Верховний
Суд

Гарантування права на приватність в умовах інтеграції ШІ у правосуддя

Ян БЕРНАЗЮК,
суддя Касаційного адміністративного суду у складі Верховного Суду,
доктор юридичних наук, професор

НАЦІОНАЛЬНА ШКОЛА СУДДІВ УКРАЇНИ
Проєкт Ради Європи «HELP (Освіта в галузі прав людини для представників юридичних професій) для України, у тому числі під час війни», Фаза II

Тьюторський курс HELP «Захист персональних даних при опублікуванні судових рішень»

17 березня 2026 року

ПЛАН

1. ШІ у правосудді: нова реальність і ризики для приватності
2. Як саме ШІ створює загрози приватності (технологічний аспект)
3. Європейська правова рамка (AI Act, CoE Convention, GDPR-тренди)
4. Судова практика: нові межі приватності
5. Український підхід: етика, регулювання, інституційні рішення
6. Soft law і стандарти для суддів
7. Практичні поради безпечної роботи з ШІ

Ukraine 2025 Report SWD(2025) 759 final
ЄК: Звіт щодо України за 2025 рік (04.11.2025)

https://enlargement.ec.europa.eu/document/download/17115494-8122-4d10-8a06-2cf275eecde7_en?filename=ukraine-report-2025.pdf

ЄС фіксує активне впровадження ШІ та e-justice в Україні, але відсутність гармонізації з AI Act

Захист персональних даних у судовій цифровізації залишається проблемним і потребує законодавчого оновлення

Судова цифровізація оцінюється ЄС через призму фундаментальних прав, а не лише ефективності

ШІ без належних гарантій приватності та контролю судової влади - ризик для верховенства права

Рекомендації з кіберзахисту інформаційно-комунікаційних систем, які використовують технології штучного інтелекту, затверджені наказом Адміністрації Держспецзв'язку від 23.02.2026 № 154

https://cip.gov.ua/ua/docs/nakaz-administraciyi-derzhspeczv-yazku-vid-23-02-2026-154-pro-zatverdzhennya-rekomendacii-z-kiberzakhistu-informaciino-komunikaciinikh-sistem-yaki-vikoristovuyut-tekhnologiyi-shtuchnogo-intelektu

Україна запровадила перші державні рекомендації з кіберзахисту систем, що використовують штучний інтелект, які визначають специфічні кіберзагрози для AI-систем, зокрема data poisoning, prompt injection, model inversion та model theft.

Документ підкреслює необхідність управління ризиками, контролю доступу, перевірки навчальних даних та використання методів диференціальної конфіденційності, щоб запобігти витоку персональних даних і компрометації моделей ШІ.

Українська національна LLM та “суверенний ШІ”

https://mezha.ua/news/ukrainian-llm-will-use-google-gemma-model-306690
https://thedigital.gov.ua/news/progress/pochynayemo-pratsiuvaty-z-nvidia-dlia-rozbudovy-suverennoho-shi-v-ukrayini

Україна створює національну LLM (Diia AI) як елемент цифрового суверенітету та нацбезпеки

Модель базується на Google Gemma 3 і призначена для державних сервісів та законодавчого контексту

Ключовий правовий виклик: які дані використовуються для навчання та донавчання моделей

Суверенний ШІ зменшує зовнішні ризики, але збільшує внутрішній ризик, якщо відсутні незалежний аудит і судовий контроль

Україна створює свій ChatGPT: Інтерв'ю з Мінцифри щодо національної LLM та AI-агентів (РБК-Україна, 16.03.2026).

https://www.rbc.ua/rus/news/ukrayina-stvoryue-sviy-chatgpt-chi-zaminit-1773144607.html

Коли ми пишемо запит до ChatGPT, то розуміємо, що там використовують хмарні рішення… а ваші персональні дані фактично йдуть за кордон. Для нас такий сценарій неможливий, особливо в напрямі оборони, охорони здоров'я, держсекторі.

У Дія.AI ми використовуємо технологію "маскування", завдяки якій AI працює лише зі знеособленими даними, а не з реальним ім'ям чи номером паспорта. Тобто всі дані передають лише захищеними каналами, а історії чатів надійно зашифровані унікальним ключем, доступ до якого має лише користувач під час сесії.

КОДЕКС СУДДІВСЬКОЇ ЕТИКИ (СТАТТЯ 16)

https://zakon.rada.gov.ua/rada/show/n0001415-24#Text

Використання суддею технологій штучного інтелекту є допустимим, якщо це:

1. не впливає на незалежність та неупередженість судді,
2. не стосується оцінки доказів,
3. не стосується процесу ухвалення рішень,
4. не порушує вимог законодавства.

Коментар до Кодексу суддівської етики, затверджений рішенням Ради суддів України від 04.05.2024 № 14

https://constitutionalist.com.ua/komentar-do-statti-16-vykorystannia-suddeiu-tekhnolohij-shi-kodeksu-suddivskoi-etyky

Використання ШІ не лише не повинно порушувати, а й має забезпечувати реалізацію конституційних прав і свобод людини і громадянина. Особливу увагу слід приділити праву на захист персональних даних та повагу до особистого і сімейного життя.

Важливо враховувати вимоги законів України “Про інформацію”, “Про доступ до публічної інформації”, “Про захист персональних даних”, “Про державну таємницю” та законодавства у сфері кібербезпеки. Це запобігатиме несанкціонованому доступу до даних, їх неправомірному використанню.

Коментар до Кодексу суддівської етики, затверджений рішенням Ради суддів України від 04.05.2024 № 14

https://constitutionalist.com.ua/komentar-do-statti-16-vykorystannia-suddeiu-tekhnolohij-shi-kodeksu-suddivskoi-etyky

Перед застосуванням будь-якого цифрового інструменту судді пропонується провести коротку етичну самооцінку та поставити собі, для прикладу, такі запитання:

1. чи використовую я ШІ виключно як допоміжний засіб, а не як джерело судження?;
2. чи надає мені ШІ інформацію про використані джерела?;
3. чи зберігаю я контроль над результатом роботи ШІ, зокрема можливість змінити або відхилити його відповідь?;
4. чи не містить відповідь ШІ упередження?

Рекомендації щодо відповідального використання систем штучного інтелекту для правників (Мінцифри)

https://constitutionalist.com.ua/rekomendatsii-z-vidpovidalnoho-vykorystannia-shtuchnoho-intelektu-dlia-pravnykiv

Правникам рекомендується уникати введення в системи ШІ персональних даних клієнтів, адвокатської таємниці тощо, оскільки більшість загальнодоступних моделей використовують вхідні дані для подальшого навчання без гарантій конфіденційності.

Під час використання інструментів штучного інтелекту необхідно враховувати ризики витоку даних та забезпечувати дотримання вимог законодавства про захист персональних даних.

ПОЛОЖЕННЯ ПРО ВИКОРИСТАННЯ ТЕХНОЛОГІЙ ШІ ПРАЦІВНИКАМИ АПАРАТУ ВС (Наказ від 08.12.25 № 117)

https://court.gov.ua/storage/portal/supreme/rizne/Polozhennya_SHI.pdf

Положення визначає загальні засади та правила використання технологій ШІ працівниками Апарату ВС з метою забезпечення дотримання принципів державної служби, зокрема професіоналізму, ефективності та доброчесності.

Апарат ВС підтримує розвиток та визнає значний потенціал технологій ШІ для оптимізації, а також для вдосконалення робочих процесів.

Інтеграція технологій ШІ в діяльність Апарату ВС та їх використання мають ґрунтуватися на фундаментальних принципах верховенства права, професійної етики, прозорості та поваги до прав і свобод людини.

ЗАБОРОНЯЄТЬСЯ ВИКОРИСТАННЯ ТЕХНОЛОГІЇ ШІ ДЛЯ:

1. Опрацювання документів, які містять відомості, що охороняються законом, у тому числі таємницю ухвалення судового рішення та інформацію із закритого судового засідання;
2. Аналізу та моніторингу поведінки працівників;
3. Спроб прогнозувати індивідуальні рішення суддів у конкретних справах;
4. Автоматичного створення проєктів рішень та будь-яких інших процесуальних документів, що ухвалюються у межах судового провадження;
5. Опрацювання матеріалів судової справи, що містять персональні дані.

ПРИНЦИП КОНФІДЕНЦІЙНОСТІ ТА БЕЗПЕКИ

1. Забороняється використовувати загальнодоступні технології ШІ для роботи з інформацією з обмеженим доступом (конфіденційною, таємною та службовою інформацією).
2. Забороняється завантажувати службові документи, які містять персональні дані суб'єктів звернення або учасників процесу, банківську таємницю, адвокатську таємницю тощо.
3. Використання загальнодоступних технологій ШІ дозволяється виключно для технічних, допоміжних або навчальних завдань, що не передбачають введення інформації з обмеженим доступом.
4. Особа повинна, наскільки це технічно можливо, відмовитися від надання дозволу на використання введених даних для подальшого навчання ШІ.

ШІ МОЖЕ ВИКОРИСТОВУВАТИСЯ ДЛЯ ТАКИХ РОБІТ:

1. Узагальнення судової практики з метою забезпечення її єдності;
2. Аналіз судових рішень з метою виявлення системних причин виникнення спорів;
3. Підготовки пропозицій щодо вдосконалення законодавства;
4. Аналіз та узагальнення великих обсягів даних на основі відкритих джерел інформації;
5. Допомога у підготовці аналітичних документів та звітів;
6. Автоматизація повторюваних робочих процесів;
7. Допомога у створенні та поширенні інформації про діяльність (ведення соціальних мереж);
8. Створення чат-ботів, зокрема, для забезпечення зворотного зв'язку з відвідувачами та учасниками судових процесів;
9. Добір матеріалів для саморозвитку, підвищення кваліфікації та професійного навчання;
10. Пошук нових ідей та підходів до організації робочих процесів;
11. Допомога у перекладі документів з іноземних мов.

Claude’s Constitution: Training AI via a system of principles https://www.anthropic.com/news/claudes-constitution

Конституція Claude: Навчання ШІ через систему принципів (Anthropic).

Технологія Constitutional AI дозволяє моделі самостійно оцінювати свої відповіді на відповідність набору правил (конституції), що включає принципи Декларації прав людини ООН та стандарти захисту приватності.

Ми визнаємо, що дослідження, пов’язані з навчанням, оцінюванням та використанням Claude, порушують етичні питання щодо того, якою мірою система може давати згоду на такі дослідження і як повинні враховуватися її інтереси.

Council of Europe Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law (CETS № 225).

https://www.coe.int/en/web/conventions/full-list2?module=treaty-detail&treatynum=225

Рамкова конвенція Ради Європи про штучний інтелект і права людини, демократію та верховенство права

Кожна Сторона повинна вжити або підтримувати заходи для забезпечення того, щоб під час діяльності протягом життєвого циклу систем штучного інтелекту були захищені права осіб на приватність та їхні персональні дані

Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence (AI Act) https://eur-lex.europa.eu/eli/reg/2024/1689/oj

Регламент (ЄС) 2024/1689 про встановлення гармонізованих правил щодо штучного інтелекту (Акт про ШІ) відносить до систем високого ризику AI-системи, призначені для використання у сфері здійснення правосуддя, зокрема ті, що можуть впливати на оцінку фактів або застосування права.

Основні регуляторні обов'язки (зокрема щодо управління ризиками, точності та кібербезпеки) покладаються на постачальників таких систем.

Водночас суди як користувачі (deployers) зобов'язані забезпечувати належний людський контроль, використовувати системи відповідно до їх призначення та враховувати ризики для прав і свобод осіб.

EU Parliament blocks AI features over cyber, privacy fears // POLITICO. 16 February 2026.

https://www.politico.eu/article/eu-parliament-blocks-ai-features-over-cyber-privacy-fears/

Європейський парламент відключив вбудовані AI-функції на службових планшетах та телефонах депутатів і персоналу.

Причина: неможливість гарантувати безпеку даних.

Частина функцій передавала дані до хмарних сервісів, хоча їх можна було обробляти локально.

Базові сервіси (email, документи, календар) не обмежені.

Депутатам рекомендовано уникати використання AI-функцій для обробки службової інформації навіть на приватних пристроях.

Brussels knifes privacy to feed the AI boom // POLITICO.

https://www.politico.eu/article/brussels-knifes-privacy-to-feed-the-ai-boom-gdpr-digital-omnibus

ЄК готує пакет “digital omnibus”, який передбачає:
внесення змін до General Data Protection Regulation (GDPR, Регламент (EU) 2016/679)
Нові винятки для AI-компаній щодо обробки даних про релігійні переконання, політичні погляди, етнічність, дані про здоров’я тощо.
Можливе звуження поняття “персональні дані” - псевдонімізовані дані можуть не завжди підпадати під захист.
Ослаблення правил щодо cookie-трекінгу - розширення підстав для відстеження без згоди.

DIGITAL OMNIBUS

Commission Staff Working Document accompanying the Proposal for a Regulation of the European Parliament and of the Council amending Regulations (EU) 2016/679, (EU) 2018/1724, (EU) 2018/1725, (EU) 2023/2854 and Directives 2002/58/EC, (EU) 2022/2555 and (EU) 2022/2557 as regards the simplification of the digital legislative framework, and repealing Regulations (EU) 2018/1807, (EU) 2019/1150, (EU) 2022/868, and Directive (EU) 2019/1024 (Digital Omnibus); Amending Regulations (EU) 2024/1689 and (EU) 2018/1139 as regards the simplification of the implementation of harmonised rules on artificial intelligence (Digital Omnibus on AI) 19.11.2025 SWD(2025) 836 final https://digital-strategy.ec.europa.eu/en/library/digital-omnibus-regulation-proposal

Gemini зможе використовувати дані з Gmail, історії Пошуку та YouTube для персоналізованих відповідей

https://mezha.ua/news/gemini-personal-intelligence-307752

Gemini отримує здатність одночасно аналізувати дані з різних сервісів екосистеми (Gmail, Photos, YouTube, Search) без прямої вказівки джерела. Це створює «цілісний цифровий портрет» користувача для надання контекстуальних відповідей.

Ця функція є суворо добровільною: доступ до персональних даних активується лише за ініціативи користувача. Для чутливих категорій (наприклад, стан здоров'я) діє заборона на автоматичні припущення - ШІ працює з такою інформацією виключно за прямим запитом.

Google заявляє про дотримання принципу цільового обмеження: використовує вміст Gmail або Photos лише для формування відповіді (не навчання).

Judgment of the Court (First Chamber) of 04.09.2025 European Data Protection Supervisor v Single Resolution Board (C-413/23 P)

https://infocuria.curia.europa.eu/tabs/affair?lang=FR&searchTerm=C-413%2F23+P&sort=SCORE-DESC

Суд встановив, що статус «персональних даних» не є абсолютним, а залежить від того, чи має конкретний отримувач інформації реальні та законні засоби для ідентифікації особи.

Якщо дані передані у формі, яка не дозволяє отримувачу розкрити особу без доступу до «ключа», що залишається у відправника, то для такого отримувача ці дані вважаються неперсоналізованими.

Це може полегшити залучення зовнішніх експертів до аналізу даних, оскільки знімає з них тягар регулювання GDPR у випадках, коли ідентифікація суб'єктів для них технічно та юридично неможлива.

Apple notches win with dismissal of data privacy class action

https://www.courthousenews.com/apple-notches-win-with-dismissal-of-data-privacy-class-action

Федеральний суд США (суддя Е. Давіла) відхилив колективний позов проти Apple. Користувачі вважали, що вимкнення опції «Share Device Analytics» повністю припиняє збір даних у фірмових застосунках (App Store, Music, TV). Суд назвав такі очікування «об’єктивно необґрунтованими».

Юридичний коментар: Суд дійшов висновку, що збір аналітики всередині екосистеми розробника відрізняється за ступенем втручання від того, що закон захищає як «reasonable expectation of privacy». Для судді це означає, що суб'єктивне сприйняття користувачем налаштувань не завжди створює юридичне зобов'язання для компанії.

Apple notches win with dismissal of data privacy class action

https://www.courthousenews.com/apple-notches-win-with-dismissal-of-data-privacy-class-action

Позивачі намагалися прирівняти збір метаданих Apple до використання «pen register» (засобу негласного стеження за маршрутизацією). Суд відхилив це, зазначивши, що цей термін стосується лише зовнішніх пристроїв перехоплення, а не внутрішніх журналів логів самого пристрою.

Юридичний коментар: Спроба застосувати норми кримінального права про стеження до цивільного збору аналітики визнана помилковою. Розширене тлумачення технологічних процесів як «засоби негласного отримання інформації» може призвести до, наприклад, криміналізації звичайних списків викликів у смартфонах).

Google settles Google Assistant privacy lawsuit for $68 million:

https://www.reuters.com/sustainability/boards-policy-regulation/google-settles-google-assistant-privacy-lawsuit-68-million-2026-01-26

Google погодилася на мирову угоду вартістю 68 млн дол. США через позови про порушення приватності. Ключова проблема - «false accepts» (помилкові спрацювання), коли ШІ-асистент записував приватні розмови без свідомої активації користувачем.

Юридичний аспект: Це демонструє, що джерелом порушення права на приватність є не злам системи, а недоліки її архітектури.

Google settles Google Assistant privacy lawsuit for $68 million:

https://www.reuters.com/sustainability/boards-policy-regulation/google-settles-google-assistant-privacy-lawsuit-68-million-2026-01-26

Вторинне використання даних та порушення принципу цільового обмеження записані внаслідок помилки дані не просто зберігалися, а використовувалися для рекламного таргетингу.

Юридичний аспект: Має місце вторинне використання даних (secondary use) без інформованої згоди та порушення принципу цільового обмеження (purpose limitation). Це класичний приклад того, як технологічна «зручність» перетворюється на інструмент несанкціонованої комерціалізації приватного життя.

ТЕХНОЛОГІЧНІ МОЖЛИВОСТІ ШІ ТА РИЗИКИ ДЛЯ ПРИВАТНОСТІ

Збір та обробка персональних даних:

1. ШІ-системи аналізують великі масиви даних, що може призводити до порушення права на приватність.
2. Використання алгоритмів для прогнозування поведінки особи (predictive analytics).

Біометричні дані та технології розпізнавання обличчя:

1. Проблеми використання відеоспостереження та біометричних систем без згоди громадян.
2. Вплив автоматизованого прийняття рішень на приватність.

ПРОТОКОЛ ЗАХИСТУ ПРИВАТНОСТІ ПРИ РОБОТІ З ШІ

1. **Застосовуйте глибоке знеособлення (анонімізацію) даних.** Перед завантаженням будь-яких матеріалів у систему ШІ видаляйте не лише імена та адреси, а й непрямі ідентифікатори: номери справ, унікальні обставини, назви компаній, дати та суми транзакцій.

2. **Надавайте перевагу локальним (On-premises) рішенням.** Для обробки конфіденційної інформації використовуйте моделі, розгорнуті на локальному обладнанні або у закритому контурі організації.

3. **Використовуйте режим «нульового збереження» (Zero Data Retention).** Активуйте налаштування, що забороняють зберігання історії чатів (наприклад, Temporary Chat). Пам’ятайте: навіть видалення чату вручну не гарантує, що провайдер не зберіг інформацію на сервері для технічних цілей.

ПРОТОКОЛ ЗАХИСТУ ПРИВАТНОСТІ ПРИ РОБОТІ З ШІ

4. Вимикайте використання даних для навчання моделей (Opt-out). У налаштуваннях приватності обов’язково відмовтеся від участі у програмах покращення якості сервісу.

5. Аналізуйте юрисдикцію та умови надання послуг (ToS). Зважайте на місцезнаходження серверів провайдера та застосовне право. Уникайте сервісів, що підпадають під юрисдикції з низьким рівнем захисту даних або широкими повноваженнями спецслужб.

6. Ураховуйте ризик «мозаїчної деанонімізації». Не вводьте в систему розрізнені факти, які при зіставленні з відкритими джерелами (OSINT) дозволяють ідентифікувати справу чи особу.

UNESCO, AI Essentials for Judges, 2026, https://unesdoc.unesco.org/ark:/48223/pf0000396991

Основи ШІ для суддів - це спеціалізований навчальний документ ЮНЕСКО для суддів, який прямо розглядає питання приватності, незалежності суддів, алгоритмічних упереджень та кібербезпеки судових даних; пояснює, як суди можуть використовувати ШІ для пошуку правової інформації, аналізу документів, підготовки проєктів рішень та адміністративної підтримки, водночас зберігаючи повний людський контроль над судовими рішеннями.

Суддям рекомендується дотримуватися суворої «інтелектуальної приватності», уникаючи передачі конфіденційної інформації в системи ШІ.

Instrucción 2/2026 sobre la utilización de sistemas de inteligencia artificial en el ejercicio de la actividad jurisdiccional (General Council of the Judiciary). https://www.boe.es/boe/dias/2026/01/30/pdfs/BOE-A-2026-2205.pdf

Інструкція 2/2026 Генеральної ради судової влади Іспанії про використання систем штучного інтелекту у здійсненні юрисдикційної діяльності.

Суддям заборонено завантажувати будь-які «судові дані» (datos judiciales) у системи ШІ, які не були офіційно надані органами судового врядування, при цьому використання відкритих моделей (наприклад, для перекладу) дозволяється виключно на основі публічної інформації.

ДОДАТКОВІ ДЖЕРЕЛА

1. Берназюк Ян. Сучасні можливості штучного інтелекту та питання приватності (31.10.24) https://court.gov.ua/storage/portal/supreme/prezentacii_2024/104_AI_privacy_bernaziuk.pdf
2. Берназюк Ян. Штучний інтелект та право на приватність: баланс між інноваціями та захистом персональних даних (20.02.25) https://court.gov.ua/storage/portal/supreme/prezentacii_2025/119_AI_personal_data_protection_bernaziuk.pdf
3. Берназюк Ян. Сучасні можливості ШІ та питання приватності (27.11.25) https://court.gov.ua/storage/portal/supreme/160.%20AI_Advances_and_Privacy_bernaziuk%20%D0%B7%D1%80%D0%BE%D0%B1%D0%B8%D1%82%D0%B8%20%D0%B3%D0%BE%D1%82%D0%BE%D0%B2%D0%BE.pdf
4. Берназюк Ян. ШІ та право на приватність і баланс між інноваціями та захистом персональних даних (12.12.25) https://court.gov.ua/storage/portal/supreme/163.%20AI_balance_and_Privacy_bernaziuk%20%D0%B3%D0%BE%D1%82%D0%BE%D0%B2%D0%BE.pdf
5. Берназюк Ян. Обов'язки судді щодо гарантування права на приватність при роботі доказами в умовах застосування ШІ (30.01.26) https://court.gov.ua/storage/portal/supreme/prezent2026/165_Judicial_Privacy_Duties_AI_Evidence_bernaziuk.pdf
6. Берназюк Ян. Судовий захист права на приватність при використанні технологій штучного інтелекту (Обов'язки судді щодо гарантування права на приватність при роботі доказами в умовах застосування ШІ) (19.02.26) https://court.gov.ua/storage/portal/supreme/prezent2026/sydovuy_zahust_privatnist_AI.pdf
7. Берназюк Ян. Штучний інтелект у правосудді: від практики Суду ЄС до європейських стандартів (13.03.26) https://nsj.gov.ua/ua/ogoloshennya/natsionalna-shkola-suddiv-ukraini-ogoloshue-pro-provedennya-kruglogo-stolu-/

ДОДАТКОВІ ДЖЕРЕЛА

1. Берназюк Ян. Штучний інтелект та система правосуддя України: результати співпраці у році, що минув https://so.supreme.court.gov.ua/authors/934/shtuchnyi-intelekt-ta-systema-pravosuddia-ukrainy-rezultaty-spivpratsi-u-rotsi-sh%D1%81ho-mynuv
2. Берназюк Ян. Наукові надбання як основа для наступних кроків на шляху інтеграції штучного інтелекту в систему правосуддя https://so.supreme.court.gov.ua/news/949/naukovi-nadbannia-iak-osnova-dlia-nastupnykh-krokiv-na-shliakhu-intehratsii-shtuchnoho-intelektu-v-systemu-pravosuddia
3. Берназюк Ян. Цифрова ера правосуддя: роль ШІ у забезпеченні єдності судової практики в Україні https://so.supreme.court.gov.ua/news/986/tsyfrova-era-pravosuddia-rol-shi-u-zabezpechenni-iednosti-sudovoi-praktyky-v-ukraini
4. Bernaziuk Ian. Artificial Intelligence and the Judicial system of Ukraine: results of cooperation in the past year https://constitutionalist.com.ua/artificial-intelligence-and-the-judicial-system-of-ukraine-results-of-cooperation-in-the-past-year
5. Берназюк Ян. Штучний інтелект і його використання для забезпечення єдності судової практики як складової довіри до суду // Слово Національної школи суддів України. – 2024, № 2(49), С. 16-35 https://slovo.nsj.gov.ua/images/pdf/2024_4_49/nsj_4_49_2024.pdf
6. Берназюк Ян. Ера ШІ й роль верховних судів у цифровій трансформації правосуддя // Юридична газета. № 4 (792). - С. 16-18. https://yur-gazeta.com/publications/practice/sudova-praktika/era-shi-y-rol-verhovnih-sudiv-u-cifroviy-transformaciyi-pravosuddya.html
7. Bernaziuk Ian. Artificial Intelligence in the Ukrainian Judiciary: Charting the Course Under the Digital Gavel https://constitutionalist.com.ua/artificial-intelligence-in-the-ukrainian-judiciary-charting-the-course-under-the-digital-gavel
8. Bernaziuk Ian. Benchmarking Justice: Can AI Uphold the Rule of Law? https://law.ukma.edu.ua/wp-content/uploads/2025/11/Rule-of-Law-and-AI-Challenges.pdf
9. Берназюк Ян. Правосуддя майбутнього збереження незалежності та людяності в еру ШІ https://court.gov.ua/storage/portal/supreme/161.%20Future_justice_independent_humane%20AI-era_bernaziuk%20%D0%B3%D0%BE%D1%82%D0%BE%D0%B2%D0%BE.pdf
10. Берназюк Ян. Межі втручання у приватне життя в умовах загроз національній безпеці: стандарти і виклики для правосуддя https://court.gov.ua/storage/portal/supreme/135.%20Limits_of_Interference_Private_Life_under_National_Security%20Threats_bernaziuk.pdf
11. Берназюк Ян, Фонова Олена. Правосуддя 2035: між правом і кодом»: Випуск № 18 подкастів НШСУ https://youtu.be/UlghLhHV8os?si=nCpvAl5p5KP3tY_G
12. Штучний інтелект у роботі адвоката та судовому процесі: можливості, межі, відповідальність https://youtu.be/-qJ2FCeOEWQ
13. Коментар до статті 16 (використання суддею технологій ШІ) Кодексу суддівської етики https://constitutionalist.com.ua/komentar-do-statti-16-vykorystannia-suddeiu-tekhnolohij-shi-kodeksu-suddivskoi-etyky

Верховний
Суд

Дякую за увагу!