

DOI: 10.18523/2617-2607.2025.15.78-85

УДК 342.738:347.77:004.89

Олександр Кожухар

Аспірант кафедри загальнотеоретичного правознавства та публічного права
факультету правничих наук

Національний університет «Києво-Могилянська академія», Київ, Україна

<https://orcid.org/0009-0006-4183-3289>

o.kozhukhar@ukma.edu.ua

ПРИНЦИП ПРОЗОРОСТІ В КОНТЕКСТІ ПРАВОВОГО РЕГУЛЮВАННЯ СИСТЕМ ШТУЧНОГО ІНТЕЛЕКТУ

Україна продовжує розробляти власний підхід до правового регулювання штучного інтелекту. З огляду на це важливою є теоретико-правова дискусія щодо основних аспектів регулювання ШІ на рівні Європейського Союзу, який на сьогодні є лідером у цій сфері. Дискурс щодо питань регулювання ШІ демонструє, що технології ШІ — їхнє розроблення та подальше використання — повинні бути прозорими. Саме прозорість є важливою гарантією від зловживань, пов'язаних із ШІ, та передумовою реалізації інших ключових принципів, пов'язаних із регулюванням ШІ, зокрема підзвітності та відповідальності розробників та користувачів систем ШІ. Водночас прозорість є комплексною вимогою, а для її застосування потрібно врахувати особливості самої технології ШІ та законодавчих обмежень, включно з обмеженнями щодо захисту персональних даних та охорони об'єктів права інтелектуальної власності. У статті досліджено передумови виникнення вимоги щодо прозорості систем ШІ, підтверджено важливість прозорості в контексті регулювання ШІ та розглянуто теоретико-правові аспекти цього принципу та його трансформацію в регуляторні вимоги на рівні ЄС.

Ключові слова: правове регулювання, прозорість, принцип прозорості, штучний інтелект, ШІ.

Постановка проблеми

У попередній статті за темою «Правове регулювання систем штучного інтелекту в ЄС: передумови, сучасний стан та перспективи» ми розглядали питання етичних витоків правового регулювання систем штучного інтелекту (ШІ). Ми звертали увагу на дискусії щодо можливостей, викликів та ризиків, пов'язаних із певними технологіями, включно із ШІ. У цій статті також стверджували, що результати дискусій знаходили закріплення в міжнародних і національних джерелах права, наприклад, в Акті про ШІ, який було прийнято в березні 2024 р. в Європейському Союзі (ЄС)¹.

Як зазначено раніше, важливим елементом теоретико-правових та практичних обговорень щодо регулювання ШІ є питання прозорості (*transparency*) систем ШІ. Це питання є важливим через властиву системам ШІ закритість (*opacity*), на якій наголошують дослідники та законодавці. Така закритість може збільшувати негативний ефект ризиків, які несуть системи ШІ для людини та суспільства. Такими ризиками традиційно є поширення дезінформації та упередженість систем ШІ. Підсилення негативного ефекту може відбуватися внаслідок ускладнення незалежного нагляду та контролю за функціонуванням закритих систем ШІ.

З огляду на зазначене вище **метою цієї статті** є дослідити зміст принципу прозорості, його значення для регулювання систем ШІ, а також стан його впровадження в нормативних актах на рівні ЄС.

¹ Олександр Кожухар, «Правове регулювання систем штучного інтелекту в ЄС: передумови, сучасний стан та перспективи», *Наукові записки НаУКМА. Юридичні науки* 13 (2024): 65–73, <https://doi.org/10.18523/2617-2607.2024.13.65-73>.

Аналіз досліджень

Наукові дослідження, які стосуються принципу прозорості, зосереджені на питаннях його ролі в регулюванні систем ШІ та взаємозв'язку з іншими принципами, включно з підзвітністю й відповідальністю, а також на розробленні відповідних вимог до розробників і користувачів систем ШІ.

Варто зазначити, що дослідження принципу прозорості не є новими. Заклики до прозорості можна відстежити з моменту появи перших систем, які передбачали алгоритмічне ухвалення рішень. Такі заклики зрозумілі, якщо брати до уваги історичну роль прозорості (відкритості) в демократичних суспільствах. Завдяки прозорості досягають контролю за обґрунтованістю рішень — насамперед органів державної влади — із можливістю їхнього подальшого оскарження, що також зміцнює підзвітність та верховенство права². Це також важливо в контексті регулювання систем ШІ: прозорість дає змогу своєчасно виявляти зловживання або певні особливості функціонування ШІ та належно реагувати на них.

З огляду на зазначене прозорість часто входить до переліку основних принципів розроблення та використання систем ШІ. Проте змістове наповнення цього принципу та оцінювання його достатності для вирішення практичних проблем, пов'язаних із системами ШІ, залишаються предметом дискусій.

Принцип прозорості крізь призму мети регулювання ШІ

Протягом тривалого часу етичні та теоретико-правові дискусії щодо регулювання ШІ спрямовані на зменшення ризиків, пов'язаних зі стрімким розвитком цієї технології. Деякі з цих ризиків ми згадували в нашій попередній публікації про етичні витоки регулювання ШІ: упередженість ШІ та дискримінація, небезпечність, непередбачуваність тощо. Комплексно ці виклики розглянуто як у наукових публікаціях, так і в урядових документах.

Зокрема, ще у 2017 р. Пол де Лаат підсумував проблему ухвалення рішень на основі алгоритмів. Дослідник зазначав, що на колективному рівні результати функціонування алгоритмів (як у приватному, так і в публічному секторах) можуть бути упередженими до окремих груп за певною ознакою; до того ж усі аспекти алгоритмічного ухвалення рішень залишаються непрозорими, а пояснення тих чи інших рішень немає, а якщо і є, то зазвичай незрозумілі³.

Отже, важливим і часто центральним питанням дискусій щодо регулювання ШІ є питання підзвітності та відповідальності, а саме визначення суб'єкта, який повинен нести відповідальність за функціонування системи ШІ. Особливістю обговорень є технологічний елемент ШІ. Системи ШІ можуть діяти творчо та непередбачувано, зокрема за принципом «чорної скриньки». У такому разі розробник системи чи її користувач не завжди можуть передбачити наслідки її функціонування та повністю пояснити алгоритми ухвалення рішень⁴. Безпосередніми наслідками цієї особливості є таке:

- *питання вини та відповідальності*: непередбачуваність системи ШІ підважує основи деліктного права, особливо якщо вважати, що вина є обов'язковою умовою виникнення деліктних зобов'язань⁵;
- *швидка зміна моделі функціонування системи ШІ*: система мінлива і за короткий проміжок часу може відійти від тих стандартів, які в певний момент декларував її розробник. У результаті система ШІ, яку розробник позиціонує як етичну, безпечну та сумісну з юридичними вимогами, може відійти від задекларованих стандартів без відома розробника. У результаті може відбуватися неконтрольований негативний вплив системи ШІ, наприклад, на окрему групу людей, щодо якої таку систему використовують.

Ще одним важливим питанням є «якість даних», які використовують для розроблення (тренування) систем ШІ. Те, у який спосіб було створено систему ШІ, які дані для цього використовували, має вирішальне значення для її подальшого функціонування. Зокрема, це визначатиме, чи будуть у системі певні упередження та чи виникатиме ризик дискримінації.

З огляду на наведені виклики очевидно, що регулювання має зменшити ризики, пов'язані із ШІ. До того ж, наскільки це можливо, воно не має перешкоджати подальшому розвитку ШІ. Важливим елементом збалансованого регулювання, яке забезпечує, зокрема, підзвітність та відповідальність певного суб'єкта, є прозорість таких систем.

Беручи за основу працю Девіда Бріна «Прозоре суспільство», Мірей Хільдебрандт та Берт-Яп Купс зазначають, що «прозорість є одним зі стовпів верховенства права та неодмінною передумовою

² Peter Cane et al., *The Oxford Handbook of Comparative Administrative Law* (Oxford University Press, 2021).

³ Paul B. de Laat, "Algorithmic Decision-Making Based on Machine Learning from Big Data: Can Transparency Restore Accountability?," *Philosophy & Technology* 31, no. 4 (2017): 526, <https://doi.org/10.1007/s13347-017-0293-z>.

⁴ Cane et al., *The Oxford Handbook of Comparative Administrative Law*.

⁵ Woodrow Barfield, "Towards a Law of Artificial Intelligence," in *Research Handbook on the Law of Artificial Intelligence* (Edward Elgar Publishing, 2018), 27, <https://doi.org/10.4337/9781786439055.00011>.

підзвітності й відповідальності»⁶. В українському контексті Біла книга з регулювання ШІ в Україні прямо згадує взаємозв'язок відповідальності та прозорості, вказуючи, що, зокрема, прозоре розкриття того, як системи ШІ побудовані, має вирішальне значення для безпеки та контролю ШІ; крім цього, «якщо система ШІ завдає шкоди або поводить несподівано (невідповідно до заздалегідь окреслених очікувань), важливо знати, хто несе відповідальність, для того, щоб виправити таку ситуацію»⁷.

Ми погоджуємося з цим підходом. Важливо, щоб прозорість сприяла іншим компонентам регулювання ШІ, включно з підзвітністю та відповідальністю. Для досягнення цієї мети важливо, щоб було належне розкриття інформації про систему ШІ — від самого факту, що в певному випадку застосовується алгоритмічне ухвалення рішень, до деталей алгоритму: хто є розробником системи, як алгоритм функціонує, з якою метою його застосовано, тощо. Ці питання виводять на важливе місце прозорість систем ШІ — прозорість на кожному етапі всього циклу функціонування систем.

Водночас, як зазначає Френк Паскуале, автор фундаментальної праці «Суспільство чорної скриньки», прозорість є не самоціллю, а проміжним кроком до зрозумілості систем ШІ⁸, наголошуючи на ролі прозорості як «фасилітатора» інших елементів регулювання ШІ. Про взаємозв'язок прозорості та відповідальності йдеться в праці Джоанни Брайсон в Оксфордському посібнику з етики ШІ. Дослідниця зазначає, що саме людина повинна бути в підсумку відповідальною за результати функціонування конкретної системи ШІ, а регулювання має забезпечувати «відстежуваність дій людини та відповідальність за дії людини, пов'язані з розробленням та використанням розумних систем»⁹. З огляду на це прозорість ШІ є важливою та часто базовою вимогою регулювання. Саме прозорість дає змогу чітко визначати, який саме суб'єкт і за які дії повинен відповідати. Ба більше, прозорість дає змогу забезпечувати реалізацію нагляду за всіма етапами впровадження ШІ людиною¹⁰. Такий нагляд можливий, оскільки система ШІ створює достатньо інформації (*logs*), що дає змогу встановити, коли, як, ким і з якою метою таку систему створено¹¹.

Отже, встановивши взаємозв'язки між метою регулювання ШІ та принципом прозорості, потрібно дослідити, яким чином прозорість може сприяти цій меті, якими є межі прозорості, а також яким є обсяг вимог, які впливають із принципу прозорості.

Теоретико-правові аспекти принципу прозорості в контексті регулювання систем ШІ

Нині є значна кількість досліджень, які стосуються питання прозорості алгоритмів (*algorithmic transparency*), що охоплює, зокрема, ШІ. Спільним знаменником більшості досліджень є згода з тим, що заклик до прозорості систем ШІ (як у приватному, так і в публічному секторі) є обґрунтованим, зокрема через причини, згадані в попередньому розділі (наприклад, непередбачуваність цих систем)¹².

Проте дослідники по-різному підходять до того, що саме означає прозорість як принцип, наскільки вимогу прозорості можна виконати на практиці та які виклики виникають через її впровадження. Водночас ми можемо спостерігати певний консенсус науковців: прозорість не означає повного розкриття всієї інформації про систему ШІ. Такий підхід є як непрактичним, так і неналежним.

Непрактичність підходу з повним розкриттям інформації (який не враховує особи адресата такого розкриття) пояснюють декількома причинами. Зокрема, зазвичай унаслідок цього буде опубліковано масив даних, незрозумілих для пересічного кінцевого користувача, який не зможе отримати чіткі відповіді на основні питання про систему ШІ — як вона впливає на конкретного користувача системи. Як зазначає Ендрю Мюррей, надання деталізованої інформації «перевантажило б навіть досвідчених користувачів, оскільки параметри ухвалення рішень [системами ШІ] є мінливими та невизначеними»¹³.

Неналежність такого підходу впливає з певних взаємозв'язків на перетині розкриття інформації про систему ШІ та охорони об'єктів права інтелектуальної власності, пов'язаних із системою ШІ. У системи ШІ зазвичай вкладають значні інвестиції, а їхні розробники прагнуть забезпечити максимальну охорону систем від конкурентів. Ці зусилля можуть бути знівельовані, якщо розробник

⁶ Mireille Hildebrandt and Bert-Jaap Koops, "The Challenges of Ambient Law and Legal Protection in the Profiling Era," *The Modern Law Review* 73, no. 3 (2010): 448, <https://doi.org/10.1111/j.1468-2230.2010.00806.x>.

⁷ Біла книга з регулювання ШІ в Україні (2024), 21, <https://thedigital.gov.ua/storage/uploads/files/page/community/docs/%D0%A0%D0%B5%D0%B3%D1%83%D0%BB%D1%8E%D0%B2%D0%B0%D0%BD%D1%8F%20%D0%A8%D0%86.pdf>.

⁸ Frank Pasquale, *The Black Box Society* (Harvard University Press, 2015), 8.

⁹ Markus Dirk Dubber, Frank Pasquale, and Sunit Das, *The Oxford Handbook of Ethics of AI* (Oxford University Press, 2021), 7.

¹⁰ Ibid., 23.

¹¹ Ibid., 8.

¹² de Laat, "Algorithmic Decision-Making Based on Machine Learning from Big Data: Can Transparency Restore Accountability?," 527.

¹³ Andrew Murray, *Almost Human: Law and Human Agency in the Time of Artificial Intelligence* (T. M. C. Asser Press, 2021), 30, <https://www.asser.nl/upload/documents/20240926T102230-AL6-Murray-WEB%20new.pdf>.

чи користувач буде зобов'язаний розкрити всю інформацію про власну систему. Ще одним небажаним наслідком таких вимог буде редоміліяція (переміщення) розробників систем ШІ в держави з нижчими стандартами регулювання ШІ, що підважуватиме міжнародні зусилля з розроблення глобальних стандартів у сфері ШІ.

Френк Паскуале зазначає, що обидва варіанти (повна секретність інформації про ШІ та повне розкриття інформації) є неналежними підходами до регулювання¹⁴. На думку дослідника, повна прозорість була б «жахом для приватності та [мала б наслідком] крадіжку інтелектуальної власності»¹⁵. Водночас дослідник визнає засадничу важливість прозорості, додаючи, що без прозорості не буде підзвітності та відповідальності¹⁶.

Обговорюючи питання «повного розкриття інформації», Пол де Лаат зазначає, що, хоч існує певне обґрунтування заклику до такого розкриття (на будь-який запит розкривається весь масив даних про систему ШІ)¹⁷, глибше розуміння взаємозв'язків прозорості з іншими аспектами системи ШІ ставить під сумнів такий підхід. Крім наведених вище питань щодо охорони об'єктів права інтелектуальної власності та складності в інтерпретації даних про систему ШІ, дослідник згадує питання приватності (розкриття може мати наслідком витік чутливих даних про суб'єктів персональних даних) та ризик маніпулювання системою третіми особами (коли її алгоритми будуть загальнодоступними)¹⁸. Звідси висновок, що повна прозорість може лише нашкодити досягненню відповідальності та підзвітності розробників систем ШІ; проте вона може бути доречною в обмежених випадках — наприклад, для доступу до системи наглядових органів¹⁹.

Розуміючи вказані ризики та беручи до уваги потребу в розробленні збалансованого регулювання, Ніколас Діакопулос наголошує, що прозорість (дослідник розглядає її як доступність інформації про актора, що дає змогу іншим акторам відстежувати діяльність або результати діяльності актора) повинна сприяти управлінню алгоритмічними системами та відповідальності²⁰. Цього можна досягти, на думку дослідника, завдяки «практичній прозорості» (*usable transparency*) — розкриттю тієї інформації, яка справді має значення для її адресата²¹. Звідси важливий аспект підходу до прозорості — контекстуальність, коли враховано особу адресата для визначення обсягу інформації про алгоритмічну систему, що підлягає розкриттю. Дослідник пропонує пірамідальну структуру розкриття інформації, коли більш детальну інформацію розкривають залежно від адресата²².

Ми можемо погодитися з таким підходом. Обсяг розкриття інформації про систему ШІ може варіювати залежно від особи, якій така інформація підлягає розкриттю, та циклу функціонування системи ШІ. Наприклад, на етапі попереднього погодження високоризикової системи ШІ, коли її безпечність перевіряє держава або орган сертифікації, варто очікувати, що систему перевірятимуть особи з належним рівнем експертизи. Через це обсяг розкриття буде більшим; водночас розкрита інформація не стає загальнодоступною, її надаватимуть лише особам, які будуть зобов'язані забезпечувати належний рівень її конфіденційності²³.

Також ми розуміємо, що розкриття інформації для кінцевих споживачів, які є користувачами системи, з погляду «практичної прозорості», буде меншим за обсягом. Важливо, щоб розкриття було зрозумілим і достатнім для того, щоб такий адресат зміг оцінити вплив системи ШІ на нього.

Як зазначає Александра Бал,

щоб досягти належного рівня прозорості в алгоритмічному ухваленні рішень, потрібно забезпечити можливість пояснення будь-яких рішень, створених автоматизованою системою, людям, на яких вони впливають, а ці пояснення мають бути зрозумілими для цільової аудиторії; ба більше, має бути чітко визначено, хто має повноваження переглядати та потенційно скасовувати алгоритмічні рішення, а алгоритми слід контролювати та регулярно перевіряти, щоб забезпечити їхню суспільну актуальність та відповідність сучасним вимогам²⁴.

¹⁴ Pasquale, *The Black Box Society*, 142.

¹⁵ Ibid.

¹⁶ Ibid., 176.

¹⁷ de Laet, "Algorithmic Decision-Making Based on Machine Learning from Big Data: Can Transparency Restore Accountability?" 528.

¹⁸ Ibid.

¹⁹ Ibid.

²⁰ Dubber, Pasquale, and Das, *The Oxford Handbook of Ethics of AI*, 204.

²¹ Ibid.

²² Ibid.

²³ Ibid., 210.

²⁴ Bart Custers and Eduard Fosch-Villaronga, *Law and Artificial Intelligence: Regulating AI and Applying AI in Legal Practice* (T.M.C. Asser Press, 2022), 236.

Крім цього, у будь-якому разі розкриття інформації має бути достатньо «динамічним», щоб враховувати зміни в процесі функціонування системи ШІ²⁵.

Про необхідність диференціювання підходів до прозорості також зазначено в Кембриджському посібнику з питань права, етики та політики, які стосуються ШІ. У розділі, присвяченому ролі ШІ в медіа, наголошено, що доцільно розмежовувати внутрішню та зовнішню прозорість, а також прозорість, яка стосується третіх осіб. Дослідники визначають їх так:

- внутрішня прозорість: наявність у працівників організації належних знань про систему ШІ, яку використовує організація;
- зовнішня прозорість: надання цільовій аудиторії системи ШІ інформації про таку систему;
- прозорість, що стосується третіх осіб: наявність інформації про те, як система ШІ була натренована і як вона функціонує²⁶.

Іншим аспектом прозорості є обсяг розкриття інформації про систему ШІ. Ми вже згадували про «контекстуальність» розкриття, а також про можливість повного розкриття інформації в певних випадках. Водночас важливо розуміти, яка інформація про систему, в принципі, є важливою для розкриття.

Ще у 2014 р. Френк Паскуале та Даніель Сітрон обґрунтовували потребу в застосуванні концепції належної процедури до використання систем скорингу, зокрема тих, які використовують технологію ШІ, для того щоб такі системи забезпечували справедливість і точність²⁷. Дослідники згодні з тим, що людина повинна бути поінформована про використання певного алгоритму щодо неї, а також у певних випадках мати можливість оспорювати використання алгоритму²⁸. На можливості оспорювати використання алгоритмів (розумних технологій) також наголошено в праці Мірей Хільдебрандт та Берта-Япа Купса, які зазначають, що потрібно розвивати інструменти, які сприяють прозорості, щоб рішення, ухвалені з використанням розумних технологій, могли піддаватися оскарженню²⁹.

Ніколас Діакопулос наводить принаймні три групи питань про систему ШІ, на які доцільно отримати відповідь:

- рівень і природа залучення людини до створення, функціонування та управління системою ШІ, включно з метою системи та особами, відповідальними за неї;
- дані, використані для тренування системи та для її функціонування, щоб визначити якість цих даних;
- деталі про саму систему (модель) ШІ³⁰.

Водночас Н. Діакопулос критично оцінює необхідність того, щоб системи ШІ надавали пояснення стосовно ухвалення своїх рішень (додатково до загального опису свого функціонування). Дослідник звертає увагу, що такі пояснення можуть бути приблизними, фрагментарними та неточними; натомість потрібно надати достатньо інформації про ці системи, щоб зацікавлені особи, включно з органами нагляду, змогли самостійно дійти висновку про причини ухвалення системою рішень³¹.

Крім обговорення питань важливості прозорості та обсягу розкриття, який впливає з принципу прозорості, ми бачимо в науковій літературі деякі критичні позиції щодо цього принципу. Наприклад, часто наголошують, що лише прозорості недостатньо для мінімізації всіх ризиків, пов'язаних із ШІ, потрібно застосовувати комплексний підхід до регулювання ШІ. Крім цього, у контексті дискусії про прозорість є сумніви щодо того, наскільки ефективно її можна застосовувати на практиці. У цій дискусії згадано обмежені ресурси регуляторних органів щодо перевірки технічних аспектів систем ШІ з огляду на складність сучасних систем ШІ, особливо заснованих на глибокому навчанні, коли навіть розробники систем ШІ не можуть повністю пояснити логіку ухвалення рішень. Інші проблемні аспекти та обмеження вже згадано вище: захист персональних даних, охорона об'єктів права інтелектуальної власності та проблема «інформаційного перевантаження», коли через надмірну деталізацію розкрита інформація може бути незрозумілою для кінцевих користувачів.

²⁵ Dubber, Pasquale, and Das, *The Oxford Handbook of Ethics of Ai*, 204.

²⁶ Nathalie A. Smuha, *The Cambridge Handbook of the Law, Ethics and Policy of Artificial Intelligence* (Cambridge University Press, 2025), 297.

²⁷ Danielle Keats Citron and Frank Pasquale, "The Scored Society: Due Process for Automated Predictions," *Washington Law Review* 89, no. 1 (2014): 1.

²⁸ Ibid.

²⁹ Hildebrandt and Koops, "The Challenges of Ambient Law and Legal Protection in the Profiling Era," 460.

³⁰ Dubber, Pasquale, and Das, *The Oxford Handbook of Ethics of Ai*, 202.

³¹ Ibid., 205.

Незважаючи на проблемні аспекти, переважна більшість дослідників не ставить під сумнів, що прозорість (у певному вигляді) має бути однією з основних вимог щодо ШІ. Як результат теоретичний дискурс щодо прозорості алгоритмів та ШІ набув продовження у двох фундаментальних нормативних актах, прийнятих на рівні Європейського Союзу: у Загальному регламенті про захист даних та Акті про ШІ. Кожен із документів певною мірою врегулював питання прозорості та містить елементи «контекстуальності» регулювання, що враховує адресата розкриття інформації та ризиковість самих систем ШІ.

Загальний регламент про захист даних, який насамперед регулює питання обробки персональних даних, закріплює вимоги щодо прозорості обробки персональних даних та захисту від автоматизованого ухвалення рішень, включно з профайлінгом, а прозорість є одним із фундаментальних принципів регулювання цих питань³². Згідно з регламентом, суб'єкт персональних даних має бути поінформований про наявність у конкретному випадку автоматизованого ухвалення рішень щодо персональних даних такого суб'єкта, а також про логіку такої обробки даних, значущість та наслідки для суб'єкта такої обробки даних³³. Крім цього, такий суб'єкт повинен мати право не підлягати рішенням, яке ґрунтується винятково на автоматизованій обробці даних, що породжує правові наслідки для нього чи подібним чином істотно впливає на нього³⁴. Водночас контролер даних (в українській термінології — володілець персональних даних) зобов'язаний належно документувати всі процеси, пов'язані з обробкою персональних даних у такий спосіб, зокрема, оцінювати їхній вплив на захист персональних даних³⁵.

Акт про ШІ містить комплексні механізми забезпечення прозорості систем ШІ, які буде застосовано до цих систем незалежно від того, чи здійснюють вони обробку персональних даних. З урахуванням підходу, який ґрунтується на ризиках, що є основою документа, Акт про ШІ встановлює декілька рівнів прозорості систем ШІ. По-перше, будь-яка система ШІ підпадає під загальний обов'язок розкриття факту взаємодії із ШІ; додаткові зобов'язання щодо розкриття такого факту покладено на системи, які безпосередньо взаємодіють з людьми. По-друге, високоризикові системи ШІ підпадають під додаткові зобов'язання, покликані забезпечити їхню прозорість, що передбачає наявність детальної технічної документації, ведення обліку про функціонування системи, а самі системи повинні бути достатньо прозорі, щоб у користувачів було розуміння, як пояснювати результати функціонування системи.

Отже, ми спостерігаємо, що теоретико-правова дискусія щодо прозорості дедалі чіткіше кристалізується в нормативних вимогах до розробників і користувачів систем ШІ. Незважаючи на технічні обмеження й виклики, пов'язані з регулюванням ШІ, саме завдяки прозорості можна буде належно відстежувати функціонування систем ШІ на практиці та вчасно реагувати на технологічні виклики. Водночас уникнення надмірності в розкритті інформації про системи ШІ (збалансований підхід) має бути гарантією, що впроваджене регулювання не перешкоджатиме подальшому науково-технічному прогресу у сфері ШІ.

Висновки та перспективи подальшої розробки тематики ШІ

Прозорість є фундаментальним принципом регулювання систем ШІ та передумовою ефективної реалізації інших принципів, зокрема підзвітності та відповідальності суб'єктів, які розробляють і використовують системи ШІ. Водночас застосування принципу прозорості потребує належного збалансування всіх інтересів, врахування контексту його застосування та визнання потенційних обмежень щодо обсягу розкриття інформації про систему ШІ в кожному окремому випадку. Це обмеження, пов'язані з особливостями систем ШІ (зокрема тих, які працюють за принципом «чорної скриньки»), із застосуванням законодавства про захист персональних даних та про охорону об'єктів права інтелектуальної власності. Законодавці та дослідники питань ШІ не заперечують важливості принципу прозорості, а закликають до більш обґрунтованого врахування цих обмежень під час розроблення систем.

Зроблені висновки та актуальна дискусія щодо прозорості систем ШІ є важливими для України. На сьогодні в Україні розробляють свій підхід до регулювання ШІ — на цьому етапі *bottom-up* підхід, коли перевагу віддають підготовці організацій до потенційного регулювання та саморегулюванню

³² Smuha, *The Cambridge Handbook of the Law, Ethics and Policy of Artificial Intelligence*, 146.

³³ Загальний регламент про захист даних, ст. 13(f), https://zakon.rada.gov.ua/laws/show/984_008-16#Text.

³⁴ Там само, ст. 24.

³⁵ Там само, ст. 35.

з подальшим ухваленням відповідних нормативно-правових актів щодо питань ШІ. В умовах формування власного підходу потрібно відстежувати тенденції регулювання ШІ, зокрема на рівні ЄС, а також проблематику такого регулювання, включно з межами прозорості систем ШІ. Наприклад, в Україні доречно розглянути можливість встановлення винятків щодо розкриття інформації про системи ШІ з погляду національної безпеки, якщо ці системи використовують у секторі безпеки та оборони.

Водночас — в умовах задекларованого активного впровадження ШІ в публічному секторі — потрібно забезпечити, щоб таке використання відповідало стандартам, які вже на сьогодні існують, наприклад, у Європейському Союзі, тобто щоб у таких випадках було забезпечено одночасно прозорість, підзвітність і відповідальність суб'єктів, які використовують системи ШІ. Наші подальші розвідки будуть зосереджені на теоретико-правових і практичних питаннях регулювання систем ШІ в Україні, а результати цієї статті буде використано в дисертаційному дослідженні.

Список використаної літератури

- Кожухар, Олександр. «Правове регулювання систем штучного інтелекту в ЄС: передумови, сучасний стан та перспективи». *Наукові записки НаУКМА. Юридичні науки* 13 (2024): 65–73. <https://doi.org/10.18523/2617-2607.2024.13.65-73>.
- Barfield, Woodrow. “Towards a Law of Artificial Intelligence.” In *Research Handbook on the Law of Artificial Intelligence*. Edward Elgar Publishing, 2018. <https://doi.org/10.4337/9781786439055.00011>.
- Cane, Peter, Herwig C. H. Hofmann, Eric C. Ip, and Peter L. Lindseth. *The Oxford Handbook of Comparative Administrative Law*. Oxford University Press, 2021.
- Citron, Danielle Keats, and Frank Pasquale. “The Scored Society: Due Process for Automated Predictions.” *Washington Law Review* 89, no. 1 (2014). <https://digitalcommons.law.uw.edu/wlr/vol89/iss1/2>.
- Custers, Bart, and Eduard Fosch-Villaronga. *Law and artificial intelligence: Regulating AI and applying AI in legal practice*. T.M.C. Asser Press, 2022.
- Dubber, Markus Dirk, Frank Pasquale, and Sunit Das. *The Oxford Handbook of Ethics of Ai*. Oxford University Press, 2021.
- Hildebrandt, Mireille, and Bert-Jaap Koops. “The Challenges of Ambient Law and Legal Protection in the Profiling Era.” *The Modern Law Review* 73, no. 3 (2010): 428–60. <https://doi.org/10.1111/j.1468-2230.2010.00806.x>.
- Laat, Paul B. de. “Algorithmic Decision-Making Based on Machine Learning from Big Data: Can Transparency Restore Accountability?” *Philosophy & Technology* 31, no. 4 (2017): 525–41. <https://doi.org/10.1007/s13347-017-0293-z>.
- Murray, Andrew. *Almost Human: Law and Human Agency in the Time of Artificial Intelligence*. T. M. C. Asser Press, 2021. <https://www.asser.nl/upload/documents/20240926T102230-AL6-Murray-WEB%20new.pdf>.
- Pasquale, Frank. *The Black Box Society*. Harvard University Press, 2015.
- Smuha, Nathalie A. *The Cambridge Handbook of the Law, Ethics and Policy of Artificial Intelligence*. Cambridge University Press, 2025.

Bibliography

- Barfield, Woodrow. “Towards a Law of Artificial Intelligence.” In *Research Handbook on the Law of Artificial Intelligence*. Edward Elgar Publishing, 2018. <https://doi.org/10.4337/9781786439055.00011>.
- Cane, Peter, Herwig C. H. Hofmann, Eric C. Ip, and Peter L. Lindseth. *The Oxford Handbook of Comparative Administrative Law*. Oxford University Press, 2021.
- Citron, Danielle Keats, and Frank Pasquale. “The Scored Society: Due Process for Automated Predictions.” *Washington Law Review* 89, no. 1 (2014). <https://digitalcommons.law.uw.edu/wlr/vol89/iss1/2>.
- Custers, Bart, and Eduard Fosch-Villaronga. *Law and artificial intelligence: Regulating AI and applying AI in legal practice*. T.M.C. Asser Press, 2022.
- Dubber, Markus Dirk, Frank Pasquale, and Sunit Das. *The Oxford Handbook of Ethics of Ai*. Oxford University Press, 2021.
- Hildebrandt, Mireille, and Bert-Jaap Koops. “The Challenges of Ambient Law and Legal Protection in the Profiling Era.” *The Modern Law Review* 73, no. 3 (2010): 428–60. <https://doi.org/10.1111/j.1468-2230.2010.00806.x>.
- Kozhukhar, Oleksandr. “Legal Regulation of Artificial Intelligence Systems in the EU: Prerequisites, Current State and Prospects.” *NaUKMA Research Papers. Law* 13 (2024): 65–73. <https://doi.org/10.18523/2617-2607.2024.13.65-73> [in Ukrainian].

- Laat, Paul B. de. “Algorithmic Decision-Making Based on Machine Learning from Big Data: Can Transparency Restore Accountability?” *Philosophy & Technology* 31, no. 4 (2017): 525–41. <https://doi.org/10.1007/s13347-017-0293-z>.
- Murray, Andrew. *Almost Human: Law and Human Agency in the Time of Artificial Intelligence*. T. M. C. Asser Press, 2021. <https://www.asser.nl/upload/documents/20240926T102230-AL6-Murray-WEB%20new.pdf>.
- Pasquale, Frank. *The Black Box Society*. Harvard University Press, 2015.
- Smuha, Nathalie A. *The Cambridge Handbook of the Law, Ethics and Policy of Artificial Intelligence*. Cambridge University Press, 2025.

Oleksandr Kozhukhar

Doctoral student

Department of General Legal Theory and Public Law, Faculty of Law
National University of Kyiv-Mohyla Academy, Kyiv, Ukraine

<https://orcid.org/0009-0006-4183-3289>

o.kozhukhar@ukma.edu.ua

THE PRINCIPLE OF TRANSPARENCY IN THE CONTEXT OF LEGAL REGULATION OF ARTIFICIAL INTELLIGENCE SYSTEMS

Abstract

Ukraine continues to develop its own approach to the legal regulation of artificial intelligence, with due regard to the international standards developed to date. One of the objectives of the proposed legal regulation is to ensure it remains balanced and flexible so that it does not hinder further technological developments, while also protecting the rights of individuals who might be affected by AI systems, including data subject rights, insofar as AI systems involve certain personal data processing operations. For these purposes, a theoretical and legal discussion regarding the main aspects of AI regulation at the European Union level — currently the leading authority in this field — is important. Its risk-based regulatory framework and existing transparency requirements should be properly considered in Ukraine, especially in light of Ukraine’s commitment to implement the EU *acquis* in accordance with the EU-Ukraine Association Agreement.

The discourse on AI regulation in the EU and beyond demonstrates that AI technologies—their development and subsequent use—must be transparent, with transparency often construed broadly. Notably, transparency itself is an important safeguard against AI-related abuses and a prerequisite for implementing other key principles of AI regulation, particularly accountability and responsibility on the part of AI system developers and deployers. At the same time, transparency is a complex requirement, and its application requires consideration of the peculiarities of AI technology itself and existing legislative limitations, including those relating to personal data protection and the protection of intellectual property rights.

The article explores the prerequisites for the emergence of the transparency requirement for AI systems, confirms the importance of transparency in the context of AI regulation, and examines the theoretical and legal aspects of this principle and its transformation into regulatory requirements at the EU level.

Keywords: legal regulation, transparency, principle of transparency, artificial intelligence, AI.

Матеріал надійшов 14.03.2025



Creative Commons Attribution 4.0 International License (CC BY 4.0)