

ШТУЧНИЙ ІНТЕЛЕКТ В ПРАКТИЦІ ТА РІШЕННЯХ ЄВРОПЕЙСЬКОГО СУДУ З ПРАВ ЛЮДИНИ

УДК 341.1/8:342.7

DOI <https://doi.org/10.32782/ehrlrichsjournal-2025-12.05>

ОЛЕКСАНДР КУТОВИЙ

аспірант кафедри конституційного,

міжнародного права та публічно-правових дисциплін

Київського університету інтелектуальної власності та права, Україна

ORCID: 0009-0004-7939-8847

СЕРГІЙ БУРМА

кандидат юридичних наук, доцент кафедри конституційного,

міжнародного права та публічно-правових дисциплін

Київського університету інтелектуальної власності та права, Україна

ORCID: 0000-0002-8682-542X

Анотація. У статті розглянуто вплив алгоритмічних та комп'ютерних систем, методів і програмного забезпечення штучного інтелекту (ШІ) на судову практику Європейського суду з прав людини (ЄСПЛ), зокрема, виклики та можливості, які виникають через технологічний розвиток суспільства. Проаналізовано практику ЄСПЛ щодо згадок у текстах судових рішень про системи та засоби ШІ, пов'язані з проблемними питаннями реалізації прав людини, констатовані та потенційні порушення прав людини. Особливу увагу приділено питанням приватності, захисту й обробки персональних даних та контролю за їх використанням. Це питання особливо гостро постає у справах, що стосуються автоматичної обробки даних, алгоритмічних рішень, втрати контролю над персональними даними, які можуть порушувати право на приватність у світлі статті 8 Конвенції про захист прав людини і основоположних свобод. Досліджуються конкретні рішення ЄСПЛ, в яких ШІ згадується прямо або опосередковано, визначаються основні проблеми, що виникають у судовій практиці. Із набранням чинності Акта про штучний інтелект (EU Artificial Intelligence Act) Європейського Союзу, Регламент (ЄС) № 2024/1689 Європейського Парламенту та Ради від 13 червня 2024 року, що встановлює гармонізовані правила щодо ШІ, можна очікувати, що питання використання ШІ стане ще актуальнішим для розвитку судової практики, адже технології ШІ все більше впливатимуть на демократичні процеси та основні права громадян. Тому подальше дослідження судової практики та нормативних ініціатив, спрямованих на забезпечення прав людини в умовах цифровізації, є важливим для розробки правових стандартів для використання ШІ. Стаття підкреслює, що наявні рішення ЄСПЛ, хоча й не охоплюють безпосередньо використання ШІ, дають важливі орієнтири для розвитку правових стандартів, які можуть бути адаптовані до нових реалій, зокрема для захисту персональних даних і гарантій приватності у цифровому середовищі.

Ключові слова: штучний інтелект (ШІ); системи та засоби ШІ; Європейський суд з прав людини (ЄСПЛ); Рада Європи; Європейський Союз; міжнародне правосуддя; права людини; міжнародний захист прав людини; прецедентне право; судовою практика; цифрове правосуддя; цифровізація судочинства; доступ до правосуддя.

ARTIFICIAL INTELLIGENCE IN THE CASE-LAW OF THE EUROPEAN COURT OF HUMAN RIGHTS

UDC 341.1/8:342.7

DOI <https://doi.org/10.32782/ehrlrichsjournal-2025-12.05>

OLEKSANDR KUTOVYI

Postgraduate Student at the Department of Constitutional,

International Law and Public Law Disciplines

Kyiv University of Intellectual Property and Law, Ukraine

ORCID: 0009-0004-7939-8847

SERGII BURMA

Candidate of Legal Sciences, Associate Professor at the Department of Constitutional, International Law and Public Law Disciplines

Kyiv University of Intellectual Property and Law, Ukraine

ORCID: 0000-0002-8682-542X

Abstract. This article examines the impact of algorithmic and computer systems, methods, and artificial intelligence (AI) software on the judicial practice of the European Court of Human Rights (ECtHR), particularly the challenges and opportunities arising from the technological development of society. The article analyzes the ECtHR's practice regarding references to AI systems and tools in the text of judicial decisions, related issues concerning the implementation of human rights, as well as identified and potential human rights violations. Special attention is given to issues of privacy, the protection and processing of personal data, and control over their use. These issues are particularly pressing in cases involving the automatic processing of data, algorithmic decisions, and the loss of control over personal data, which may violate the right to privacy under Article 8 of the European Convention on Human Rights and Fundamental Freedoms. The article explores specific ECtHR decisions where AI is mentioned directly or indirectly and identifies key issues arising in judicial practice. With the entry into force of the Artificial Intelligence Act (AI Act), Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024, it can be expected that the use of AI will become even more relevant for the development of judicial practice, as AI technologies increasingly impact democratic processes and fundamental human rights. Therefore, further research on judicial practice and normative initiatives aimed at ensuring human rights in the context of digitalization is crucial for the development of legal standards for the use of AI. The article emphasizes that although existing ECtHR decisions do not directly address the use of AI, they provide important guidelines for the development of legal standards that can be adapted to new realities, particularly for the protection of personal data and privacy guarantees in the digital environment.

Key words: artificial intelligence (AI); AI systems and tools; European Court of Human Rights (ECtHR); Council of Europe; European Union; international justice; human rights; international protection of human rights; case law; judicial practice; digital justice; digitalization of court proceedings; access to justice.

Упродовж останніх років як на міжнародній арені, так і на рівні національних законодавств окремих держав неухильно зростає увага до проблем використання та правового регулювання систем та засобів штучного інтелекту (надалі – ШІ). Європейський суд з прав людини (надалі – ЄСПЛ, Суд), будучи головним навігатором для просування та захисту прав людини на європейському континенті, стикається з очевидною необхідністю врахування у своїй діяльності засобів технологічного розвитку, нових можливостей та викликів, які з'являтимуться із еволюцією ШІ.

Розвиток ШІ приносить як суттєві переваги, так і нові екзистенційні ризики. Роль Ради Європи, безсумнівно, полягає в забезпеченні того, щоб права людини, демократія та верховенство права були дотримані, захищені та підтримувані в цифровому середовищі. Як зазначила Генеральний секретар Ради Європи Марія Пейчинович-Бурич, «Рада Європи неодноразово демонструвала свою здатність створювати нові стандарти, які стали світовими орієнтирами. Ми будемо працювати з ШІ в цій традиції, застосовуючи цей підхід з багатьма зацікавленими сторонами, співпрацюючи з іншими міжнародними організаціями, громадянським суспільством, бізнесом та академічною спільнотою... ШІ вже є частиною нашого життя – він змінює інформацію, яку ми отримуємо, вибори, які ми робимо, та способи, якими функціонують наші суспільства. У найближчі роки ШІ відіграватиме ще більшу роль у тому, як працюють уряди та публічні установи, а також у тому, як громадяни взаємодіють і беруть участь у демократичному процесі» [1].

Постає запитання, як ЄСПЛ реагуватиме на ці нові виклики та діятиме в умовах, що є новими для нього. Інтеграція ШІ в наше повсякденне життя вже не є чимось неочікуваним ані для науковців, ані для практиків, ані для звичайних громадян; існує безліч публікацій, що аналізують теоретичні аспекти взаємодії ШІ та прав людини. Хоча теоретичні дослідження можуть підтримувати практичні підходи та впливати на їх розвиток, вони не здатні повністю замінити практичний досвід. Тому для повного розуміння того, як ШІ впливає на захист прав людини, необхідно вивчати реальний вплив ШІ в практичній площині. Ми спробуємо дослідити та проаналізувати судову практику ЄСПЛ, пов'язану зі ШІ, зокрема через прямі згадки в текстах рішень.

У сучасній науковій літературі все більше уваги приділяється ролі ШІ у правовій сфері, зокрема його застосуванню у судочинстві та впливу на права людини.

Окремі аспекти використання ШІ у судочинстві розглядали Я. Берназюк, Д. Белов, М. Белова, Н. Блажівська, Т. Буоч, М. Василенко, В. Городовенко, І. Голубовський, К. Зеров, А. Калараш, С. Козьяков, Є. Краснов, В. Крат, М. Войнов, А. Мергалієв, Н. Плевачук, Н. Піпченко, О. Синиця, В. Слатвінська, Т. Степанова, А. Херн, Г. Юровська та ін.

Більшість дослідників наголошує на необхідності обережного впровадження ШІ у судову систему з урахуванням можливих ризиків, таких як алгоритмічна несправедливість, недостатня прозорість ухвалення рішень, питання відповідальності та етичні дилеми. Також підкреслюється потреба в нормативному регулюванні використання ШІ, навчанні суддів роботи з такими технологіями та запровадженні механізмів моніторингу, що дозволить мінімізувати потенційні загрози та забезпечити справедливе й ефективне правосуддя. Важливими аспектами є довіра до технологій, збереження незалежності суддів та дотримання європейських стандартів у використанні ШІ.

Звіти Агентства Європейського Союзу з основних прав (FRA) за 2020 та 2022 роки [2; 3] підкреслюють проблему упередженості алгоритмів ШІ, що може призводити до дискримінаційних наслідків. Вони наголошують на необхідності врахування основних прав людини у розробці та застосуванні технологій ШІ. У звітах аналізується вплив систем ШІ на соціальні, економічні та правові аспекти, зокрема у сфері правосуддя. Також підкреслюється важливість контролю за використанням ШІ для запобігання порушенням прав людини.

Європейська комісія з ефективності правосуддя (CEPEJ) активно досліджує вплив цифрових технологій, зокрема ШІ, на судову систему. У лютому 2025 року CEPEJ оприлюднила 1-й звіт про ШІ у судовій системі, який базується на даних з Ресурсного центру CEPEJ з кіберюстиції та ШІ [4]. Цей звіт аналізує впровадження ШІ у судову систему Європи, висвітлює основні можливості та виклики, пов'язані з використанням ШІ у судочинстві, зокрема у контексті автоматизації судових процесів, поліпшення ефективності правосуддя та забезпечення доступу до правосуддя. Звіт також розглядає питання етики, прозорості та потенційного впливу ШІ на права людини у судовій практиці.

Ці дослідження є важливою основою для подальшого аналізу правових стандартів у судовій практиці, пов'язаних з використанням ШІ, а також застосування систем та засобів ШІ у судочинстві.

Метою цієї статті є аналіз рішень ЄСПЛ, в яких безпосередньо чи опосередковано згадується ШІ, а також перевірка гіпотези, згідно з якою однією з основних проблем, пов'язаних зі ШІ у практиці ЄСПЛ, є захист і обробка персональних даних та втрата контролю над ними, що може призвести до констатації порушень за статтею 8 Європейської конвенції з прав людини «Право на повагу до приватного і сімейного життя».

Перша складність, з якою стикається дослідник, що починає вивчати ШІ, полягає в труднощах визначення понятійного апарату цього явища, неоднозначності трактування ключових термінів та неясності їх меж. Це зумовлено, з одного боку, новизною проблеми та недостатньою розробленістю цього феномену, а з іншого – його багатовимірністю й різноманітністю. Першою відомою підтвердженою згадкою про «ШІ» є наукова пропозиція, підготовлена та опублікована Дж. Маккарті, М. Мінські, Н. Рочестерем і К. Шенноном під назвою «Пропозиція до Дартмутського літнього дослідницького проекту з штучного інтелекту» (DSRPAI) у 1956 році [5]. Незважаючи на те, що термін «штучний інтелект» почав використовуватися в науці майже 70 років тому і про нього написано безліч наукових праць технічного, гуманітарного профілю та міждисциплінарного характеру, а майже 1/3 держав-членів ООН ухвалили національні закони та стратегії щодо використання ШІ, це поняття досі трактується по-різному.

Рада Європи неодноразово підкреслювала важливість взаємодії між ШІ та правами людини, поставивши перед собою завдання розробити рекомендації щодо посилення захисту прав людини у контексті використання ШІ. Вже за відносно короткий період Рада Європи досягла значного прогресу у цій сфері. Протягом останніх десяти років розроблено низку стандартів, починаючи з Резолюції Парламентської асамблеї Ради Європи (надалі – ПАРЕ) № 2051 (2015) «Дрони і цілеспрямовані вбивства: необхідність відстоювати права людини і міжнародне право» [6] та Рекомендації ПАРЕ № 2102 (2017) «Технологічна конвергенція, штучний інтелект і права людини» в 2017 році [7], а також ухвалено кілька міжнародно-правових документів, які стосуються ШІ. Одним із останніх важливих досягнень стало прийняття Комітетом Міністрів Рамкової конвенції Ради Європи щодо штучного інтелекту, прав людини, демократії та верховенства права 17 травня 2024 року [8] та відкриття конвенції для підписання в рамках неформальної конференції міністрів юстиції у м. Вільнюс 5 вересня 2024 року

під егідою Литовського головування в Комітеті Міністрів. Конвенція має на меті забезпечити, щоб розробка та використання технологій ШІ відповідали основним правам людини, демократичним цінностям та верховенству права, відповідаючи на такі ризики, як дезінформація, алгоритмічна дискримінація та загрози для державних установ. Принагідно варто звернути увагу, що моніторинг впливу цих та інших актів Ради Європи на права людини в рамках зобов'язань держав-членів щодо дотримання Конвенції про захист прав людини і основоположних свобод (надалі – ЄКПЛ, Конвенція) залишається в компетенції ЄСПЛ.

Обговорення ШІ часто пов'язане з ідеєю надінтелекту або суперінтелекту, який перевершить людський інтелект. Боснійська правозахисниця та Комісар Ради Європи з прав людини (2018–2024) Дуня Міятович, підтримуючи позицію, що наразі немає узгодженого визначення терміна «ШІ», визначає ШІ як «загальний термін, що охоплює набір наук, теорій і технік, спрямованих на покращення здатності машин виконувати завдання, що вимагають інтелекту. Система ШІ – це машинна система, яка робить рекомендації, прогнози або приймає рішення для заданого набору цілей. Це досягається шляхом: (i) використання машинних та/або людських входів для сприйняття реальних і/або віртуальних середовищ; (ii) абстрагування цих сприйнять у моделі вручну або автоматично; та (iii) отримання результатів з цих моделей чи то за допомогою людини, чи автоматизованими засобами у вигляді рекомендацій, прогнозів або рішень» [9, р. 5]. Організація економічного співробітництва та розвитку (OECD), а також Європейський Союз надають свої визначення цього явища [10; 11].

Науковці також працюють над різними підходами до визначення ШІ. Оскільки технології активно розвиваються, нині дуже складно, а подекуди й неможливо створити єдине загальне визначення, оскільки ШІ охоплює безліч термінів, таких як «великі дані», «машинне навчання», «глибоке навчання», «сильний та слабкий ШІ» тощо.

Основною проблемою цих визначень є їхня нечіткість і постійні зміни у змісті дефініцій. Це означає, що для потенційної цільової аудиторії (права якої можуть бути порушені) ШІ може включати як суперкомп'ютери, які використовуються для розв'язання складних наукових та інженерних задач, так і розумну техніку для дому чи дрони, оснащені ШІ. Сильний ШІ має на меті досягти рівня інтелекту людини, який здатний до самонавчання та творчого мислення, проте його розробка наразі залишається лише теоретичною концепцією. Реальна проблема полягає в тому, що навіть передові фахівці у сфері ШІ та правозахисники мають обмежене уявлення про те, де закінчується «глибоке навчання» і де починається концепція «надінтелекту».

Важко не погодитися з тим, що, як зауважує у своєму звіті Агентство Європейського Союзу з основних прав (FRA), «ШІ вже відіграє роль у визначенні, яку допомогу по безробіттю отримає особа, де ймовірно відбудеться крадіжка, чи є у когось ризик раку, або хто побачить ту привабливу рекламу на низькі ставки за іпотекою. Його використання постійно зростає, відкриваючи майже безмежні можливості. Однак ми повинні забезпечити повне дотримання стандартів основних прав у разі використання ШІ» [2]. Таким чином, показник використання ШІ може впливати на інтенсивність порушень прав людини, що виникають через нього. Якщо ми приймаємо позицію, що ШІ ще не досяг рівня «надрозуму» і лише «відіграє роль у прийнятті людських рішень», то порушення прав людини, ймовірно, ставатимуть результатом використання ШІ як інструменту та методу розв'язання завдання. У такому разі ЄСПЛ буде значно простіше визначити порушника і змусити його компенсувати шкоду потерпілій стороні. Однак ситуація стає значно складнішою, коли прийняття рішень повністю переходить до ШІ, оскільки в такому випадку важко визначити, хто є відповідальним: розробник системи ШІ, користувач чи, можливо, сам «суперінтелект».

Розглядаючи практику ЄСПЛ за статтею 8 Конвенції, що гарантує право на повагу до приватного і сімейного життя, можна припустити, що це основне право, яке може бути порушене за допомогою систем та засобів ШІ, особливо в контексті проблем, пов'язаних із захистом персональних даних та втратою контролю над ними.

Посібник із судової практики ЄСПЛ під назвою «Захист даних», станом на 31 серпня 2024 року, у розділі «Технологічний прогрес, алгоритми та штучний інтелект» визначає десять основних рішень ЄСПЛ, присвячених технологічному прогресу, алгоритмам та ШІ [12]. Усі вони були ухвалені після 2008 року, що свідчить про те, що технологічний прогрес став проблемою для прав людини у другому

десятилітті XXI століття. Всі ці рішення Суду, крім одного (буде зазначено нижче), не містять прямих згадок про ІІІ.

У справах «S. та Marper проти Сполученого Королівства», № 30562/04 та № 30566/04, § 112, рішення Великої Палати від 4 грудня 2008 року (це рішення є одним із найстаріших у контексті використання ІІІ) та «Подчасов проти Росії», № 33696/19, § 62, рішення від 13 лютого 2024 року, що стосуються збору, зберігання та використання органами влади біометричних персональних даних, відбитків пальців, біологічних зразків і профілів ДНК осіб, підозрюваних або засуджених за вчинення злочинів, без достатніх гарантій захисту від зловживань та обмеження термінів зберігання після припинення кримінального провадження, Суд чітко зазначив, що використання новітніх наукових методів повинно бути обґрунтованим та не повинно порушувати права людини. Для досягнення такого балансу необхідно враховувати потенційні переваги та ризики широкого застосування цих методів, зокрема у сфері захисту приватного життя. «Будь-яка Держава, яка претендує на роль першопрохідця в розвитку нових технологій, несе особливу відповідальність за дотримання правильного балансу в цьому відношенні» [12, с. 106]. Суд також підкреслив, що розвиток генетичних та інформаційних технологій може призвести до нових загроз для приватності, тому необхідно ретельно оцінювати можливі наслідки для прав людини (§ 71). Суд визнав, що автоматична обробка даних (яка є ключовою характеристикою ІІІ – *автори*) потребує більш суворих заходів захисту, ніж це передбачено зазвичай (§ 103).

У справі «Gaughan проти Сполученого Королівства», № 45245/15, § 70, рішення від 13 лютого 2020 року, заявник оскаржував зберігання його фотографій та інших біометричних даних після того, як його судимість була погашена, Суд зазначив, що «стрімкий розвиток все більш досконалих технологій, що дозволяють, серед іншого, застосовувати до фотографій фізичних осіб методи розпізнавання і відображення обличчя, робить проблематичним фотографування осіб, а також зберігання і можливе поширення отриманих даних» [12, с. 106]. Національні суди мають враховувати ці нові реалії під час розгляду питань втручання у приватне життя особи. Суд наголосив, що сучасні технології є більш складними, що національні суди не приділили достатньої уваги цьому аспекту під час розгляду питання про необхідність втручання у право на повагу до приватного життя заявника, фотографія якого була зроблена органами влади після незначного правопорушення та зберігалася навіть після того, як його судимість була видалена з обліку після спливу строку, встановленого законом (§§ 96–98).

У справі «Breuer проти Німеччини», № 50001/12, § 88, рішення від 30 січня 2020 року, заявники скаржилися на обов'язкову реєстрацію для передплатених SIM-карт, що порушує їхнє право на приватність, Суд визнав, що в контексті боротьби з організованою злочинністю та тероризмом сучасні засоби телекомунікацій та зміни в комунікативній поведінці вимагають адаптації слідчих засобів. На думку Суду, вимога до операторів мобільного зв'язку зберігати дані та надавати їх за запитом органів влади є адекватною відповіддю на зміни в комунікаційних технологіях [13, § 88]. Незважаючи на те, що ця справа напряду не стосується систем, засобів та безпосередньо ІІІ, ми вважаємо цю справу важливою для практики ЄСПЛ саме в контексті зберігання великих обсягів даних.

Як слушно зазначив у своїй окремій думці суддя ЄСПЛ від Ліхтенштейну Карло Ранцоні, «наявні гарантії зовсім не є достатніми для ефективного запобігання зловживанню та використанню в неналежний спосіб величезних обсягів персональних даних, що я вважаю набагато більш важливим, ніж мої колеги з Палати. Тому я вважаю, що втручання в права заявника за статтею 8 не було пропорційним до досягнутих легітимних цілей, зокрема тому, що національне законодавство не обмежувалося заходами проти тероризму або інших тяжких злочинів чи питаннями національної безпеки, а фактично виходило далеко за межі цього. Втручання не відповідало «нагальній соціальній потребі» і, відповідно, не було необхідним у демократичному суспільстві» [13, § 26].

У вищезгаданій справі «Подчасов проти Росії», № 33696/19, §§ 70–79, рішення від 13 лютого 2024 року, Суд також розглядав випадок, коли національне законодавство вимагало від постачальників послуг інтернет-зв'язку зберігати зміст усіх інтернет-комунікацій протягом шести місяців, а також надавати правоохоронним органам доступ до збережених даних на їхню вимогу разом з інформацією, необхідною для розшифрування електронних повідомлень. Суд був вражений надзвичайно широким обов'язком зберігати інформацію та визнав таке втручання надзвичайно широкомасштабним і серйозним. Суд також зазначив, що, згідно з національним законодавством, правоохоронні органи не зобов'язані пред'являти судовий дозвіл відповідному постачальнику послуг зв'язку перед отриманням доступу

до комунікацій певної особи. Фактично постачальники послуг зв'язку були зобов'язані встановити обладнання, яке надавало б зазначеним органам прямий доступ до даних, що зберігаються. Хоча в такій системі необхідність захисту від свавілля та зловживань була особливо великою, національне законодавство не передбачало таких гарантій. Що стосується законодавчої вимоги розшифровувати повідомлення, то здається, що будь-які такі заходи не будуть обмежуватися конкретними особами й послаблять шифрування для всіх користувачів, таким чином впливаючи на всіх без винятку, включаючи осіб, які не становлять загрози законним інтересам; отже, такі заходи, на думку Суду, є непропорційним втручанням у права людини [12, с. 107].

У справі «Роман Захаров проти Росії», № 47143/06, §§ 229, 302–305, рішення Великої Палати від 04 грудня 2015 року, заявник стверджував, що «система таємного перехоплення мобільного телефонного зв'язку в Росії порушила його право на повагу до приватного життя та кореспонденції». Суд постановив, що ризик зловживань, притаманний будь-якій системі таємного спостереження, був особливо високим у системі, де спецслужби та поліція мали прямий доступ за допомогою технічних засобів до всіх мобільних телефонних комунікацій. Суд визнав порушення статті 8, вважаючи, що російське законодавство, яке дозволяє загальне перехоплення комунікацій, не забезпечує адекватних та ефективних гарантій проти свавілля і ризику зловживань, притаманних будь-якій системі таємного спостереження [12, с. 107]. Як і в попередніх рішеннях, ШІ прямо не згадується, але технологічний прогрес враховувався як важливий фактор: «Вкрай важливо мати чіткі, детальні правила щодо перехоплення телефонних розмов, особливо зважаючи на те, що доступні для використання технології постійно ускладнюються» (§ 229).

У справі «Szabó та Vissy проти Угорщини», № 37138/14, §§ 68, 73–89, рішення від 12 січня 2016 року, заявники подали скаргу за статтями 8, 13 і 6 ЄКПЛ проти уряду Угорщини, стверджуючи, що одна з форм масового спостереження за комунікаціями, дозволена національним законом, була «необґрунтованою і непропорційно інвазивною». Без прямої згадки про ШІ Суд врахував технологічні фактори та взаємодію з великими обсягами даних під час ухвалення рішення. Суд визнав, що природним наслідком форм, які набуває сучасний тероризм, є те, що уряди вдаються до новітніх технологій, включаючи масовий моніторинг комунікацій, з метою запобігання неминучим атакам. У цій справі Суд постановив, що законодавство, яке дозволяє масове спостереження, не забезпечує необхідних гарантій проти зловживань, оскільки нові технології дозволяють владі легко перехоплювати великі обсяги даних, що стосуються навіть осіб, які не належать до категорії, на яку спочатку була спрямована операція. Більше того, заходи такого роду можуть бути призначені виконавчою владою без будь-якого контролю і без будь-якої оцінки того, чи були вони дійсно необхідними, а також за відсутності будь-якого ефективного судового або іншого засобу правового захисту [14, §§ 68, 73–89]. Основний аргумент Суду полягав у тому, що в угорській правовій системі було не досить гарантій, тому порушення було визнано одноголосно. За статтями 6 та 13 Конвенції Суд порушення не встановив.

Попри те, як зазначив у своїй окремій (збіжній) думці суддя ЄСПЛ від Португалії Пауло Пінто де Альбукерке [14, §§ 1–2], Палата в цьому рішенні відхилилася від підходу Великої Палати, ухваленого у справі «Роман Захаров проти Росії», особливо в питаннях необхідності заходів таємного спостереження та рівня підозри щодо осіб, за якими воно проводиться. Суддя підкреслив, що використання загальної «індивідуальної підозри» є занадто нечітким і дозволяє надмірне втручання в права людини без належних гарантій, що може призвести до зловживань і порушень основних прав, таких як право на приватність, що суперечить підходу Великої Палати, яка наголошувала на більш строгих вимогах до підозри та судового контролю.

У справі «Akgün проти Туреччини», № 19699/18, §§ 178–181, рішення від 20 липня 2021 року, заявник скаржився на порушення його права на свободу та особисту недоторканність через незаконне збирання та зберігання даних про його комунікації. Під час початкового досудового ув'язнення заявника висновок про те, що він використовував зашифровану систему обміну повідомленнями ByLock, був єдиним доказом, який був наданий для обґрунтування підозри у скоєнні ним злочину, Суд підкреслив, що використання таких доказів як єдиної підстави для підозри може викликати низку делікатних питань, оскільки за своєю природою процедура і технології, застосовані під час збору цих доказів, були складними і, відповідно, могли зменшити здатність національних судів встановити їх автентичність, точність і цілісність [12, с. 107–108].

У справах «Centrum för rättvisa проти Швеції», № 35252/08, § 261 та «Big Brother Watch та інші проти Сполученого Королівства», № 58170/13 62322/14 24960/15, §§ 322–323 два рішення Великої Палати від 25 травня 2021 року, заявники скаржилися на масове збирання та зберігання персональних даних без належного нагляду і контролю, а також протестували проти програм масового спостереження, що порушують їхнє право на приватність, Суд прямо визнав, що використання режиму масового перехоплення саме по собі не суперечить статті 8 Конвенції, зважаючи на поширення загроз, з якими наразі стикаються Держави від міжнародних мереж ворожих акторів державних чи недержавних, що використовують Інтернет для спілкування, а також на існування дедалі більш складних технологій, що дають змогу цим суб'єктам спілкуватися, не будучи виявленими. Однак Суд наголосив, що з огляду на постійний розвиток сучасних комунікаційних технологій, його звичайний підхід до режимів цільового спостереження повинен бути адаптований для відображення специфічних особливостей режиму масового перехоплення з огляду на ризик зловживання повноваженнями на масове перехоплення і законну необхідність дотримання таємниці в таких операціях. Зокрема, цей процес повинен був підпадати під дію «наскрізних гарантій», що означає, що на національному рівні на кожному етапі процесу повинна проводитися оцінка необхідності та пропорційності вжитих заходів; що на масове перехоплення із самого початку має надаватися незалежний дозвіл, якщо об'єкт і масштаби операції визначені; і що за операцією має здійснюватися нагляд і незалежний розгляд *ex post facto* [12, с. 108].

У справі «Глухін проти Росії», № 11519/20, §§ 86, 88–90, рішення від 04 липня 2023 року, заявник скаржився на порушення його права на приватність та свободу вираження поглядів через незаконне перехоплення та зберігання його комунікацій. Суд уперше розглянув питання використання поліцією технології розпізнавання обличчя. Ця технологія була застосована для ідентифікації заявника за фотографіями та відео, опублікованими на публічному каналі Telegram, а також для його розшуку та арешту під час поїздки в метрополітені. Суд відзначив «дуже інтрузивний характер цих заходів», зазначивши, що для того, щоб такі методи вважалися «необхідними в демократичному суспільстві», необхідне досить вагоме обґрунтування, причому найвищі вимоги обґрунтування ставляться до використання технології розпізнавання обличчя в реальному часі. Суд також підкреслив, що заявник був притягнутий до відповідальності за незначне правопорушення, що полягало в проведенні одиночної демонстрації без попереднього повідомлення, без будь-яких обвинувачень у вчиненні серйозних правопорушень під час демонстрації, таких як перешкоджання транспорту, пошкодження майна чи насильство. У таких обставинах Суд вирішив, що використання технології розпізнавання обличчя для ідентифікації заявника та його розшуку й арешту не відповідало «нагальній суспільній потребі» і не могло бути визнано «необхідним у демократичному суспільстві» [12, с. 108]. Суд констатував порушення статей 8 та 10 Конвенції.

Станом на березень 2025 року, згідно з базою даних Суду HUDOC, у практиці ЄСПЛ є лише три рішення, в яких прямо згадується словосполучення «штучний інтелект» (*англ.* artificial intelligence), але Посібник з прецедентного права Суду [12] їх не згадує.

У справі «**Sigurður Einarsson та інші проти Ісландії**», № 39757/15, рішення від 4 червня 2019 року, Суд розглядав питання законності збору і обробки персональних даних. Заявники стверджували, що їхні права, згідно зі статтями 6 та 8 Конвенції, були порушені. ШІ згадувався в контексті статті 6 Конвенції, частини 1 та 3(b) і (d). За словами заявників, у кримінальному провадженні проти них їм було відмовлено у повному доступі до справи, що була в обвинувачення, доступ було надано лише до частини «документів розслідування», виявлених системою електронного виявлення під назвою «Clearwell». Хоча Суд не визнав порушення ЄКПЛ, суддя ЄСПЛ від Албанії Даріан Павлі опублікував частково розбіжну окрему думку, що стосується цього питання. За його словами, ЄСПЛ у цій справі «вибравши обхід тесту Van Wesenbeeck (метод, який використовується для оцінки порушення прав людини ЄСПЛ, – *автори*) на користь глобальної констатації, що загальна справедливість судового процесу не була порушена, рішення чинить ведмежу послугу ясності та послідовності нашої судової практики та упускає можливість висловитися щодо складних питань на перехресті нових технологій і проблем з великою кількістю доказів» [15, § 4]. Він звернув увагу на те, що технологічний прогрес може поставити під сумнів загальноприйняті принципи, зокрема принцип рівності сторін. Суд одноголосно визнав порушення частини 1 статті 6 Конвенції, відхиливши інші скарги.

Загалом, суддя Павлі у своїй окремій думці згадує ШІ кілька разів, зазначивши, що «суди принаймні двох юрисдикцій (Сполученого Королівства та Ірландії) схвалили використання технологічно-асистованого огляду документів, використовуючи форму ШІ, відому як предиктивне кодування, для цілей електронного розкриття інформації в значних цивільних судових процесах» [15, § 15], що також може застосовуватися до кримінальних справ з подібною складністю. Суддя підкреслює «складність аналізу великих та взаємопов'язаних обсягів даних розслідування, незалежно від того, чи використовує людина «лише» людський інтелект, чи їй допомагає ШІ [15, § 21].

У справі **«Verein Klimaseniorinnen Schweiz та інші проти Швейцарії»**, № 53600/20, рішення Великої Палати від 09 квітня 2024 року, Суд розглянув питання використання технологій для моніторингу і контролю за публічними протестами, зокрема для виявлення та ідентифікації осіб, що беруть участь у демонстраціях. ШІ згадується у пункті 181, де зазначається, що Комітет з економічних, політичних, соціальних та культурних прав ООН у своєму Зауваженні загального порядку № 25 (2020) про науку та економічні, соціальні та культурні права (пункти 1 b), 2, 3 та 4 статті 15 Міжнародного пакту про економічні, соціальні та культурні права) підкреслив важливість міжнародної співпраці для вирішення найбільших глобальних ризиків, пов'язаних з наукою та технологіями, «таких як зміна клімату, швидка втрата біорізноманіття, розробка небезпечних технологій, таких як автономна зброя на основі штучного інтелекту, або загроза зброї масового знищення, зокрема ядерної зброї...» [16, § 181]. Хоча конкретно ШІ у справі більше не згадувався, Суд розглядав питання застосування новітніх технологій для розпізнавання осіб і збору інформації, що потенційно могли б включати алгоритми ШІ для розпізнавання облич. Суд зазначив, що використання таких технологій має бути обмежене і ретельно регламентоване, щоб уникнути порушень права на приватність, і застеріг від надмірного застосування автоматизованих систем без належних гарантій для захисту прав людини.

У справі **«Călin Georgescu проти Румунії»**, № 37327/24, ухвала щодо неприйнятності від 11 лютого 2025 року, заявник – кандидат у президенти Румунії Келін Джорджеску подав скаргу у зв'язку з рішенням Конституційного суду Румунії скасувати результати першого туру президентських виборів. Заявник посилався на статті 6, 10, 11 та 13 Конвенції та статтю 3 Протоколу 1 до Конвенції.

Конституційний суд зазначив, що президентський виборчий процес був порушений на всіх етапах, спотворюючи свободу голосування громадян і порушуючи правила фінансування виборчої кампанії. Він підкреслив важливість дотримання Конституції Румунії та законодавства, а також позитивне зобов'язання держави і її нейтралітету, посилаючись на «Тлумачну декларацію Кодексу належної практики у виборчих справах щодо цифрових технологій та штучного інтелекту», прийнятій Венеціанською комісією на 141-й пленарній сесії (Венеція, 6–7 грудня 2024 року), Конституційний суд також вказав на порушення права виборців на точну інформацію та захист від маніпуляцій, зокрема через агресивне просування кандидатами своїх повідомлень за допомогою алгоритмів масмедіа-платформ, переважно китайської соцмедійної платформи TikTok, що обійшло виборче законодавство і призвело до дезінформації. Крім того, Конституційний суд відзначив порушення принципу прозорості фінансування кампанії, оскільки один із кандидатів заявив про відсутність витрат, що суперечило даним аналізу.

ЄСПЛ не знайшов порушення статей 6, 13 Конвенції та статті 3 Протоколу 1 до Конвенції. Щодо можливого порушення статей 10 та 11 Конвенції Суд зазначив, що заявник не висунув жодних фактичних та юридичних аргументів на підтримку своїх скарг [17].

У будь-якому випадку в контексті цієї справи варто звернути увагу на «Тлумачну декларацію Кодексу належної практики у виборчих справах щодо цифрових технологій та штучного інтелекту» (2024) (надалі – Декларація) [18]. Декларація розглядає принципи, які мають бути дотримані в умовах впровадження новітніх технологій, зокрема цифрових технологій та ШІ, у виборчі процеси. Вона наголошує на важливості забезпечення прозорості, рівності та справедливості виборчих кампаній, захисту прав виборців і забезпечення демократичних принципів у разі використання цих технологій. Декларація підкреслює необхідність законодавчого регулювання для запобігання маніпуляціям, зокрема через алгоритми на платформах соціальних мереж, а також закликає до посилення міжнародної співпраці для розробки та імплементації етичних стандартів у цьому контексті.

Ми переконані, що Декларація може бути корисною для майбутньої практики Суду, оскільки надає орієнтири для тлумачення питань, пов'язаних з використанням цифрових технологій та ШІ у виборчих процесах. Вона може допомогти Суду оцінювати випадки, коли ці технології порушують

права людини, зокрема право на вільні вибори, згідно зі статтею 3 Першого протоколу до Конвенції. Рекомендації та принципи Декларації можуть слугувати важливим інструментом для забезпечення дотримання прав людини в умовах цифровізації та розвитку інформаційних технологій, які впливають на демократичні процеси.

Оглядаючи рішення, зазначені в Посібнику із судової практики ЄСПЛ – «Захист даних», можна зробити кілька проміжних висновків. Жодне з рішень, що наведені в розділі «Технологічний прогрес, алгоритми та штучний інтелект», не містить прямого посилання на ШІ. У більшості рішень Суд відзначає технологічний прогрес не як проблему чи загрозу для прав людини, а як фактор, який слід враховувати у разі створення механізмів захисту прав людини, зокрема для забезпечення приватного життя.

Більшість порушень Судом встановлено за статтею 8 Конвенції. Крім того, на додаток до встановлення порушення права на повагу до приватного і сімейного життя Суд також знайшов порушення статей 5 («Akgün проти Туреччини») та 10 («Big Brother Watch та інші проти Сполученого Королівства» і «Глухін проти Росії») Конвенції. Стверджуване заявниками порушення статті 6 було детально розглянуто Судом у справах «Szabó та Vissy проти Угорщини» та «Глухін проти Росії», однак ЄСПЛ дійшов висновку, що немає необхідності розглядати ці скарги щодо статті 6 Конвенції. Нам видається необачним припускати, що справи, пов'язані з ШІ, в практиці Суду так чи інакше зосереджені навколо статті 8 Конвенції. Право, гарантоване статтею 8, є інтегрованим та багатоаспектним правом, яке охоплює кілька аспектів приватного життя. Як підкреслив Суд у своєму рішенні у справі «Breuer проти Німеччини», стаття 8 захищає, зокрема, «право на ідентичність і особистий розвиток, а також право встановлювати та розвивати стосунки з іншими людьми та із зовнішнім світом» [13, § 73].

Наявний стан речей дає підстави для констатації того, що основним контекстом, в якому може фігурувати ШІ та термінологія, що з ним пов'язана («великі дані», «машинне навчання», «глибоке навчання», «сильний та слабкий ШІ» тощо), в прецедентному праві Суду, є судові рішення у сфері захисту і обробки персональних даних та втрати контролю над ними, збирання, зберігання, використання і поширення інформації про приватне життя фізичної особи.

Зрештою, вістря проблеми цим не обмежується, практика Суду у справах «Sigurður Einarsson та інші проти Ісландії», «Verein Klimasenioren Schweiz та інші проти Швейцарії», а також «Călin Georgescu проти Румунії» дозволяє припустити з тією чи іншою мірою ймовірності, що системи та засоби ШІ в найближчому майбутньому можуть зачіпати не одне право, гарантоване Конвенцією, а кілька, зокрема право на свободу та особисту недоторканність, право на справедливий суд, право на свободу вираження поглядів.

Насамкінець варто особливо відзначити, що ЄСПЛ вкрай рідко використовує лексему «штучний інтелект» (англ. *artificial intelligence*). З урахуванням лексики судової практики, наукових джерел та їх інтерпретацій під час роботи з інформаційно-пошуковою базою даних HUDOC, щоб знайти відповідні рішення Суду щодо застосування ШІ, ми радимо для подальших наукових розвідок у цьому напрямі комбінувати такі ключові слова: *artificial intelligence, AI, algorithm, machine learning, data protection, privacy, personal data, surveillance, data processing, automated decision-making, digital technologies, privacy rights, transparency, freedom of expression, right to a fair trial, digital rights*.

Отже, з викладеного вище можна дійти кількох висновків.

Після узагальнення пошуку та аналізу результатів можна зробити висновок, що до цього часу ЄСПЛ не розглядав справ, безпосередньо пов'язаних із ШІ, хоча ШІ, безперечно, може стосуватися кількох прав, захищених Конвенцією, зокрема статтями 8, 5–6 та 10. За результатами проведеного узагальнення судової практики ЄСПЛ ми не знайшли рішень (та ухвал) Суду, у яких ШІ було б визнано порушником прав без людського втручання. Рішення ухвалювали державні або правоохоронні органи держав-учасниць Конвенції; ШІ ніколи не діяв автономно, приймаючи рішення без втручання людини. У практиці Суду ШІ розглядається виключно як інструмент і метод прийняття рішень, система та засіб виконання завдань, які зазвичай потребують людського інтелекту.

Попри те, що науковці й практики зазначають, що система захисту прав людини перебуває під загрозою через стрімкий розвиток ШІ, ми знайшли лише нечисленні згадки про цю проблему в практиці та рішеннях Суду. Проте це не означає, що з часом Суду не доведеться частіше розглядати справи, пов'язані із ШІ, оскільки він дедалі більше проникає в наше життя та має величезний потенціал для

розвитку. Це може вимагати зміцнення міжнародної співпраці держав-учасниць Конвенції, що сприятиме посиленню ефективності правового регулювання.

Апостеріорним підтвердженням такого стану речей може слугувати введення в дію 2 серпня 2024 року Акта про штучний інтелект (EU Artificial Intelligence Act) Європейського Союзу, Регламент (ЄС) № 2024/1689 [11]. Нормативний акт, ухвалений 13 березня 2024 року Європейським парламентом, набрав чинності 1 серпня 2024 року, ставши обов'язковим для всіх держав-членів ЄС та Ради Європи, що перебувають під юрисдикцією ЄСПЛ. З огляду на час, необхідний для адаптації індустрії, підготовки національних урядів та розробки нормативної бази, яка забезпечить ефективне застосування цього Регламенту, найближчим часом можна очікувати, що фізичні та юридичні особи з юрисдикції держав-членів ЄС звертатимуться до ЄСПЛ, оскільки дотримання законодавства ЄС не буде виправданням для порушень прав людини, пов'язаних із використанням ШІ.

Міжнародна суддівська спільнота розглядає дедалі більше справ, пов'язаних із використанням систем і засобів ШІ. Хоча більшість таких справ розглядається у США та КНР, держави-члени Ради Європи, що перебувають під юрисдикцією ЄСПЛ, також уже мають рішення національних судів, пов'язані з технологіями ШІ. До того ж в Україні в Єдиному державному реєстрі судових рішень з'являється дедалі більше справ, що стосуються використання технологій ШІ.

У будь-якому разі ЄСПЛ навряд чи уникатиме справ, пов'язаних із ШІ, проте технології ШІ (слабкий ШІ), ймовірно, залишатимуться інструментом порушення прав людини, а не самим порушником – щонайменше до того часу, поки у сфері життя людини не увійдуть сильний ШІ, можливості якого вже не поступатимуться когнітивним здібностям людини, а за ним – «суперінтелект» або «надрозум».

REFERENCES

1. Artificial intelligence and human rights. *Council of Europe*. Retrieved from: <https://www.coe.int/en/web/artificial-intelligence/secretary-general-marija-pejcinovic-buric> (date of access: 31.03.2025).
2. Getting the future right – Artificial intelligence and fundamental rights. *European Union Agency for Fundamental Rights*. Retrieved from: <https://fra.europa.eu/en/publication/2020/artificial-intelligence-and-fundamental-rights> (date of access: 31.03.2025).
3. Bias in algorithms – Artificial intelligence and discrimination. *European Union Agency for Fundamental Rights*. Retrieved from: <https://fra.europa.eu/en/publication/2022/bias-algorithm> (date of access: 31.03.2025).
4. 1st AIAB Report on the use of Artificial Intelligence (AI) in the judiciary, based on the information contained in the CEPEJ's Resource Centre on Cyberjustice and AI. *European Commission for the Efficiency of Justice (CEPEJ)*. Retrieved from: <https://rm.coe.int/cepej-aiab-2024-4rev5-en-first-aiab-report-2788-0938-9324-v-1/1680b49def> (date of access: 31.03.2025).
5. Artificial Intelligence (AI) Coined at Dartmouth. *Dartmouth*. Retrieved from: <https://home.dartmouth.edu/about/artificial-intelligence-ai-coined-dartmouth> (date of access: 31.03.2025).
6. Resolution 2051 (2015) Drones and targeted killings: the need to uphold human rights and international law: *Parliamentary Assembly*. Retrieved from: <https://pace.coe.int/en/files/21746/html> (date of access: 31.03.2025).
7. Recommendation 2102 (2017) Technological convergence, artificial intelligence and human rights: *Parliamentary Assembly*. Retrieved from: <https://pace.coe.int/en/files/23726/html> (date of access: 31.03.2025).
8. Council of Europe Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law. *Council of Europe*. Retrieved from: <https://rm.coe.int/1680afae3c> (date of access: 31.03.2025).
9. Unboxing Artificial Intelligence: 10 steps to protect Human Rights. *Commissioner for Human Rights*. Retrieved from: <https://rm.coe.int/unboxing-artificial-intelligence-10-steps-to-protect-human-rights-reco/1680946e64> (date of access: 31.03.2025).
10. Recommendation of the Council on Artificial Intelligence. *OECD Legal Instruments*. Retrieved from: <https://legalinstruments.oecd.org/en/instruments/%20OECD-LEGAL-0449> (date of access: 31.03.2025).
11. Regulation – EU – 2024/1689. *EUR-Lex*. Retrieved from: <https://eur-lex.europa.eu/eli/reg/2024/1689/oj> (date of access: 31.03.2025).
12. Guide to the Case-Law of the of the European Court of Human Rights – Data protection. *Council of Europe / European Court of Human Rights*. Retrieved from: https://ks.echr.coe.int/documents/d/echr-ks/guide_data_protection_eng (date of access: 31.03.2025).
13. Case of Breyer v. Germany. *HUDOC – European Court of Human Rights*. Retrieved from: <https://hudoc.echr.coe.int/eng?i=001-200442> (date of access: 31.03.2025).
14. Case of Szabó and Vissy v. Hungary. *HUDOC – European Court of Human Rights*. Retrieved from: <https://hudoc.echr.coe.int/eng?i=001-160020> (date of access: 31.03.2025).
15. Case of Sigurður Einarsson and Others v. Iceland. *HUDOC – European Court of Human Rights*. Retrieved from: <https://hudoc.echr.coe.int/eng?i=001-193494> (date of access: 31.03.2025).

16. Case of Verein Klimaseniorinnen Schweiz and Others v. Switzerland. *HUDOC – European Court of Human Rights*. Retrieved from: <https://hudoc.echr.coe.int/eng?i=001-233206> (date of access: 31.03.2025).
17. Călin Georgescu v. Romania. *HUDOC – European Court of Human Rights*. Retrieved from: <https://hudoc.echr.coe.int/eng?i=001-242417> (date of access: 31.03.2025).
18. Interpretative declaration of good practice in electoral matters as concerns digital technologies and artificial technologies. *Venice Commission*. Retrieved from: [https://www.venice.coe.int/webforms/documents/default.aspx?pdffile=CDL-AD\(2024\)044-е](https://www.venice.coe.int/webforms/documents/default.aspx?pdffile=CDL-AD(2024)044-е) (date of access: 31.03.2025).

ВИКОРИСТАНІ МАТЕРІАЛИ

1. Artificial intelligence and human rights. *Council of Europe*. URL: <https://www.coe.int/en/web/artificial-intelligence/secretary-general-marija-pejcinovic-buric> (дата звернення: 31.03.2025).
2. Getting the future right – Artificial intelligence and fundamental rights. *European Union Agency for Fundamental Rights*. URL: <https://fra.europa.eu/en/publication/2020/artificial-intelligence-and-fundamental-rights> (дата звернення: 31.03.2025).
3. Bias in algorithms – Artificial intelligence and discrimination. *European Union Agency for Fundamental Rights*. URL: <https://fra.europa.eu/en/publication/2022/bias-algorithm> (дата звернення: 31.03.2025).
4. 1st AIAB Report on the use of Artificial Intelligence (AI) in the judiciary, based on the information contained in the CEPEJ's Resource Centre on Cyberjustice and AI. *European Commission for the Efficiency of Justice (CEPEJ)*. URL: <https://rm.coe.int/cepej-aiab-2024-4rev5-en-first-aiab-report-2788-0938-9324-v-1/1680b49def> (дата звернення: 31.03.2025).
5. Artificial Intelligence (AI) Coined at Dartmouth. *Dartmouth*. URL: <https://home.dartmouth.edu/about/artificial-intelligence-ai-coined-dartmouth> (дата звернення: 31.03.2025).
6. Resolution 2051 (2015) Drones and targeted killings: the need to uphold human rights and international law. *Parliamentary Assembly*. URL: <https://pace.coe.int/en/files/21746/html> (дата звернення: 31.03.2025).
7. Recommendation 2102 (2017) Technological convergence, artificial intelligence and human rights. *Parliamentary Assembly*. URL: <https://pace.coe.int/en/files/23726/html> (дата звернення: 31.03.2025).
8. Council of Europe Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law. *Council of Europe*. URL: <https://rm.coe.int/1680afae3c> (дата звернення: 31.03.2025).
9. Unboxing Artificial Intelligence: 10 steps to protect Human Rights. *Commissioner for Human Rights*. URL: <https://rm.coe.int/unboxing-artificial-intelligence-10-steps-to-protect-human-rights-reco/1680946e64> (дата звернення: 31.03.2025).
10. Recommendation of the Council on Artificial Intelligence. *OECD Legal Instruments*. URL: <https://legalinstruments.oecd.org/en/instruments/%20OECD-LEGAL-0449> (дата звернення: 31.03.2025).
11. Regulation – EU – 2024/1689. *EUR-Lex*. URL: <https://eur-lex.europa.eu/eli/reg/2024/1689/oj> (дата звернення: 31.03.2025).
12. Посібник із судової практики Європейського суду з прав людини – Захист даних. *Рада Європи / Європейський суд з прав людини*. URL: https://ks.echr.coe.int/documents/d/echr-ks/guide_data_protection_ukr (дата звернення: 31.03.2025).
13. Case of Breyer v. Germany. *HUDOC – European Court of Human Rights*. URL: <https://hudoc.echr.coe.int/eng?i=001-200442> (дата звернення: 31.03.2025).
14. Case of Szabó and Vissy v. Hungary. *HUDOC – European Court of Human Rights*. URL: <https://hudoc.echr.coe.int/eng?i=001-160020> (дата звернення: 31.03.2025).
15. Case of Sigurður Einarsson and Others v. Iceland. *HUDOC – European Court of Human Rights*. URL: <https://hudoc.echr.coe.int/eng?i=001-193494> (дата звернення: 31.03.2025).
16. Case of Verein Klimaseniorinnen Schweiz and Others v. Switzerland. *HUDOC – European Court of Human Rights*. URL: <https://hudoc.echr.coe.int/eng?i=001-233206> (дата звернення: 31.03.2025).
17. Călin Georgescu v. Romania. *HUDOC – European Court of Human Rights*. URL: <https://hudoc.echr.coe.int/eng?i=001-242417> (дата звернення: 31.03.2025).
18. Interpretative declaration of good practice in electoral matters as concerns digital technologies and artificial technologies. *Venice Commission*. URL: [https://www.venice.coe.int/webforms/documents/default.aspx?pdffile=CDL-AD\(2024\)044-е](https://www.venice.coe.int/webforms/documents/default.aspx?pdffile=CDL-AD(2024)044-е) (дата звернення: 31.03.2025).