



Верховний
Суд

НАЦІОНАЛЬНА ШКОЛА СУДДІВ УКРАЇНИ
Організація з безпеки і співробітництва в Європі (ОБСЄ)

Тренінг:
Специфіка та спеціальний правовий статус електронних
доказів. Виклики сучасності

27 листопада 2025 року

Сучасні можливості ШІ та питання приватності

Ян БЕРНАЗЮК

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

ПЛАН

1. Конституційні гарантії приватності в Україні
2. Глобальні виклики приватності в епоху штучного інтелекту
3. Технологічні ризики та механізми деанонімізації
4. Практичні протоколи захисту приватності при роботі з ШІ
5. Вимоги та обмеження у судовій системі щодо використання ШІ
6. Рекомендації для правників і стратегічні напрям

КОНСТИТУЦІЯ УКРАЇНИ

Стаття 28 – Забезпечує право кожного на повагу до його гідності, що також пов'язане з приватністю, оскільки включає захист особистих даних.

Стаття 30 – Забезпечує право на недоторканність житла. У статті зазначено, що проникнення до житла або іншого володіння особи, проведення в них огляду чи обшуку допускається лише за вмотивованим рішенням суду.

Стаття 31 – Гарантує таємницю листування, телефонних розмов, телеграфної та іншої кореспонденції. Винятки допускаються тільки на підставі судового рішення в передбачених законом випадках.

Стаття 32 – Прямо визначає право на невтручання в особисте та сімейне життя. Також заборонено збір, зберігання, використання та поширення конфіденційної інформації про особу без її згоди. Гарантує особі право знайомитися з інформацією про себе.

Sam Altman just made the best argument for not using ChatGPT

<https://www.pcworld.com/article/2861037/sam-altman-just-made-the-best-argument-for-not-using-chatgpt.html>

В інтерв'ю Сем Альтман наголосив, що OpenAI може бути юридично зобов'язана розкрити зміст приватних діалогів користувачів на вимогу суду або в межах інших процесуальних дій, що демонструє реальну вразливість ШІ щодо захисту конфіденційної інформації та персональних даних. Така ситуація підкреслює, що навіть за умови декларованої приватності сервісу, закон не встановлює спеціальних гарантій анонімності чи професійної таємниці, а отже, будь-яке звернення до ШІ може бути потенційно розкрито в судовому провадженні.

Ці обставини особливо актуалізують питання обережності у використанні ШІ для чутливих, особистих або професійно охоронюваних комунікацій, оскільки відсутність юридичних гарантій конфіденційності створює ризики для користувачів. Водночас це підсилює аргументацію на користь локальних моделей ШІ, які працюють без відправлення даних у хмару, надаючи значно вищий рівень інформаційної безпеки та дозволяючи користувачеві контролювати зберігання, обробку і видалення власних даних без втручання третіх осіб.

Brussels knifes privacy to feed the AI boom

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

ЄК в межах «цифрового омнібусу» пропонує послабити окремі положення GDPR, розширивши можливості використання спеціальних категорій даних та псевдонімізованої інформації для тренування й функціонування систем ШІ, що вже викликає суттєві застереження серед експертів і правозахисників щодо впливу на фундаментальні права людини.

Такі зміни суттєво зміщують баланс між приватністю та економічними інтересами, відкриваючи шлях до глибшої й масштабнішої обробки даних, підсилення механізмів онлайн-стеження та появи нових ризиків для користувачів, що може означати відхід від усталених європейських стандартів захисту персональної інформації й цифрової автономії громадян.

AI-powered radar can spy on phone calls from 10 feet, exposing new privacy risks

<https://interestingengineering.com/culture/ai-radar-phone-call-privacy-threat>

Дослідження університету Пенсільванії засвідчило, що поєднання міліметрового радара та алгоритмів ШІ здатне дистанційно зчитувати мікровібрації динаміка смартфона і відтворювати частину телефонної розмови з кількох метрів, що суттєво розширює спектр можливостей для прихованого стеження за комунікаціями.

Хоча точність розпізнавання становить близько 60%, навіть фрагментарні збіги ключових слів можуть розкривати чутливу інформацію, демонструючи ризики для приватності та необхідність захисту від такого перехоплення.

The New York Times wants your private ChatGPT history — even the parts you've deleted

<https://thehill.com/opinion/technology/5383530-chatgpt-users-privacy-collateral-damage>

Американський федеральний суд (справа за позовом до The New York Times) 6 липня 2025 року зобов'язав OpenAI зберігати практично всі історії спілкування користувачів із ChatGPT — включно з тими, які люди навмисно видалили, що створює прецедент втручання в приватність понад 70 млн осіб та підважує можливість повного видалення даних.

Тобто, за заявою корпоративного позивача може бути «заморожено» величезний обсяг чутливих особистих даних, фактично нормалізуючи масове збереження приватних комунікацій, посилюючи ризики судового доступу до приватної інформації.

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.

ПОЛОЖЕННЯ ПРО ВИКОРИСТАННЯ ТЕХНОЛОГІЙ ШІ ПРАЦІВНИКАМИ АПАРАТУ ВС

<https://constitutionalist.com.ua/poperednij-proiekt-polozhennia-pro-vykorystannia-tekhnohij-shi-pratsivnykamy-aparatu-vs>

Робоча група Верховного Суду щодо стратегії забезпечення єдності судової практики у період з 7 липня по 24 листопада 2025 року розробила проєкт Положення про використання технологій ШІ працівниками апарату Верховного Суду.

ОСНОВНІ ПРИНЦИПИ

1. Принцип захисту основоположних прав і свобод
2. Принцип відповідальності
3. Принцип конфіденційності та безпеки
4. Принцип добросовісності та достовірності
5. Принцип етичності та недискримінації

ПРИНЦИП ЗАХИСТУ ОСНОВОПОЛОЖНИХ ПРАВ І СВОБОД ЛЮДИНИ І ГРОМАДЯНИНА

1. Використання ШІ має відповідати Конституції та законодавству України, зокрема у сферах захисту персональних даних та інтелектуальної власності.
2. У випадку використання ШІ для створення документа або його частини особа у супровідній інформації або в самому документі **повідомляє** осіб, яким надається відповідна інформація, про таке використання.
3. **Не вимагається повідомлення** про використання ШІ, якщо технологія застосовувалася для виконання суто технічних завдань (наприклад, перевірка граматики, форматування тексту, транскрибування тощо).

ПРИНЦИП ВІДПОВІДАЛЬНОСТІ

1. Остаточне рішення про використання результатів, отриманих з використанням ШІ, у своїй роботі особа приймає самостійно на власний критичний розсуд.
2. Застосування ШІ у роботі не знімає з особи відповідальність за результати його власної роботи.
3. Особа зобов'язана ретельно перевіряти отримані результати. Усі фактичні дані, цитати та посилання на нормативні акти чи судову практику необхідно звіряти з першоджерелами (актами законодавства, офіційними базами даних тощо) та, за потреби, коригувати.

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.

ПРИНЦИП ДОБРОСОВІСНОСТІ ТА ДОСТОВІРНОСТІ

1. Будь-яка інформація, створена з використанням ШІ, підлягає обов'язковій фаховій перевірці на точність, достовірність та відсутність упереджень.
2. Для підвищення якості роботи з ШІ слід формулювати чіткі та коректні запити, а також вживати заходів для виявлення та перевірки першоджерел наданої інформації. Якщо перевірити достовірність джерела неможливо, слід утриматися від використання такого результату як належного підтвердженого.
3. При роботі з технологіями ШІ необхідно приділяти особливу увагу походженню та достовірності вхідних даних (завантаженої інформації та документів). Для аналізу та узагальнень слід використовувати, наскільки це можливо, дані з офіційних джерел.

ПРИНЦИП ЕТИЧНОСТІ ТА НЕДИСКРИМІНАЦІЇ

1. Використання ШІ має здійснюватися таким чином, щоб гарантувати справедливе, неупереджене та поважне ставлення до кожної людини, незалежно від її походження, статі, віку, переконань чи інших ознак.
2. Необхідно виявляти та мінімізувати ризики упередженості, які можуть бути закладені в алгоритмах ШІ, зокрема, у разі виявлення ознак такої упередженості – уникати негативного впливу цього фактору на роботу.
3. При виборі та затвердженні технологій ШІ перевагу слід надавати тим інструментам, розробники яких гарантують належний захист даних, відповідність вимогам безпеки, конфіденційності, контроль доступу, а також надають прозору інформацію про архітектуру технології, дані для її навчання та вжиті заходи для зменшення ризику алгоритмічної упередженості.

ЗАБОРОНЯЄТЬСЯ ВИКОРИСТАННЯ ТЕХНОЛОГІЙ 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.

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.

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.

УХВАЛА АПЕЛЯЦІЙНОЇ ПАЛАТИ ВИЩОГО АНТИКОРУПЦІЙНОГО СУДУ ВІД 01 ВЕРЕСНЯ 2025 РОКУ У СПРАВІ № 991/3222/25

<https://reyestr.court.gov.ua/Review/129856098>

Судом підтверджено, що вирок на підставі угоди про визнання винуватості стосується виключно обвинуваченого, не має преюдиційного значення щодо інших осіб і не може бути використаний як доказ їхньої винуватості, навіть якщо за допомогою систем штучного інтелекту (зокрема ChatGPT) можна спробувати ідентифікувати «знеособлену» особу за фрагментами тексту.

Суд окремо наголосив, що відповіді ШІ не є ані достовірним джерелом інформації, ані процесуальним доказом у кримінальному провадженні, що має принципове значення для питань приватності: навіть за наявності технологічної можливості деанонімізації суд захищає людину від автоматичного ототожнення та не допускає, щоб алгоритмічні припущення підміняли собою належну доказову базу.

РЕКОМЕНДАЦІЇ ДЛЯ ПРАВНИКІВ ЩОДО БЕЗПЕЧНОГО ВИКОРИСТАННЯ ШТУЧНОГО ІНТЕЛЕКТУ (ЛИПЕНЬ 2025)

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

Ці секторальні рекомендації є одним зі складників дорожньої карти з регулювання ШІ в Україні. Системи ШІ можуть бути корисні на різних етапах діяльності правників — від первинного аналізу документів до формування стратегії захисту клієнта та підготовки процесуальних документів.

Ці рекомендації розроблено для того, щоб надати правникам практичні поради щодо відповідального використання ШІ в професійній діяльності

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-krokv-na-shliakhu-intehratsii-shtuchoho-intelektu-v-systemu-pravosuddia>
3. Берназюк Ян. Сучасні можливості штучного інтелекту та питання приватності <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. Основні принципи відповідального використання ШІ у системі правосуддя <https://www.nsj.gov.ua/ua/news/natsionalna-shkola-suddiv-ukraini-rozpochala-tridennu-onlayn-pidgotovku-dlya-kerivnikiv-sudiv>
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



Верховний
Суд

Дякую за увагу!