абонентів, зокрема, через регулювання можливості обробки та зберігання даних. Федеральний конституційний суд Німеччини також підтвердив, що обов'язок постачальників телекомунікаційних послуг зберігати такі дані не суперечить Основному закону Німеччини, що засвідчило відповідність національного законодавства міжнародним стандартам прав людини.

Відтак, ЄСПЛ, розглядаючи справу Breyer v. German, підтвердив, що у разі наявності чітко визначених законних цілей та належного рівня захисту особистих даних, обов'язковий збір і зберігання персональних даних абонентів, передбачений національним законодавством, може бути визнаний таким, що не порушує статтю 8 Європейської конвенції з прав людини [15].

Відтак, на нашу думку, сучасний розвиток цифрових технологій вимагає постійного перегляду правової оцінки ступеня втручання в особисте життя через використання таких технологій і зазначене рішення не слід розглядати як таке, що збільшує рівень втручання в особисті свободи в інтересах безпеки. Аналіз рішення свідчить про те, що воно було ухвалене з особливою обережністю та застереженнями, із детальним вивченням як інформації, що передавалася операторам мобільного зв’язку, так і термінів її зберігання. Подібні питання були предметом аналізу й Судом Європейського Союзу, який приймав різні рішення в залежності від обсягу інформації, що зберігалася щодо конкретного абонента. Таким чином, висновки ЄСПЛ у вище згаданій справі слід розглядати в контексті усіх фактичних обставин справи.

**Висновки.** Таким чином, практика ЄСПЛ щодо захисту персональних даних є важливим етапом у розумінні того, як міжнародне правове співтовариство реагує на виклики цифрової епохи та як ефективно захищати права громадян у світі, де персональні дані стали одним із найбільших ресурсів, що потребують ретельного контролю та захисту. З огляду на швидкий розвиток цифрових технологій і зростаючу загрозу втручання у приватне життя через збір, зберігання та обробку персональних даних, досвід ЄСПЛ набуває особливої значущості для країн, які прагнуть удосконалити свою правову систему та механізми захисту прав людини.

Для України, яка прагне поглибити свою інтеграцію з ЄС та забезпечити високі стандарти захисту прав людини, досвід ЄСПЛ у досліджуваній сфері є важливим орієнтиром. Оскільки, людина та захист її прав є найвищою цінністю, що закріплено в Конституції України та міжнародних правових актах, одним із ключових аспектів забезпечення цієї цінності є ефективний захист персональних даних, який гарантує недоторканність приват-

ного життя та свободу особи, особливо в сучасних умовах цифрової трансформації, коли зростає ризик зловживання персональними даними, на державу покладається відповідвльність щодо створення дієвих правових механізмів для запобігання незаконному збору, використанню та розповсюдженню таких даних. З огляду на це, саме дотримання міжнародних стандартів та практики ЄСПЛ у сфері захисту персональних даних буде сприяти забезпеченню прав людини та підіймати рівень довіри громадян до органів публічної влади.

**ЛІТЕРАТУРА**


1. Теремецький В. І., Цвірюк Д. В. Застосування зарубіжного досвіду правового захисту персональних даних в Україні. *Часопис Академії адвокатури України*. 2014. Т. 7, № 2. С. 73–82.
2. Report on the initial assessment of the progress in the implementation of the European Union legal Acts (EU ACQUIS). *Кабінет Міністрів України.* URL: https://eu-ua.kmu.gov.ua/wp-content/uploads/Zvit_EN.pdf.
3. Ukraine 2023 Report Accompanying the document Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions Brussels, 8.11.2023 SWD (2023) 699 final. *European Neighbourhood Policy and Enlargement Negotiation*s. URL:https://neighbourhood-enlargement.ec.europa.eu/ system/files/2023-11/SWD_2023_699%20 Ukraine%20report.pdf.
4. Directive (EU) 2016/680 of the European Parliament and of the Council, of 27 April 2016. URL: https:///eur-lex.europa.eu/legalcont ent/ en/TXT/%3Furi%3DCELEX%253A32016L0680 &p rev=search.
5. Проект Закону про Національну комісію з питань захисту персональних даних та доступу до публічної інформації / *Верховна Рада України*. URL: .
6. Заярний О. До питання щодо забезпечення правомірної обробки біометричних даних в діяльності національної поліції національні та міжнародні стандарти. *Юридичний вісник* 2021. № 6. С. 160–164. URL: http://yuv.onua.edu.ua/index.php/yuv/article/view/2278/2552.
7. Цьоменко А.В. Адміністративно-правове забезпечення захисту персональних даних громадян суб'єктами публічної адміністрації. Дисертація на здобуття ступеня доктора філософії. URL: https://uacademic.info/ua/document/0824U003112#google_vignette.
8. Пунда О.О., Арзянцева Д.А. Забезпечення захисту персональних даних фізичних осіб в умовах розвитку штучного інтелекту. *Наука і техніка перспективи*. *Серія «Право, економіка, педагогіка, техніка, фізико-математичні науки»*. 2024. № 2(30). С.132–143.
9. Case of Leander v. Sweden, App. №. 9248/81. *European Court of Human Rights*. URL: http://hudoc.echr.coe.int/eng?i=001-57519.
10. Case of Gaskin v. The United Kingdom, App. №. 10454/83. *European Court of Human Rights*. URL: http://hudoc.echr.coe.int/ eng?i=001-57491.
11. Case of K.H. and others v. Slovakia, App. №. 32881/04. *European Court of Human Rights.* URL: http://hudoc.echr.coe.int/ eng?i=001-145421.
12. Case of Haralambie v. Romania, App. №. 21737/03. *European Court of Human Rights.* URL: http://hudoc.echr.coe.int/eng?i=002-1286.
13. Case of Odievre v. France, App. №. 42326/98. *European Court of Human Rights.* URL: http://hudoc.echr.coe.int/eng?i=001-60935.
14. Case of Rotaru v. Romania, App. №. 28341/95. *European Court of Human Rights.* URL: http://hudoc.echr.coe.int/eng?i=001-58586.
15. Case of Breyer v. Germany, App.№. 50001/12. *European Court of Human Rights.* URL: https://hudoc.echr.coe.int/eng?i=001-200442.