

Кожухар О. Г.

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

ПРИНЦИП ПРОЗОРОСТІ В КОНТЕКСТІ ПРАВОВОГО РЕГУЛЮВАННЯ СИСТЕМ ШТУЧНОГО ІНТЕЛЕКТУ

Україна продовжує розробляти власний підхід до правового регулювання штучного інтелекту. Для цих цілей важливою є теоретико-правова дискусія щодо основних аспектів регулювання ШІ на рівні Європейського Союзу, який на сьогодні є лідером у відповідній 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 її застосування вимагає врахування особливостей самої технології ШІ та наявних законодавчих обмежень, включно з обмеженнями з точки зору 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, які існують 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» розглядалося 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 вказаній статті також стверджувалося, 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 зазначалося раніше, важливим елементом теоретико-правових та практичних обговорень щодо регулювання ШІ виступає питання прозорості (*transparency*) систем ШІ. Це питання є важливим, враховуючи властиву для систем ШІ закритість (*opacity*), на якій наголошують дослідники та законодавці. Така закритість може збільшувати негативний ефект ризиків, які несуть системи ШІ для людини та суспільства. Такі ризики традиційно включають поширення дезінформації та упередженість систем ШІ. Підсилення негативного ефекту може відбуватися внаслідок ускладнення незалежного нагляду та контролю за функціонуванням закритих систем ШІ.

У зв'язку із цим, 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.

Аналіз наявних досліджень. Наявні наукові дослідження, які стосуються принципу прозорості, зосереджені на питаннях його ролі в регулюванні систем ШІ та взаємозв'язку з іншими принципами, включаючи підзвітність та відповідальність, а також на розробленні відповідних вимог до розробників та 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 прийняття рішень. Такі заклики зрозумілі, якщо брати

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

до уваги історичну роль прозорості (відкритості) в демократичних суспільствах. Завдяки прозорості досягається контроль за обґрунтованістю рішень – насамперед органів державної влади – із можливістю їхнього подальшого оскарження, що також зміцнює підзвітність та верховенство права.² Це ж є важливим у контексті регулювання систем ШІ: прозорість дозволяє своєчасно виявляти зловживання або певні особливості функціонування ШІ та належним чином реагувати на них.

У зв'язку із цим, прозорість часто включається в перелік основних принципів, застосовних до розроблення та використання систем ШІ. Водночас змістовне наповнення цього принципу та оцінка 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 теоретично-правові дискусії щодо регулювання ШІ спрямовані на зменшення ризиків, які пов'язані зі стрімким розвитком відповідної технології. Деякі із цих ризиків ми згадували в нашій попередній публікації щодо етичних витоків регулювання ШІ: упередженість ШІ та дискримінація, небезпечність та непередбачуваність, тощо. Комплексно відповідні виклики розглянуті як в наукових публікаціях, так і в урядових документах.

Так, ще в 2017 році Пол де Лаат підсумував проблему прийняття рішень на основі алгоритмів. Дослідник зазначав, що на колективному рівні результати функціонування алгоритмів (як у приватному, так і публічному секторах) можуть бути упередженими до окремих груп за певною ознакою; при цьому, усі аспекти алгоритмічного прийняття рішень залишаються непрозорими, а пояснення тих

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

чи інших рішень не надаються, а якщо і надаються, вони є зазвичай незрозумілими³.

Відповідно, важливим та часто центральним питанням дискусій щодо регулювання ІІ є питання підзвітності та відповідальності – а саме визначення суб'єкта, який повинен нести відповідальність за функціонування системи ІІ. Особливістю обговорень є технологічна складова ІІ. Системи ІІ можуть діяти у творчий та непередбачуваний спосіб, зокрема за принципом «чорної скриньки». У такому випадку розробник системи чи її користувач не завжди в змозі передбачати наслідки її функціонування та пояснити повністю алгоритми прийняття рішень.⁴ Безпосередніми наслідками такої особливості є таке:

- *питання вини та відповідальності*: непередбачуваність системи ІІ підважує основи деліктного права, особливо якщо вважати, що вина є обов'язковою умовою виникнення деліктних зобов'язань;⁵ та
- *швидка зміна моделі функціонування системи ІІ*: система мінлива і у межах короткого проміжку часу може відійшовши від тих стандартів, які декларувалися у певний момент її розробником. У результаті цього система ІІ, яку розробник позиціонує як етичну, безпечну та сумісну з юридичними вимогами, може відійти від задекларованих стандартів без відома розробника. У результаті цього може відбуватися неконтрольований негативний вплив системи ІІ, наприклад, на окрему групу людей, щодо якої така система використовується.

Ще одним важливим питанням є питання «якості даних», які використовуються для розробки (тренування) систем ІІ. Те, у який спосіб було створено систему ІІ, які дані для цього використовувалися, має визначальне

³ Paul B. de Laat, "Algorithmic Decision-Making Based on Machine Learning from Big Data: Can Transparency Restore Accountability?," *Philosophy & Technology* 31, no. 4 (November 12, 2017). <https://doi.org/10.1007/s13347-017-0293-z>, 526.

⁴ Peter Cane et al., *The Oxford Handbook of Comparative Administrative Law* (Oxford, United Kingdom: Oxford University Press, 2021).

⁵ Woodrow Barfield, "Towards a Law of Artificial Intelligence," *Research Handbook on the Law of Artificial Intelligence*, December 28, 2018, <https://doi.org/10.4337/9781786439055.00011>, 27.

значення для її подальшого функціонування. Зокрема, це визначатиме, чи будуть у системи певні упередження та чи виникатиме ризик дискримінації.

Розуміючи наведені виклики, стає очевидним, що регулювання повинно зменшити ризики, пов'язані зі ШІ. При цьому, воно повинно, наскільки це можливо, не 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 необхідною передумовою підзвітності та відповідальності».⁶ Говорячи про український контекст, 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 поводиться 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 здійснювалося належне розкриття інформації про систему ШІ – від самого факту, що у певному випадку застосовується алгоритмічне прийняття рішень, до деталей алгоритму: хто є розробником системи, як алгоритм функціонує, із якою метою він застосовується, 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 не є ціллю в собі, а проміжним

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 (May 2010): 428–60, <https://doi.org/10.1111/j.1468-2230.2010.00806.x>, 448.

⁷ "Біла Книга з Регулювання ШІ в Україні" (2024), 21.

кроком до зрозумілості [систем ШІ]⁸, наголошуючи на ролі прозорості як «фасилітатора» інших елементів регулювання ШІ. Схожий взаємозв'язок прозорості та відповідальності згадується 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 повинно забезпечувати «відстежуваність дій людини та відповідальність за дії людини, які пов'язані з розробленням та використанням розумних систем»⁹. У зв'язку з цим, прозорість ШІ є важливою та часто базовою вимогою регулювання. Саме прозорість дозволяє чітко визначати, який саме суб'єкт і за які дії повинен бути відповідальним. Більше того, прозорість дозволяє забезпечувати реалізацію нагляду за всіма етапами впровадження ШІ людиною.¹⁰ Такий нагляд є можливим, оскільки система ШІ створює достатньо інформації (*logs*), що дозволяє встановити, коли, як, ким і з якою метою така система створювалася.¹¹

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

Теоретико-правові аспекти принципу прозорості в контексті регулювання систем ШІ. Нині існує 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, з причин, згаданих у попередньому розділі (до прикладу, непередбачуваність відповідних систем).¹²

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* (New York: Oxford University Press, 2021), 7.

¹⁰ Там само, 23.

¹¹ Там само, 8.

¹² Paul B. de Laat, "Algorithmic Decision-Making Based on Machine Learning from Big Data: Can Transparency Restore Accountability?," *Philosophy & Technology* 31, no. 4 (November 12, 2017): 525–41, <https://doi.org/10.1007/s13347-017-0293-z>, 527.

У той же час дослідники по-різному підходять до того, що саме включає прозорість як принцип, наскільки вимоги щодо прозорості є виконуваними та досяжними на практиці та які виклики виникають у зв'язку з впровадженням вимог щодо прозорості. Водночас ми можемо спостерігати певний консенсус науковців: прозорість не повинна дорівнювати повному розкриттю всієї інформації про систему ШІ. Такий підхід є як непрактичним, так і неналежним.

Непрактичність підходу із повним розкриттям інформації (який не враховує особу адресата такого розкриття) пояснюється декількома причинами. Зокрема, зазвичай це матиме наслідком публікацію масиву даних, що є незрозумілим для пересічного кінцевого користувача, а також не дозволить останньому отримати чіткі відповіді на основні питання щодо системи ШІ – яким є її вплив на конкретного користувача системи. Як зазначає Ендрю Мюррей, надання деталізованої інформації «перевантажило б навіть досвідчених користувачів, оскільки параметри прийняття рішень [системами ШІ] є мінливими та невизначеними».¹³

Що стосується неналежності такого підходу, він слідує із певних взаємозв'язків на перетині розкриття інформації про систему ШІ та охорони об'єктів права інтелектуальної власності, які пов'язані із системою ШІ. Так, у системи ШІ зазвичай вкладаються значні інвестиції, а розробники останніх мають намір забезпечити максимальну охорону систем від конкурентів. Відповідні зусилля можуть бути знівельовані, якщо розробник чи користувач буде зобов'язаний розкрити всю інформацію про власну систему. Ще одним небажаним наслідком таких вимог буде т. зв. редоміциліація розробників систем ШІ в держави із нижчими стандартами регулювання ШІ – наслідок, який буде підважувати міжнародні зусилля на розроблення глобальних стандартів у сфері ШІ.

Френк Паскуале зазначає, що обидва варіанти (повна секретність інформації про ШІ та повне розкриття інформації про неї) є неналежними

¹³ Andrew Murray, "Almost Human: Law and Human Agency in the Time of Artificial Intelligence," TMC Asser Press, April 25, 2021, <https://www.asser.nl/upload/documents/20240926T102230-AL6-Murray-WEB%20new.pdf>, 30.

підходами до регулювання¹⁴. Як зазначає дослідник, повна прозорість була б «жахом для приватності та [мала б наслідком] крадіжку інтелектуальної власності»¹⁵. Водночас дослідник визнає фундаментальну 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 загальнодоступні).¹⁸ Звідси висновок, що повна прозорість може лише нашкодити досягненню відповідальності та підзвітності розробників систем ШІ; натомість вона може бути доречною в обмежених випадках – наприклад, для цілей доступу до системи зі сторони наглядових органів.¹⁹

Розуміючи вказані ризики та беручи до уваги потребу в розробленні збалансованого регулювання, Ніколас Діакопулос наголошує, що прозорість (яку дослідник розглядає як доступність інформації про актора, що дозволяє іншим акторам відстежувати діяльність або результати діяльності актора) повинна сприяти управлінню алгоритмічними системами та відповідальності.²⁰ Це досягається, на думку дослідника, завдяки «практичній прозорості» (*usable*

¹⁴ Frank Pasquale, *The Black Box Society* (Harvard University Press, 2015), 142.

¹⁵ Там само, 142

¹⁶ Там само, 176

¹⁷ Paul B. de Laat, "Algorithmic Decision-Making Based on Machine Learning from Big Data: Can Transparency Restore Accountability?," *Philosophy & Technology* 31, no. 4 (November 12, 2017): 525–41, <https://doi.org/10.1007/s13347-017-0293-z>, 528.

¹⁸ Там само, 528

¹⁹ Там само, 528.

²⁰ Markus Dirk Dubber, Frank Pasquale, and Sunit Das, *The Oxford Handbook of Ethics of Ai* (New York: Oxford University Press, 2021), 204.

transparency) – завдяки розкриттю інформації, яка дійсно має значення для її адресата.²¹ Звідси важливий аспект підходу до прозорості – контекстуальність, коли враховується особа адресата для визначення обсягу інформації про алгоритмічну систему, що підлягає розкриттю. Дослідник пропонує пірамідальну структуру розкриття інформації, коли більш детальна інформація розкривається в залежності від адресата.²²

Ми можемо погодитися з таким підходом. Обсяг розкриття інформації про систему ШІ може варіюватися в залежності 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. У зв'язку з цим, обсяг розкриття буде більшим; водночас розкрита інформація не стає загальнодоступною, а буде надаватися лише особам, які будуть зобов'язані забезпечувати належний рівень її конфіденційності.²³

Що стосується розкриття інформації для кінцевих споживачів, які є користувачами системи, ми розуміємо, що, із точки зору «практичної прозорості», розкриття інформації буде меншим за обсягом. При цьому, важливо, щоб таке розкриття було зрозумілим та достатнім для того, щоб такий адресат зміг оцінити вплив системи ШІ на нього. Як зазначає Александра Бал, «щоб досягти належного рівня прозорості в алгоритмічному прийнятті рішень, необхідно забезпечити можливість пояснення будь-яких рішень, створених автоматизованою системою, людям, на яких вони впливають, а ці пояснення мають бути зрозумілими для цільової аудиторії; більше того, 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

²¹ Там само, 204.

²² Там само, 204

²³ Там само, 210.

вимогам».²⁴ Крім цього, у будь-якому випадку розкриття інформації повинно бути достатньо «динамічним», щоб враховувати зміни в процесі функціонування системи ШІ.²⁵

Необхідність диференціювати підходи до прозорості також вказується в Кембриджському посібнику щодо питань права, етики та політики, які стосуються ШІ. Так, у розділі, який присвячений ролі ШІ в медіа, наголошується, що доцільно розмежовувати внутрішню та зовнішню прозорість, а також прозорість, яка стосується третіх осіб, які дослідники визначають у такий спосіб:

- внутрішня прозорість: наявність у працівників організації належних знань про систему ШІ, яку організація використовує;
- зовнішня прозорість: надання цільовій аудиторії системи ШІ інформації про таку систему; та
- прозорість, що стосується третіх осіб: наявність інформації про те, як система ШІ була натренована і як вона функціонує.²⁶

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

Ще в 2014 році Френк Паскуале та Даніель Сітрон обґрунтовували потребу в застосуванні концепції належної процедури до використання систем скорингу, зокрема тих, які використовують технологію ШІ, із тим, щоб такі системи забезпечували справедливість та точність.²⁷ У цьому ключі дослідники згодні з тим, що людина повинна бути поінформована про використання певного алгоритму щодо неї, а також у певних випадках мати можливість оспорювати

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

²⁵ Markus Dirk Dubber, Frank Pasquale, and Sunit Das, *The Oxford Handbook of Ethics of Ai* (New York: Oxford University Press, 2021), 204.

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

²⁷ Danielle Keats Citron and Frank Pasquale, "The Scored Society: Due Process for Automated Predictions," *Washington Law Review* 89 (2014), 1.

використання алгоритму.²⁸ Можливість оспорювати використання алгоритмів (розумних технологій) також підкреслюється в праці Мірей Хільдебрандт та Берта-Япа Купса, які зазначають, що необхідно розвивати інструменти, які сприяють прозорості, щоб рішення, які приймаються із використанням розумних технологій, могли піддаватися оскарженню.²⁹

Щодо цього питання Ніколас Діакопулос згадує принаймні три групи питань про систему ШІ, щодо яких доцільно отримати відповідь. Це включає:

- рівень та природу залучення людини до створення, функціонування та управління системою ШІ, включно з метою системи та особами, які є за неї відповідальними;
- дані, які використовувалися для тренування системи та які використовуються для її функціонування, для того, щоб визначити якість таких даних; та
- деталі про саму систему (модель) ШІ.³⁰

Водночас Ніколас Діакопулос критично оцінює необхідність того, щоб системи ШІ надавали пояснення стосовно прийняття своїх рішень (додатково до загальної дескрипції свого функціонування). Дослідник звертає увагу, що такі пояснення можуть бути приблизними, фрагментарними та неточними; натомість необхідно надати достатньо інформації про відповідні системи, щоб зацікавлені особи, включно з органами нагляду, змогли самостійно дійти до висновку в частині причин прийняття системою тих чи інших рішень.³¹

Крім обговорення питань щодо важливості прозорості та обсягу розкриття, який слідує із принципу прозорості, ми бачимо в науковій літературі деякі критичні позиції щодо цього принципу. До прикладу, часто наголошується, що лише прозорість не є достатньою для мінімізації всіх ризиків, пов'язаних із ШІ,

²⁸ Там же, 1.

²⁹ 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 (May 2010): 428–60, <https://doi.org/10.1111/j.1468-2230.2010.00806.x>, 460.

³⁰ Markus Dirk Dubber, Frank Pasquale, and Sunit Das, *The Oxford Handbook of Ethics of Ai* (New York: Oxford University Press, 2021), 202.

³¹ Там само, 205.

а натомість необхідно застосовувати комплексний підхід до регулювання ШІ. Крім цього, у контексті дискусії про прозорість існують сумніви щодо того, наскільки ефективно остання може застосовуватися на практиці. У цій дискусії згадуються обмежені ресурси регуляторних органів в частині перевірки технічних аспектів систем ШІ з огляду на складність сучасних систем ШІ, особливо заснованих на глибокому навчанні, де навіть розробники систем ШІ не можуть повністю пояснити логіку прийняття рішень. Інші проблемні аспекти та обмеження вже згадувалися вище: захист персональних даних, охорона об'єктів права інтелектуальної власності та проблема «інформаційного перевантаження», коли надмірна деталізація може зробити розкриття інформацію незрозумілою для кінцевих користувачів.

Незважаючи на проблемні аспекти, переважна більшість дослідників не ставить під сумнів, що прозорість (у певному вигляді) повинна бути однією з основних вимог щодо ШІ. Як результат теоретичний дискурс щодо прозорості алгоритмів та ШІ знайшов продовження у двох фундаментальних нормативних актах, які були прийняті на рівні Європейського Союзу, – а саме в 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 відповідних питань³². Так, згідно із регламентом, суб'єкту персональних даних повинно бути повідомлено про наявність у конкретному випадку автоматизованого ухвалення рішень щодо персональних даних такого суб'єкта, а також про логіку такої обробки даних, значимість та наслідки для

³²Nathalie A. Smuha, *The Cambridge Handbook of the Law, Ethics and Policy of Artificial Intelligence* (Cambridge, United Kingdom: Cambridge University Press, 2025), 146.

суб'єкта такої обробки даних.³³ Крім цього, такий суб'єкт повинен мати право не підлягати рішенню, яке ґрунтується винятково на автоматизованій обробці даних, що породжує правові наслідки для нього чи схожим чином істотно впливає на нього³⁴. Водночас контролер даних (в українській термінології – володілець персональних даних) зобов'язаний належним чином документувати всі процеси, пов'язані з обробкою персональних даних таким чином, зокрема, оцінювати їхній вплив на захист персональних даних.³⁵

Що стосується Акта про ШІ, він містить комплексні механізми забезпечення прозорості систем ШІ, які будуть застосовуватися до відповідних 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 щодо прозорості систем ШІ. По-перше, будь-яка система ШІ підпадає під загальний обов'язок розкриття факту взаємодії із ШІ; при цьому, додаткові зобов'язання щодо розкриття такого факту покладаються щодо тих систем, які безпосередньо взаємодіють з людьми. По-друге, високоризикові системи ШІ підпадають під додаткові зобов'язання, покликані забезпечити їхню прозорість, що включає 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 та користувачів систем ШІ. Незважаючи на технічні обмеження та виклики, пов'язані з регулюванням ШІ, саме прозорість дозволить належно відстежувати функціонування систем ШІ на практиці та вчасно реагувати на технологічні виклики. Водночас відсутність надмірності розкриття інформації щодо систем ШІ (збалансований підхід) повинно слугувати гарантією, що впроваджене

³³ Загальний регламент про захист даних, стаття 13(f).

³⁴ Там само, стаття 24.

³⁵ Загальний регламент про захист даних, стаття 35.

регулювання не буде перешкоджати подальшому науково-технічному прогресу у сфері ІІІ.

Висновки та перспективи подальшої розробки тематики ІІІ.

Прозорість є фундаментальним принципом регулювання систем ІІІ та передумовою ефективної реалізації інших принципів, зокрема підзвітності та відповідальності суб'єктів, які розробляють та використовують системи ІІІ. Водночас застосування прозорості вимагає належного збалансування всіх інтересів, врахування контексту його застосування та визнання потенційних обмежень щодо обсягу розкриття інформації про систему ІІІ в кожному окремому випадку. Такі обмеження включають особливості систем ІІІ, зокрема тих, які працюють за принципом «чорної скриньки», та обмеження, пов'язані із застосуванням законодавства про захист персональних даних та про охорону об'єктів права інтелектуальної власності. Незважаючи на такі обмеження, законодавці та дослідники питань ІІІ не заперечують важливості принципу прозорості, а закликають до більш ґрунтовної роботи під час розробки систем, що буде враховувати відповідні обмеження.

Вказані висновки та актуальна дискусія щодо прозорості систем ІІІ є важливою для України. На сьогодні в Україні формується свій підхід до регулювання ІІІ – на цьому етапі *bottom-up* підхід, коли перевага надається підготовці організацій до потенційного регулювання та саморегулюванню із подальшим прийняттям відповідних нормативно-правових актів щодо питань ІІІ. В умовах формування власного підходу необхідно відстежувати тенденції регулювання ІІІ, зокрема на рівні ЄС, а також проблематику такого регулювання, включно з межами прозорості систем ІІІ. До прикладу, у випадку України доречним буде розглянути можливість встановлення винятків щодо розкриття інформації про системи ІІІ з точки зору національної безпеки, якщо відповідні системи використовуються у секторі безпеки та оборони.

Водночас – в умовах задекларованого активного впровадження ІІІ в публічному секторі – необхідно забезпечити, щоб таке використання відповідало тим стандартам, які вже на сьогодні існують, наприклад, в Європейському Союзі,

тобто щоб в таких випадках забезпечувалися одночасно прозорість та підзвітність і відповідальність тих 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 будуть використані у дисертаційному дослідженні.

Список використаної літератури

- Кожухар, Олександр Георгійович. 2024. «Правове регулювання систем штучного інтелекту в ЄС: передумови, сучасний стан та перспективи». *Наукові записки НаУКМА. Юридичні науки* 13 (Жовтень):65-73. <https://doi.org/10.18523/2617-2607.2024.13.65-73>.
- Custers, Bart, and Eduard Fosch-Villaronga. *Law and artificial intelligence: Regulating AI and applying AI in legal practice*. The Hague: T.M.C. Asser Press, 2022.
- Danielle Keats Citron and Frank Pasquale, “The Scored Society: Due Process for Automated Predictions,” *Washington Law Review* 89 (2014).
- 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 (May 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 (November 12, 2017): 525–41. <https://doi.org/10.1007/s13347-017-0293-z>.
- Markus Dirk Dubber, Frank Pasquale, and Sunit Das, *The Oxford Handbook of Ethics of Ai* (New York: Oxford University Press, 2021)
- Murray, Andrew. “Almost Human: Law and Human Agency in the Time of Artificial Intelligence.” TMC Asser Press, April 25, 2021. <https://www.asser.nl/upload/documents/20240926T102230-AL6-Murray-WEB%20new.pdf>.
- Nathalie A. Smuha, *The Cambridge Handbook of the Law, Ethics and Policy of Artificial Intelligence* (Cambridge, United Kingdom: Cambridge University Press, 2025).
- Pasquale, Frank. *The Black Box Society*. Harvard University Press, 2015.
- Peter Cane et al., *The Oxford Handbook of Comparative Administrative Law* (Oxford, United Kingdom: Oxford University Press, 2021).

Bibliography

- Kozhukhar, Oleksandr. 2024. “Legal Regulation of Artificial Intelligence Systems in the EU: Prerequisites, Current State and Prospects”. *NaUKMA Research Papers. Law* 13 (October):65-73. <https://doi.org/10.18523/2617-2607.2024.13.65-73>.

- Custers, Bart, and Eduard Fosch-Villaronga. *Law and artificial intelligence: Regulating AI and applying AI in legal practice*. The Hague: T.M.C. Asser Press, 2022.
- Danielle Keats Citron and Frank Pasquale, “The Scored Society: Due Process for Automated Predictions,” *Washington Law Review* 89 (2014).
- 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 (May 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 (November 12, 2017): 525–41. <https://doi.org/10.1007/s13347-017-0293-z>.
- Markus Dirk Dubber, Frank Pasquale, and Sunit Das, *The Oxford Handbook of Ethics of Ai* (New York: Oxford University Press, 2021)
- Murray, Andrew. “Almost Human: Law and Human Agency in the Time of Artificial Intelligence.” TMC Asser Press, April 25, 2021. <https://www.asser.nl/upload/documents/20240926T102230-AL6-Murray-WEB%20new.pdf>.
- Nathalie A. Smuha, *The Cambridge Handbook of the Law, Ethics and Policy of Artificial Intelligence* (Cambridge, United Kingdom: Cambridge University Press, 2025).
- Pasquale, Frank. *The Black Box Society*. Harvard University Press, 2015.
- Peter Cane et al., *The Oxford Handbook of Comparative Administrative Law* (Oxford, United Kingdom: Oxford University Press, 2021).

O. H. Kozhukhar

The principle of transparency in the context of legal regulation of artificial intelligence systems

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 to ensure that it does not hinder further technological developments, while also protecting the rights of individuals who might be affected by AI

systems, including the 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, which is currently the leader in the relevant field, is important. Its risk-based regulatory framework and existing transparency requirements should be properly considered in Ukraine, especially amid Ukraine's commitment to implement EU acquis in accordance with the EU-Ukraine Association Agreement.

The discourse on AI regulation issues in the EU and beyond demonstrates that AI technologies - their development and subsequent use - must be transparent, where transparency is often construed broadly. Notably, transparency itself is an important safeguard against AI-related abuses and a prerequisite for implementing other key principles related to AI regulation, particularly accountability and responsibility 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 limitations in terms of personal data protection and protection of intellectual property rights.

The article explores the prerequisites for the emergence of the requirement for transparency of 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 that exist at the EU level.

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

Матеріал надійшов 14.03.2025