Омбудсман України
Ombudsman of Ukraine

Фінансується Європейським Союзом

FIIAPP
COOPERACIÓN ESPAÑOLA

Міністерство цифрової трансформації України

ПРАВА ЛЮДИНИ В ЕПОХУ ШТУЧНОГО ІНТЕЛЕКТУ

ВИКЛИКИ ТА ПРАВОВЕ РЕГУЛЮВАННЯ

2024

Права людини в епоху штучного інтелекту: виклики та правове регулювання — методичний матеріал, у якому розглядаються питання впливу новітніх технологій штучного інтелекту на права людини та підходи до його правового регулювання. А також запропоновані рекомендації щодо управління інтелектуальною системою відповідно до вимог національного законодавства та міжнародних стандартів.

Дана публікація розроблена в рамках міжнародного проєкту EU4DigitalUA у взаємодії з Офісом Омбудсмана та Міністерством цифрової трансформації України.

Участь у підготовці видання:

Уляна Шадська
Андрій Ніколаєв, Юлія Деркаченко, Володимир Бегей, Гордій Румянцев, Олег Дубно, Олександр Марченко

Проєкт EU4DigitalUA є частиною підтримки України Європейським Союзом. Погляди, думки та висновки, висловлені в тексті, належать виключно авторам і не обов›язково представляють позицію проєкту, Європейського Союзу або FIIAPP.

Омбудсман України
Ombudsman of Ukraine

Фінансується
Європейським Союзом

FIIAPP
COOPERACIÓN ESPAÑOLA

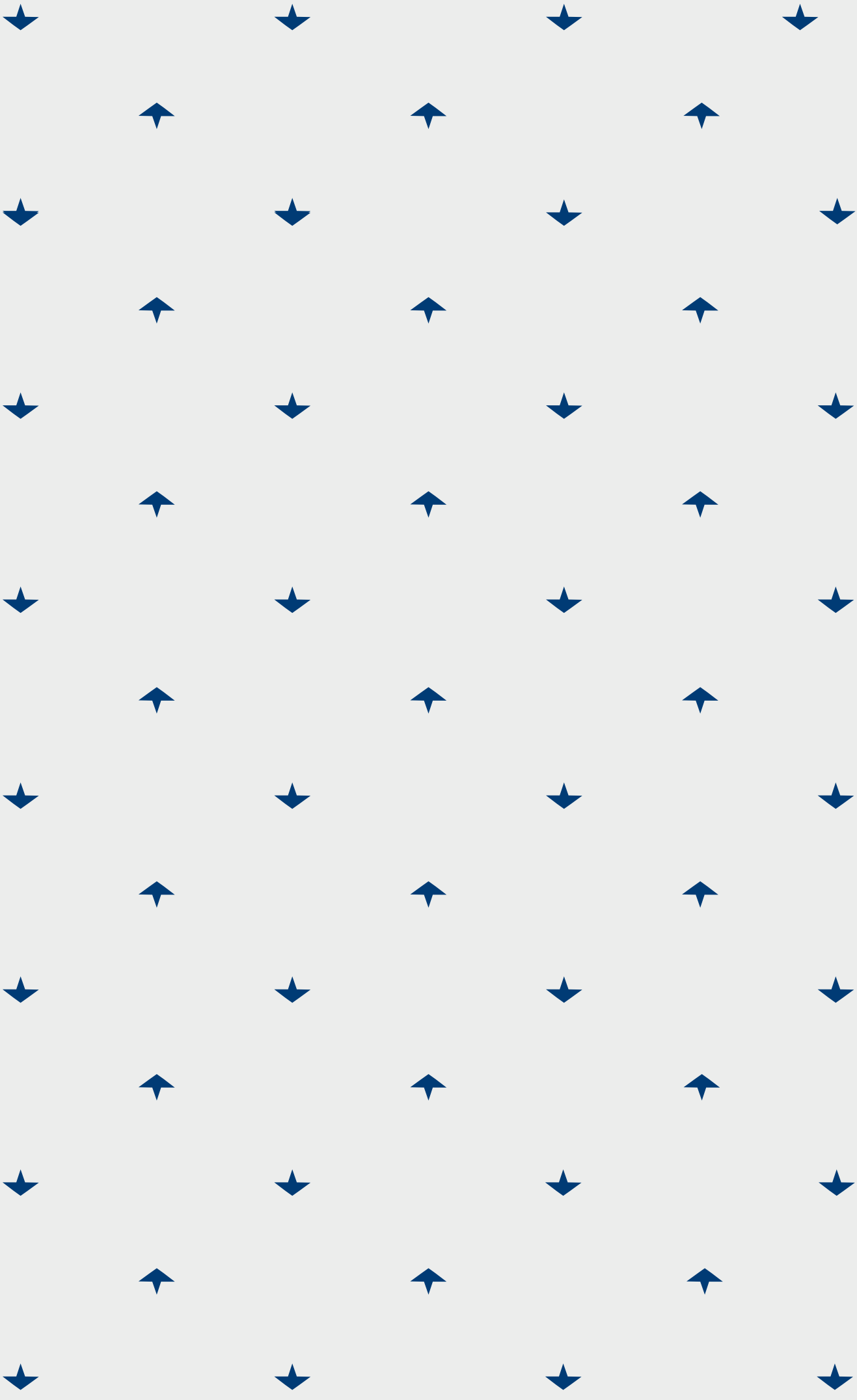
Міністерство
цифрової трансформації
України

ПРАВА ЛЮДИНИ В ЕПОХУ ШТУЧНОГО ІНТЕЛЕКТУ

ВИКЛИКИ ТА ПРАВОВЕ РЕГУЛЮВАННЯ

2024

ЗМІСТ



ПЕРЕДМОВА

Сьогодні штучний інтелект використовується майже в усіх сферах життєдіяльності людини. Новітні технології здатні виконувати різноманітні завдання: управляти автомобілем, виробничими процесами на підприємствах, генерувати текст, музику, розпізнавати обличчя та голоси людей, виконувати функції персонального асистента в смартфоні тощо. Вони вбудовані в різні пристрої, які щодня використовуються в державній політиці, міській інфраструктурі, бізнесі або просто в побуті. Попри широкі перспективи для суспільства, які можуть створювати інтелектуальні системи, потрібно також звернути увагу на етичні та правові аспекти їх використання, зокрема вплив на права та свободи людини.

Один із серйозних ризиків полягає в порушенні права на приватність[1]. Неправомірне або помилкове використання конфіденційної інформації про фізичну особу в системах штучного інтелекту може призвести до негативних для неї наслідків. Особливо коли це стосується даних, наприклад, про здоров'я людини, її статевої або етнічної приналежності, біометричних даних тощо. Це стосується як самої сутності технологій, так і особливостей їх застосування, що може призводити до складності оскарження автоматизованих рішень, упередженості або дискримінації. Ці аспекти часто пов'язані між собою.

Зацікавлені сторони, які беруть участь у життєвому циклі системи штучного інтелекту, включаючи організації чи окремих осіб, які розробляють, розгортають або використовують її, повинні запровадити організаційні та технічні заходити, щоб робота таких технологій була безпечною та відповідала положенням законодавства й міжнародним стандартам. Потрібна комплексна програма управління інтелектуальною системою, яка буде передбачати глибокий аналіз її роботи, зокрема впливу на права і свободи людини. Як показує практика, це може виявитися складним завданням, оскільки потрібно розуміти не тільки суть таких технологій і параметри їх використання, а ще й соціальний і юридичний контексти.

У зв'язку з цим, в рамках міжнародної ініціативи EU4DigitalUA у взаємодії з Офісом Омбудсмана та Міністерством цифрової трансформації України підготовлено методичний матеріал, у якому роз'яснено загальні аспекти впливу штучного інтелекту та підходи до його правового регулювання, зокрема під час обробки персональних даних. Пошук балансу між технологічним розвитком і захистом прав людини надзвичайно важливий, адже від цього буде залежати майбутнє суспільства.

Цей матеріал ґрунтується на положеннях національного і міжнародного законодавства, документах Ради Європи, Організації економічного співробітництва та розвитку (OECD), ООН, зокрема рекомендацій про етичні аспекти штучного інтелекту ЮНЕСКО. Враховані практики та роз'яснення

1 Понад 57 % споживачів розглядають використання штучного інтелекту при зборі та обробці персональних даних як значну загрозу для їхньої конфіденційності, згідно з дослідженням Міжнародної асоціації професіоналів у галузі захисту даних (IAPP) 2023 року. Режим доступу: https://iapp.org/resources/article/privacy-and-consumer-trust-summary/

наглядових органів у цій сфері, у тому числі Іспанського агентства з питань захисту даних (AEPD), Уповноваженого з питань інформації у Великій Британії (ICO), Національної комісії з обчислювальної техніки та свобод у Франції (CNIL) та інших. Також розглянуті експертні висновки, коментарі та рекомендації Уповноваженого Верховної Ради України з прав людини, Міністерства цифрової трансформації України, інших органів державної влади та українських громадських організацій.

1. ПОНЯТТЯ ТА РОЛЬ ШТУЧНОГО ІНТЕЛЕКТУ В СУЧАСНОМУ СУСПІЛЬСТВІ

У грудні 2020 року Кабінет Міністрів України затвердив[2] Концепцію розвитку штучного інтелекту в Україні, у якій визначені мета, принципи та завдання розвитку таких технологій— як одного з пріоритетних напрямів у сфері науково-технологічних досліджень[3].

У Концепції терміни використовуються в такому значенні:

Штучний інтелект (далі — технології ШІ) — організована сукупність інформаційних технологій, із застосуванням якої можливо виконувати складні комплексні завдання шляхом використання системи наукових методів досліджень та алгоритмів обробки інформації, отриманої або самостійно створеної під час роботи, а також створювати та використовувати власні бази знань, моделі прийняття рішень, алгоритми роботи з інформацією та визначати способи досягнення поставлених завдань.

Галузь штучного інтелекту — напрям діяльності у сфері інформаційних технологій, який забезпечує створення, впровадження та використання технологій ШІ.

У Європейському парламенті визначають ШІ як будь-який інструмент, що використовується програмою для відтворення поведінки, пов'язаної з людиною, такої як міркування, планування та творчість. Це поняття може бути розширено, оскільки ШІ вже може виходити за межі людських можливостей[4].

Суб'єкти ШІ — це усі ті, хто бере участь у життєвому циклі системи, включаючи організації та окремих осіб, які розгортають або керують ШІ.

Зацікавлені сторони — установи, організації, а також приватні особи, які безпосередньо чи опосередковано залучені до системи ШІ[5].

2 Розпорядження Кабінету Міністрів України «Про схвалення Концепції розвитку штучного інтелекту в Україні». Режим доступу: https://zakon.rada.gov.ua/laws/show/1556-2020-p#Text

3 Концепцію розроблено відповідно до плану пріоритетних дій Уряду на 2020 рік, затвердженого розпорядженням Кабінету Міністрів України від 9 вересня 2020 року № 1133.

4 Intelligence artificielle : définition et utilisation. Режим доступу: https://www.europarl.europa.eu/news/fr/headlines/society/20200827STO85804/intelligence-artificielle-definition-et-utilisation

5 OECD, Recommendation of the Council on Artificial Intelligence. Режим доступу: https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449

1.1. СФЕРИ ЗАСТОСУВАННЯ ШТУЧНОГО ІНТЕЛЕКТУ

Технології ШІ стрімко розвиваються в різних сферах. Медичні заклади та дослідницькі центри використовують ШІ для діагностики хвороб, вивчення медичних даних, розроблення індивідуальних підходів до лікування. Органи правопорядку впроваджують технології ШІ для забезпечення безпеки населення, прогнозування, запобігання та розслідування злочинів[6]. Наприклад, аналізуючи великі обсяги даних з камер відеоспостереження, соціальних мереж, телефонних розмов, виявляють патерни та аномалії, що можуть свідчити про потенційне правопорушення або загрозу національній безпеці в цілому.

Банківські та інші фінансові установи використовують програми зі ШІ для надання своїх послуг, дослідження економічних показників, обробки платежів та запобігання шахрайству. Також у сфері бізнесу ШІ допомагає автоматизувати рутинні завдання, таких як обробка замовлень, управління виробництвом та вивчення попиту. Різні компанії та сервіси, наприклад такі як Netflix, YouTube, Amazon, послугами яких користуються багато українців, обробляють за допомогою ШІ інформацію про своїх клієнтів, зокрема їхні поведінкові дані в мережі для створення маркетингових програм.

У галузі освіти ШІ застосовують для розробки індивідуальних підходів до навчання, оцінки знань, створення інтерактивних платформ тощо. Як зазначено на офіційному вебсайті Міністерства цифрової трансформації України: «Дані – нова нафта, штучний інтелект — нова електрика», — такими є реалії сучасності[7].

1.2. ВПЛИВ ШТУЧНОГО ІНТЕЛЕКТУ НА ПРАВА ЛЮДИНИ

Попри широкі перспективи для суспільства, що створюють сучасні технології ШІ, деякі з них можуть мати значний вплив на фундаментальні права і свободи людини. По-перше, ШІ може робити помилки. У світі вже є достатньо прецедентів, які доводять цей факт.

Наприклад, серед показових випадків — скандал у Великій Британії[8] у 2000–2014 роках, коли понад 700 співробітників поштової служби отримали покарання, а деякі навіть тюремне ув'язнення, за порушення, яких вони не вчиняли. Комп'ютерна програма компанії показала грошові недостачі, через що багатьох працівників притягнули до відповідальності. Знадобилися роки, щоб юристи довели, що система припустилася помилки. Існують й інші можливі ризики в роботі алгоритмів, які продемонстрували вчені. Ессекський університет у своєму дослідженні представив висновки, що частота помилок системи відеоспостереження британської поліції й розпізнавання облич становить 81 %[9]. Програма могла ідентифікувати з-поміж п'ятьох осіб чотирьох невинних як підозрюваних. Подібні результати також були опубліковані у звіті Джорджтаунського юридичного центру конфіденційності та технологій[10].

По-друге, робота інтелектуальних систем може передбачати обробку персональних даних. Це означає, що існує ризик порушення права людини на приватність. У січні 2020 року серед громадськості у різних країнах, у тому

6 За даними дослідження британської фінансової компанії Deloitte, у Китаї, Бразилії та Саудівській Аравії існує понад 1 000 проєктів розумних міст. Silicon Valley's scramble for China. Режим доступу: https://www.codastory.com/authoritarian-tech/silicon-valleys-scramble-for-china/

7 Мінцифра сформувала експертний комітет з питань розвитку сфери штучного інтелекту. Режим доступу: https://thedigital.gov.ua/news/mintsifra-sformuvala-ekspertniy-komitet-z-pitan-rozvitku-sferi-shtuchnogo-intelektu

8 Post Office scandal: What the Horizon saga is all about. Режим доступу: https://www.bbc.com/news/business-56718036

9 UK police's facial recognition system has an 81 percent error rate. Режим доступу: https://www.engadget.com/2019-07-04-uk-met-facial-recognition-failure-rate.html?guce_referrer=aHR0cHM6Ly93d3cuZ29vZ2xlLmNvbS8&guce_referrer_sig=AQAAAJC6imMAdnNgJ17SdmSfPn2zYD8McbsmvwlPrmjdfchxnLKvE1PwtQd9GHbVyMLxc-puxTLEAVeKSCIKf3DFtlU2EF4g7i9yQK9alYiV_3WkX2q-3DcHfJklyw-AwHWNZPupTIouU_uC3JeTaBHZ3_DtKL45scBzwqD4CqG3w3KM&utm_campaign=AI+Weekly&utm_medium=email&utm_source=Revue+newsletter&guccounter=1

10 Garbage in, garbage out. Face recognition on flawed data. Режим доступу: https://www.flawedfacedata.com/?utm_campaign=AI%20Weekly&utm_medium=email&utm_source=Revue%20newsletter

числі в Україні, велися дискусії11 щодо компанії Clearview AI, яка розробляє технології розпізнавання облич. Її система працює за допомогою ШІ й машинного навчання для збору та аналізу величезної кількості зображень людини, які вона отримує в мережі. Clearview AI заявила, що її продукт може ідентифікувати осіб за фотографіями, зробленими в реальному часі, порівнюючи їх із зображеннями у своїй базі даних, зібраними з відкритих джерел в інтернеті, таких як соціальні мережі, вебсайти новин та інші публічно доступні ресурси. Проблема в тому, що ця компанія збирає персональні дані осіб без їхньої згоди, що викликало занепокоєння щодо правомірності такої діяльності. У США проти Clearview AI було подано груповий позов, у якому компанію обвинуватили в продажі біометричних даних органам правопорядку12. Також діяльність цієї компанії заборонили в деяких європейських країнах. Попри це вона й надалі надає свої послуги по всьому світу. Неоднозначний характер цього питання породжує численні дискусії, які змушують у правовому полі знаходити баланс між перевагами технологій і ризиками. З одного боку, застосування ШІ може порушувати права людини, а з іншого — розв'язувати суспільні проблеми, наприклад через технологію ідентифікації швидко знайти небезпечного злочинця тощо.

Питання можуть стосуватися як самої сутності технологій ШІ, так і особливостей їх застосування. Це може бути пов'язано з відсутністю прозорості в розробленні та діяльності систем; ризиками упередженості та дискримінації; складністю оскарження автоматизованих рішень. Ці аспекти часто пов'язані між собою[13].

Через недостатню прозорість алгоритмів ШІ можуть виникати ситуації, коли люди, права яких порушують дії або рішення системи, не знають причини того, чому так відбулося, зокрема, чому їм було відмовлено в певній послузі або до них застосовано певне рішення. Наприклад, компанія Amazon розглядала резюме на вакантні посади за допомогою ШІ, але через деякий час виявилося, що програма відхиляла всі заявки за гендерними ознаками14. Ще один з резонансних скандалів був пов'язаний з доступом громадян до соціальної допомоги в Нідерландах15. У 2014 році під егідою Міністерства соціальних справ та праці Нідерландів кілька міст розпочали використовувати систему Systeem Risico Indicatie (далі—SyRI), спроєктовану для виявлення фактів шахрайства у сфері соціального забезпечення

11 Україна отримала доступ до бази системи розпізнавання облич Clearview AI. Режим доступу: https://zaxid.net/ukrayina_otrimala_dostup_do_bazi_sistemi_rozpiznavannya_oblich_clearview_ai_n1538330

12 In Big Win, Settlement Ensures Clearview AI Complies with Groundbreaking Illinois. Режим доступу: https://www.aclu.org/press-releases/big-win-settlement-ensures-clearview-ai-complies-with-groundbreaking-illinois

13 Rodriguez, 2020.

14 Amazon built an AI tool to hire people but had to shut it down because it was discriminating against women. Режим доступу: https://www.businessinsider.com/amazon-built-ai-to-hire-people-discriminated-against-women-2018-10

15 How Dutch activists got an invasive fraud detection algorithm banned. Режим доступу: https://algorithmwatch.org/en/syri-netherlands-algorithm/

населення. У процесі аналізу ризиків шахрайства SyRI обробляла дані отримувачів соціальної допомоги. Пізніше виявилося, що оцінювання ризиків у секторі, до якого належали люди з нижчими доходами, відбувалося нерівномірно, що викликало обурення в суспільстві та обвинувачення влади в дискримінації, оскільки потенційні бенефіціари не мали змоги зрозуміти механізми ухвалення рішень у роботі цієї системи. У 2020 році нідерландський суд визнав незаконним використання поточної версії SyRI, мотивуючи своє рішення порушенням права людини на приватне та сімейне життя відповідно до статті 8 Європейської конвенції з прав людини і основоположних свобод. Суд відзначив непрозорість системи, яка збирає надмірну кількість персональних даних без конкретних цілей.

Сьогодні в Україні мало досліджень подібних випадків, але це не означає, що їх нема. Можна сказати, що роботу в цьому напрямі тільки розпочато, зокрема це видання також має на меті привернути увагу суспільства до потреби вживати заходи для вивчення потенційних проблем використання ШІ як у приватному, так і державному секторі.

Як указано[16] в Концепції розвитку штучного інтелекту в Україні, впровадження інформаційних технологій є важливою складовою соціально-економічної, науково-технічної, оборонної та будь-якої іншої діяльності. Зокрема, зайняття Україною значного сегмента світового ринку технологій ШІ та провідних позицій у міжнародних рейтингах[17]. Проте відсутність концептуальних засад державної політики в цій галузі не дозволяє створювати та розвивати конкурентоспроможне середовище. Це свідчить про потребу розв'язання таких проблем як:

- низький рівень інвестицій у проведення досліджень зі ШІ у закладах вищої освіти;
- незначна кількість публікацій у виданнях провідних галузевих конференцій (CVPR\ICCV\ECCV — для комп'ютерного зору, NeurIPS, ICML, ICLR — для машинного навчання тощо) та провідних рецензованих виданнях;
- недосконаліть механізмів ухвалення управлінських рішень у публічній сфері, забюрократизованість системи надання адміністративних послуг, обмеженість доступу до інформації та її низька якість, недостатній рівень впровадження електронного документообігу між державними органами, а також низький ступінь оцифрованості даних, що перебувають у власності державних органів;
- складність перевірки відповідності роботи систем ШІ законодавству та етичним принципам;
- відсутність єдиних підходів, що застосовуються при визначенні критеріїв етичності під час розроблення та використання технологій ШІ для різних галузей, видів діяльності та сфер національної економіки;
- наявність ризиків зростання рівня безробіття у зв'язку з використанням технологій ШІ;
- низький рівень цифрової грамотності, поінформованості населення щодо загальних аспектів, можливостей, ризиків і безпеки використання ШІ;
- недостатній рівень інформаційної безпеки та захисту даних в інформаційно-телекомунікаційних системах державних органів внаслідок застарілості автоматичних систем виявлення та оцінювання інформаційних загроз, невикористання потенціалу прогнозування та передбачення загроз з метою своєчасної підготовки системи до можливої атаки;
- зростання кількості спроб несанкціонованого втручання в роботу автоматизованих системи, комп'ютерних мереж;
- відсутність або недосконаліть правового регулювання ШІ (у тому числі у сферах освіти, економіки, публічного управління, кібербезпеки, оборони), а також недосконаліть законодавства про захист персональних даних.

Очевидно, що технології ШІ надалі будуть розвиватися, розширюючи свої можливості у різних сферах, тому важливо аналізувати його вплив на права і свободи людини та створювати етичні й правові рамки.

16 Розпорядження Кабінету Міністрів України «Про схвалення Концепції розвитку штучного інтелекту в Україні». Режим доступу: https://zakon.rada.gov.ua/laws/show/1556-2020-p#Text

17 AI Readiness Index by Oxford Insights, AI Index by Stanford University тощо.

2. ПРАВОВЕ РЕГУЛЮВАННЯ ШТУЧНОГО ІНТЕЛЕКТУ

Україна є членом комітету зі штучного інтелекту при Раді Європи, а також бере участь у робочій групі з питань управління штучним інтелектом в Організації економічного співробітництва і розвитку[18]. У листопаді 2023 року під час міжнародного саміту щодо безпеки ШІ — AI Safety Summit, що проходив у Великій Британії, Україна підписала «Декларацію Бретчлі»[19] й таким чином доєдналася до міжнародної співпраці у дослідженні сфери безпеки ШІ. Відповідно до цього документа держави-учасниці мають взаємодіяти для подолання ризиків ШІ та сприяти тому, щоб його проєктування, розробка та використання здійснювалось у безпечний спосіб. Це стосується, як державних послуг у різних сферах, так і бізнесу. У Концепції розвитку штучного інтелекту в Україні визначено принципи, зокрема:

- розроблення та використання систем ШІ лише за умови дотримання верховенства права, основоположних прав і свобод людини і громадянина, демократичних цінностей, а також забезпечення відповідних гарантій під час використання таких технологій;
- відповідність діяльності та алгоритму рішень систем ШІ вимогам законодавства про захист персональних даних, а також додержання конституційного права кожного на невтручання в особисте і сімейне життя у зв'язку з обробкою персональних даних;
- забезпечення прозорості та відповідального розкриття інформації про системи ШІ;
- надійне та безпечне функціонування систем ШІ протягом усього його життєвого циклу та здійснення на постійній основі їх оцінювання та управління потенційними ризиками;
- покладення на організації та осіб, які розробляють, впроваджують або використовують системи ШІ, відповідальності за їх належне функціонування відповідно до зазначених принципів.

З урахуванням того, що робота технологій ШІ у багатьох випадках може передбачати обробку персональних даних[20], відповідно така діяльність підпадає під дію відповідного законодавства. У чинному Законі Україні «Про захист персональних даних» не враховані особливості роботи ШІ. Водночас Україна є стороною міжнародних угод та інших нормативно-правових документів, ратифікованих Верховною Радою України. Зокрема, у вересні 2017 року розпочала діяти Угода про асоціацію ЄС і України, де поряд з іншими вимогами, у статті 15 цієї Угоди визначені зобов'язання забезпечити захист персональних даних відповідно до європейських та міжнародних стандартів.

18 Organisation for Economic Co-operation and Development, Recommendation of the Council on Artificial Intelligence, OECD/LEGAL/0449.

19 The Bletchley Declaration by Countries Attending the AI Safety Summit, 1-2 November 2023. Режим доступу: https://www.gov.uk/government/publications/ai-safety-summit-2023-the-bletchley-declaration/the-bletchley-declaration-by-countries-attending-the-ai-safety-summit-1-2-november-2023

20 **Обробка персональних даних** — будь-яка дія або сукупність дій, таких як збирання, реєстрація, накопичення, зберігання, адаптування, зміна, поновлення, використання і поширення (розповсюдження, реалізація, передача), знеособлення, знищення персональних даних, у тому числі з використанням інформаційних (автоматизованих) систем.

Це означає, що міжнародні вимоги повинні бути враховані під час розроблення та застосування таких технологій. До того ж функціонує багато українських програм ШІ, які обробляють персональні дані осіб, які перебувають у країнах ЄС, тому вони підпадають під регулювання Загального регламенту про захист даних (далі — GDPR)[21]. Це також стосується міжнародного стандарту ISO/IEC 27701:2019[22], який розширює вимоги стандартів ISO/IEC 27001 і 27002 щодо інформаційної безпеки та захисту інформації, зокрема під час ідентифікації особи (PII); стандарту IEEE P7003™, що розробив Інститут інженерів електротехніки та електроніки (IEEE) для розв'язання конкретних викликів, пов'язаних зі ШІ. Цей стандарт звертає увагу на виявлення та усунення упереджень в алгоритмах ШІ, особливо під час обробки особливої категорії даних; та інших положень Ради Європи, ООН, Європейського суду з прав людини, які охороняються міжнародною системою в галузі прав людини. 18 грудня 2023 року Міжнародна організація зі стандартизації (ISO) опублікувала новий стандарт ISO/IEC 42001:2023, який містить вимоги щодо створення, впровадження, підтримки та постійного вдосконалення систем ШІ. Положення цього стандарту застосовуються до будь-яких установ чи організацій, незалежно від напрямку їх діяльності.[23]

Водночас потрібно звернути увагу, що в Декларації етики та захисту даних у штучному інтелекті24 визначений зв'язок між збором, використанням особистої інформації про людину та розвитком ШІ. Звідси виникає потреба в наведених нижче уточненнях:

1. Персональні дані є юридичною категорією інформації з особливими правилами, яких слід дотримуватися при розробці проєктів зі ШІ.

2. Не кожна система ШІ передбачає обробку персональних даних.

3. Персональні дані — це не єдина інформація, яка збирається, зберігається, аналізується чи використовується в розробках ШІ.

В Україні фактично тільки розпочався процес розробки правового регулювання ШІ. Міністерство цифрової трансформації України опублікувало Дорожню карту з регулювання штучного інтелекту в Україні, основою якої став bottom-up підхід[25], покликаний надати бізнесу практичних інструментів, таких як: регуляторна пісочниця, методології оцінки впливу ШІ на права людини, інструменти з маркування систем ШІ тощо.[26]

У більшості країн також ще немає спеціальних законів про ШІ[27]. Китай — виняток з його тимчасовими заходами з управління генеративними службами ШІ[28], що набрали чинності в серпні 2023 року. Цей документ спрямований на те, щоб генеративний ШІ відповідав «соціальному порядку та моралі», був точним, уникав дискримінації та дотримувався права на інтелектуальну власність. Національна стратегія штучного інтелекту Сінгапуру[29] складається з Модельної рамкової програми управління ШІ, посібника, у якому висвітлені практичні аспекти управління ШІ на організаційному рівні. Канадський закон про штучний інтелект та

21 GDPR (General Data Protection Regulation) — Загальний регламент про захист даних 2016/679, спрямований на захист фізичних осіб стосовно обробки персональних даних та вільний рух таких даних. Режим доступу: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN

22 ISO/IEC 27701:2019. Security techniques — Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management — Requirements and guidelines. Режим доступу: https://www.iso.org/standard/71670.html

23 ISO/IEC 42001 is an international standard that specifies requirements for establishing, implementing, maintaining, and continually improving an Artificial Intelligence Management System (AIMS) within organizations. Режим доступу: https://www.iso.org/standard/81230.html

24 Cfr. «Declaration on ethics and data protection in artificial intelligence». 40th International Conference of Data Protection and Privacy Commissioners. Tuesday, 23rd October 2018, Brussels.

25 Дорожня карта регулювання штучного інтелекту в Україні. Режим доступу: https://thedigital.gov.ua/news/regulyuvannya-shtuchnogo-intelektu-v-ukraini-prezentuemo-dorozhnyu-kartu

26 Дана ініціатива, на ряду з іншими, зазначена в проєкті Стратегії інновацій. Режим доступу: https://winwin.gov.ua/assets/files/Проєкт_інноваційної_стратегії.pdf?upd=1

27 На момент підготовки цього документа.

28 Temporary measures to manage artificial intelligence generative services. Режим доступу: https://www.chinalawtranslate.com/generative-ai-interim/

29 National Artificial Intelligence Strategy. Режим доступ: https://www.smartnation.gov.sg/initiatives/artificial-intelligence/

дані[30] як частина законопроєкту C-27, також ще доопрацьовується. В США сформовано федеральну політику щодо управління ШІ.[31] У Європейському Союзі розробляється новий загальний Регламент про штучний інтелект, який вже у 2024 році планують офіційно ухвалити з урахуванням перехідного періоду для його імплементації в діяльність суб'єктів ШІ.

Розуміння глобального правового контексту важливе, оскільки в більшості випадків технології ШІ мають транснаціональний вплив і вимагають балансу між прагненням до інновацій та етикою, технологією та правами людини. Глибоке розуміння цих взаємозв'язків дозволить створити ефективний законодавчий фреймворк для України.

30 The Artificial Intelligence and Data Act (AIDA) — Companion document. Режим доступу: https://ised-isde.canada.ca/site/innovation-better-canada/en/artificial-intelligence-and-data-act-aida-companion-document

31 Дані на момент написання цього документа — вересень 2023 року.

2.1. ПІДХІД ДО ПРАВОВОГО РЕГУЛЮВАННЯ В КРАЇНАХ ЄС

У Європейському Союзі розробляють положення, покликані врегулювати використання інформаційних технологій. Зокрема, вони стосуються конфіденційності у сфері електронних комунікацій[32], визначаючи, які положення GDPR будуть застосовуватися для захисту даних в інтернеті. Цей документ може мати серйозні наслідки для суб'єктів ШІ, які пропонуватимуть послуги електронного зв'язку. Далі — Закон про цифрові ринки (DMA), Закон про цифрові послуги (DSA) і Закон про управління даними (DGA). У 2023 році Європейський парламент ухвалив[33] проєкт Регламенту про регулювання ШІ (далі в тексті — AI Act)[34], концепцію якого запропонувала Європейська комісія ще у квітні 2021 року. Це положення є спробою створити загальну правову базу для всіх, хто розробляє або використовує інтелектуальні системи в країнах ЄС і не тільки. Він має стати прикладом уніфікації юридичних правил у галузі ШІ.

32 Директива Європейського парламенту і ради 2009/136/ЄС від 25 листопада 2009 року про внесення змін до Директиви 2002/22/ЄС про універсальну послугу та права користувачів щодо електронних комунікаційних мереж та послуг, Директиви 2002/58/ЄС про опрацювання персональних даних і захист приватності у сфері електронних комунікацій, Регламенту (ЄС) № 2006/2004 про співпрацю між національними органами, відповідальними за забезпечення виконання законів про захист прав споживачів.

33 Artificial Intelligence Act. Режим доступу: https://www.europarl.europa.eu/doceo/document/TA-9-2023-0236_EN.html

34 Artificial Intelligence Act. Законопроєкт Європейського Союзу, мета якого створити безпечне середовище для використання та розвитку ШІ. AI Act постав у відповідь на потребу в регулюванні технологій ШІ та їхнього впливу на суспільство.

Коротка хронологія і майбутні зміни законодавства у ЄС[35]:

Квітень 2021 року	Європейська комісія представила свою пропозицію Регламенту про штучний інтелект.
Грудень 2022 року	Європейська рада ухвалила спільну позицію (загальний підхід) щодо Регламенту про штучний інтелект36.
Червень 2023 року	Депутати Європарламенту ухвалили свою позицію щодо Регламенту про штучний інтелект.
Кінець 2023 року	Досягнуто політичної згоди щодо положень Регламенту про штучний інтелект.
Початок 2024 року	Очікується ухвалення остаточної версії Регламенту про штучний інтелект.
Кінець 2025 — початок 2026 року	Очікується, що після ймовірного 18–24-місячного перехідного періоду набере чинності Регламенту про штучний інтелект у ЄС.

Навколо AI Act точиться багато дискусій. З одного боку, лунають думки, що такий закон повинен обмежувати застосування деяких технологій ШІ, які можуть становити небезпеку для прав і свобод людини. З іншого — стверджують, що такий акт може зашкодити розвитку інновацій і соціальному прогресу загалом. Попри ці дискусії, усі сторони єдині в позиції, що технології ШІ потребують правового регулювання. Експерти ГО «Центр демократії та верховенства права» проаналізували[37] новий AI Act, виділивши важливі аспекти, на які варто звернути увагу. Зокрема, новий Регламент у ЄС:

- вимагатиме створення системи управління ризиками протягом усього життєвого циклу ШІ, а не тільки на етапі розробки;
- запроваджує обов'язкову сертифікацію для певних систем ШІ, зокрема тих, що здійснюють обробку особливих категорій даних, широкомасштабне профілювання людей, освітніх або професійних оцінювальних систем або критичної інфраструктури;
- містить положення про набори даних, які повинні бути актуальними, повними, без помилок та мати відповідні статистичні характеристики. Ця умова призначена для зниження потенційної упередженості систем і кількості дискримінаційних рішень;
- передбачає обмеження для систем, що потенційно можуть становити ризик для прав людини або державних інтересів. Наприклад, це стосується проблем дискримінації, дезінформації та інших маніпуляцій в інформаційному просторі тощо;
- встановлює вимоги для певних систем ШІ щодо необхідності інформування користувачів про те, що вони взаємодіють із системою ШІ, а не людиною;
- вимагає сприяти складанню Кодексів поведінки для суб'єктів ШІ залежно від цільового призначення відповідних систем;
- акцентує на потребі прозорості в розробленні та використанні систем ШІ;
- створює спеціальні регуляторні пісочниці. Концепція регуляторних пісочниць — один з інноваційних заходів, запропонованих AI Act, покликаний сприяти впровадженню систем ШІ в практику.

Отже, регулювання ШІ в країнах ЄС базується на ризикорієнтованому підході, також запропонованому в Білій книзі[38] штучного інтелекту у 2020 році. Але тоді в ній були описані лише два рівні ризику, потім це питання детальніше вивчили і сформували чотири рівні:

- системи ШІ з мінімальним ризиком або неризикові;

35 Contentious areas in the EU AI Act trilogues. Режим доступу: https://iapp.org/news/a/contentious-areas-in-the-eu-ai-act-trilogues/

36 Artificial Intelligence Act: Council calls for promoting safe AI that respects fundamental rights. Режим доступу: https://www.consilium.europa.eu/en/press/press-releases/2022/12/06/artificial-intelligence-act-council-calls-for-promoting-safe-ai-that-respects-fundamental-rights/

37 Ольга Петрів. Штучний інтелект та Artificial intelligence\ act: час для юридичних рамок. Режим доступу: https://cedem.org.ua/analytics/artificial-intelligence-act/

38 Commission White Paper on Artificial Intelligence: A European approach to excellence and trust, COM (2020) 65 final (February 19, 2020).

- системи ШІ з обмеженим ризиком;
- системи ШІ з високим ступенем ризику;
- заборонені системи ШІ.

Мінімальний ризик зумовлений низьким рівнем впливу на права та свободи фізичних осіб. Це може передбачати використання ШІ для автоматизації рутинних завдань, які не мають серйозних правових наслідків. Наприклад, обробка документів, генерація стандартних листів або повідомлень. На рівні *обмеженого ризику ШІ* може впливати на права та свободи осіб, однак це можна контролювати та регулювати. Користувачі таких ШІ мають усвідомлювати, що вони взаємодіють з машиною, та ухвалювати рішення — продовжувати чи припинити взаємодію. *Високий рівень ризику* вказує на можливість серйозного впливу на права, свободи та інтереси фізичних осіб. Застосування ШІ на цьому рівні, як правило, передбачає ухвалення автоматизованих рішень, що може мати юридичні наслідки. Такі системи ШІ повинні відповідати обов'язковим вимогам й пройти процедури оцінювання відповідності, перш ніж потрапити на ринок ЄС[39]. На постачальників і користувачів цих систем покладаються чіткі зобов'язання, зокрема:

- чітке та адекватне інформування про роботу технології;
- застосування заходів людського втручання для мінімізації ризиків порушення прав;
- реєстрація діяльності для забезпечення відстежуваності результатів;
- висока якість наборів даних, що живлять систему, для мінімізації ризиків і дискримінаційних результатів;
- детальна документація, що надає всю необхідну інформацію про систему та її призначення;
- забезпечення адекватних систем оцінювання та пом'якшення ризиків;
- забезпечення високого рівня надійності, безпеки та точності[40].

До заборонених технологій ШІ належать технології, які можуть становити загрозу для людини або суспільства загалом. Наприклад, використання таких програм для переслідування, маніпулювання, введення пропаганди, або застосування їх проти вразливих соціальних груп тощо.

Кожна із цих категорій ризиків має підкатегорії. Початковий список, запропонований Європейською комісією, зазнав перегляду як Європейською радою, так і парламентом. У своїх поправках Європейський парламент додав до класифікації високого ризику системи ШІ, які використовують певні платформи соціальних мереж (тобто ті, що позначені як «дуже великі онлайн-платформи» відповідно до Закону про цифрові послуги) створення рекомендацій для користувачів, особливо ті системи ШІ, за допомогою яких можна вплинути на результати виборів або інших демократичних процесів у державах[41].

Класифікація ризиків дає змогу розробникам чи користувачам ШІ визначити, у яких випадках така технологія може завдати шкоди. Загалом архітектура правозастосування AI Act нагадує GDPR, і ця паралель стає ще більш актуальна, враховуючи те, що деякі національні інституції з питань захисту персональних даних, наприклад Національна комісія Франції з інформатики та свободи (CNIL), уже позиціонують себе — як наглядовий орган у сфері ШІ.

Отже, якщо ЄС найближчим часом досягне своєї мети — ухвалить остаточний варіант AI Act, то очікується, що він набуде чинності не раніше 2026 року та буде діяти певний час, протягом якого зацікавлені сторони зможуть адаптувати свою діяльність для дотримання його норм. Ухвалення AI Act безпосередньо вплине й на регулювання ШІ в Україні, а це означає, що варто розпочинати працювати над механізмами реалізації та імплементації міжнародних стандартів в українські технологічні проєкти.

39 У статті 6 AI Act встановлено зобов'язання для систем ШІ з високим ризиком. У Додатку III перелічено вісім конкретних типів систем ШІ, які підпадають під визначення високого ризику.

40 Штучний інтелект та artificial intelligence act: час для юридичних рамок. Режим доступу: https://cedem.org.ua/analytics/artificial-intelligence-act/

41 Contentious areas in the EU AI Act trilogues. Режим доступу: https://iapp.org/news/a/contentious-areas-in-the-eu-ai-act-trilogues/

2.2. ПІДХІД ДО ПРАВОВОГО РЕГУЛЮВАННЯ В США

У США також активно формується федеральна політика в галузі ШІ. Зокрема, на різних рівнях висунуто низку ініціатив, законів і політик, які покликані забезпечити оцінювання ризиків і врегулювання роботи ШІ. Основа стратегії вже створена і дає загальне уявлення про юридичні й політичні підходи до регулювання нових технологій. Офіс політики науки та технології Білого Дому (OSTP) опублікував[42] Концепцію Закону про штучний інтелект (далі — Концепція). У ній наголошено на важливості технологічного розвитку в країні, але також висловлено занепокоєння щодо його впливу на права і свободи людини. Зокрема, випадками цифрового стеження, профілювання тощо. Тому у США запропоновано п'ять рівнів захисту, а саме:

1. Захист від небезпечних або неефективних систем.
2. Захист від цифрової дискримінації.
3. Захист персональних даних і від надмірного втручання в приватне життя людини.
4. Прозорість використання технологій ШІ, зокрема їхній потенційний вплив на права людини та навколишнє середовище.
5. Захист від автоматизованого ухвалення рішення.

Під час розроблення Концепції було розглянуто багато питань, зокрема:

- Що потрібно зробити, щоб розробники ШІ дбали про права людини ще на початку проєктування технології?
- Як зробити так, щоб технології ШІ та будь-які інші інновації використовувалися етично?

42 Blueprint for an AI Bill of Rights: A Vision for Protecting Our Civil Rights in the Algorithmic Age. Режим доступу: https://www.whitehouse.gov/ostp/news-updates/2022/10/04/blueprint-for-an-ai-bill-of-rightsa-vision-for-protecting-our-civil-rights-in-the-algorithmic-age/

У Концепції запропонована візія для суспільства, де захист прав людини стоїть на рівні з технологічним прогресом. Протягом розроблення цього документа досліджувався реальний вплив таких систем. Були враховані думки різних соціальних груп, які висловили своє бачення потреби чіткого правового регулювання ШІ й державних гарантій захисту в разі настання ризиків. Ця Концепція включає технічний додаток, у якому сформовані конкретні кроки, які можуть зробити громади, держані органи та інші сторони, щоб запровадити ключові принципи захисту від негативного впливу ШІ.

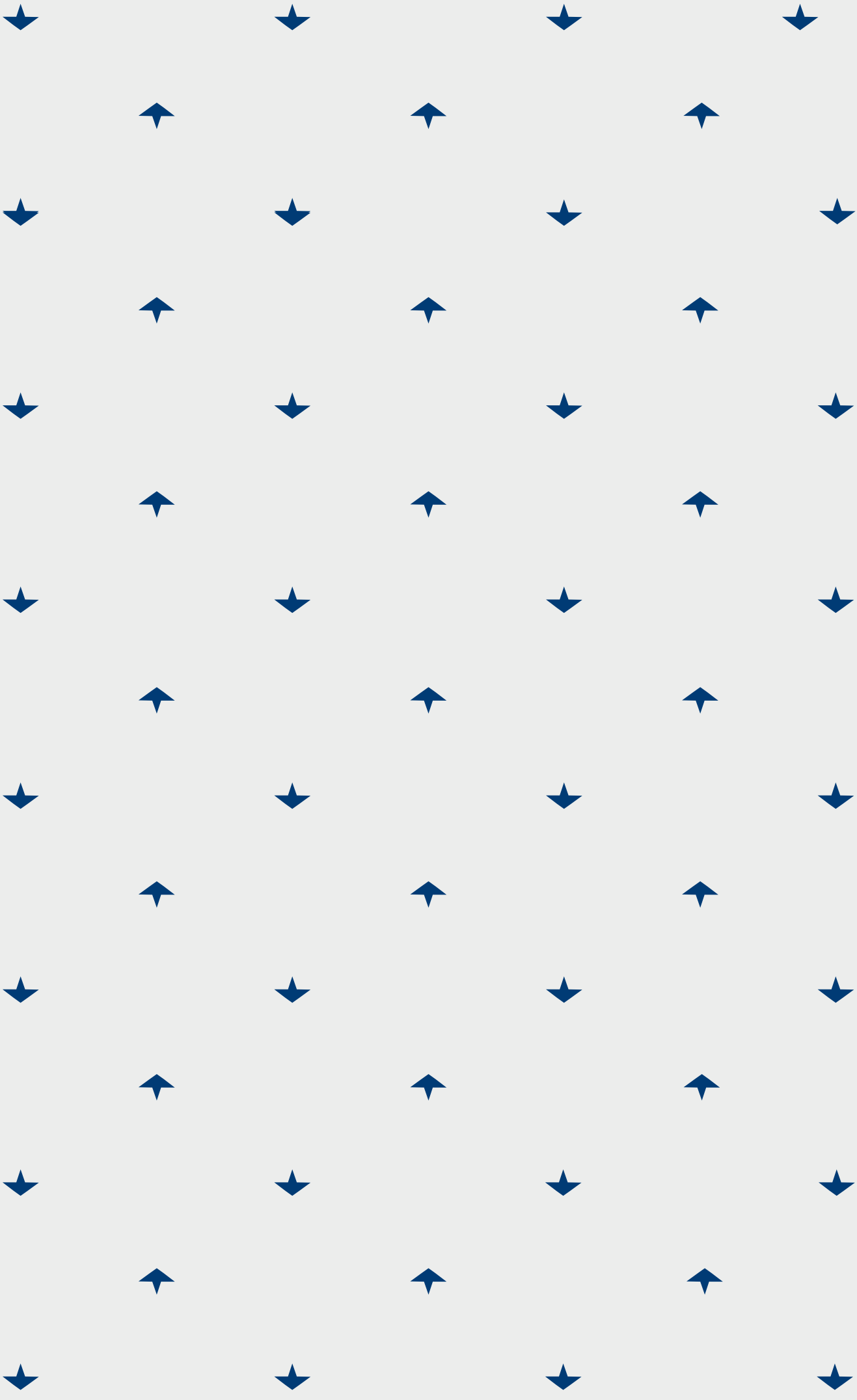
Відповідно до Концепції можна виділити декілька ключових аспектів, яким приділено увагу:

1. *Прозорість та зрозумілість.* Людина має право знати, як і коли ШІ використовується, і мати доступ до зрозумілої інформації про його принципи роботи.
2. *Запобігання дискримінації.* Системи ШІ повинні бути розроблені та використовуватися таким чином, щоб запобігти будь-яким формам дискримінації: на основі раси, статі, віросповідання, сексуальної орієнтації та інших характеристик.
3. *Захист приватності.* Люди мають право контролювати свої дані, які збираються й використовуються для технологій ШІ. У законах, які регулюють кожну галузь, мають бути передбачені вимоги до контролю за розвитком та використанням ШІ. Тобто ще на стадії розроблення будь-якого проєкту має бути вбудовано за замовчуванням принципи та стандарти, що захищають приватність людини. Пропонується посилити захист персональних даних, що стосуються чутливих сфер, включаючи здоров'я, роботу, освіту, кримінальне правосуддя та фінанси, а також молоді.
4. *Відповідальність і підзвітність.* Суб'єкти, які створюють або використовують системи ШІ, повинні бути відповідальними за свої дії й можливі наслідки. Технології повинні розвиватися, але під посиленим контролем з ефективним оцінюванням ризиків і дотриманням етичних рамок. Людина повинна бути захищена від автоматизованого ухвалення рішення в освіті, на роботі чи в інших сферах, що може обмежувати її права та свободи. Робота ШІ повинна бути максимально прозорою, тому в Концепції передбачена система звітування з боку розробників чи користувачів, особливо, якщо відбувається збір та обробка персональних даних. Такі звіти мають бути сформовані в зрозумілій формі та містити не тільки повідомлення про використання таких систем, а ще й мати оцінку впливу на права людини.
5. *Право на захист від автоматизованого ухвалення рішень.* Якщо люди стикаються з негативними наслідками внаслідок рішень, ухвалених системами ШІ, вони мають право на оскарження й виправлення. Тобто якщо рішення, яке стосується людини, ухвалила машина, тоді такий результат має бути перевірений і контрольований.

Також у Концепції наголошено на тому, що технічні можливості ШІ дуже швидко змінюються, а це означає, що потенційна шкода може виникати від використання навіть, на перший погляд, мало розвинених програм. Запропоновано двоетапний тест для визначення, які системи підпадають під дію документа: (1) автоматизованих систем, які (2) можуть мати істотний вплив на права, можливості чи доступ громадян до ключових ресурсів або послуг43. Таким чином, можна розбити висновок, що підхід США до врегулювання систем ШІ збігається з міжнародними стандартами та принципами, які визнані та застосовуються в інших країнах світу, зокрема ЄС.

Отже, вивчення досвіду інших країн щодо регулювання технологій ШІ є важливим завданням, оскільки Україна разом з іншими правовими, демократичними державами повинна прагнути до єдиних стандартів захисту прав і свобод людини в умовах розвитку технологій та кіберпросторі загалом. Знання про міжнародні принципи та правила регулювання ШІ може сприяти створенню середовища для наукових досліджень та інтеграції українських розробок на світовий ринок.

43 Data privacy. You should be protected from abusive data practices via built-in protections, and you should have agency over how data about you is used. Режим доступу: https://www.whitehouse.gov/ostp/ai-bill-of-rights/data-privacy-2/



3. МІЖНАРОДНІ ПРИНЦИПИ

У різних міжнародних положеннях запропоновано низку принципів, які утворюють загальноприйняті стандарти розвитку та правового регулювання технологій ШІ[44]. Наприклад, міжнародна група експертів Європейської комісії опублікувала посібник з етики для надійного штучного інтелекту[45], де сформовано концептуальні правила роботи ШІ залежно від контексту його використання. Зокрема, мова йде про:

a. *Законність.* Необхідно дотримуватися всіх законів і правил, визначених у міжнародних і національних положеннях.
b. *Етика та відповідальність.* Робота ШІ повинна відповідати етичним принципам і цінностям як місцевих, так і глобальних спільнот.
c. *Надійність.* Системи ШІ мають бути надійними та безпечними для людини.

За словами доцента інженерних систем і послуг Університету Умео Вірджинії Дігнум[46], оскільки розвиток машинного навчання дозволяє ШІ самостійно ухвалювати рішення та діяти без прямого контролю людини, тому на всіх рівнях повинна просуватися концепція етичного та відповідального ШІ, зокрема, яка має включати:

a. *Прозорість та підзвітність* — необхідність пояснювати та обґрунтувати рішення про розроблення та використання ШІ, які мають вплив на права і свободи людини.
b. *Відповідальність* і ролі людей виявляти помилки або неправомірні результати.

Розглянемо декілька принципів, які згадуються в міжнародних документах та практиках.

44 Доповідь Спеціального доповідача Генеральної Асамблеї ООН щодо права на недоторканність приватного життя Джозефа А. Каннатачі: «Штучний інтелект та недоторканність приватного життя, а також недоторканність приватного життя дітей».

45 The Ethics Guidelines for Trustworthy Artificial Intelligence (AI) is a document prepared by the High-Level Expert Group on Artificial Intelligence (AI HLEG). This independent expert group was set up by the European Commission in June 2018, as part of the AI strategy announced earlier that year. Режим доступу: https://ec.europa.eu/futurium/en/ai-alliance-consultation.1.html

46 The ART of AIDesign — Accountability, Responsibility, Transparency. Режим доступу: https://www.delftdesignforvalues.nl/2018/the-art-of-ai-accountability-responsibility-transparency/

ПРОЗОРІСТЬ

Прозорість — необхідність опису та перевірки механізмів, за допомогою яких системи ШІ ухвалюють рішення. Прозорість має важливе значення у контексті ШІ, бо вона сприяє формуванню довіри до таких технологій. Зрозуміти, як і чому система дійшла певного рішення, важливо для забезпечення надійності й передбачуваності. Особливо у сферах, де застосовуються системи автоматизованого ухвалення рішень. Забезпечення прозорості має позитивний вплив на проведення валідації[47] та сертифікації систем ШІ. Наприклад, якщо система приймає рішення щодо надання субсидії або кредиту, тоді важливо зрозуміти, які критерії оцінювання потенційних отримувачів були використані та чи відповідають вони юридичним вимогам.

Законодавчі рамки можуть вимагати від організацій прийняття прозорих і зрозумілих моделей ШІ. Якщо проти організації порушується судовий позов, прозорість їхніх систем ШІ сприяє чіткому поясненню того, як працює їхня технологія та чому вона прийняла певне рішення. Це може допомогти забезпечити можливість вжиття превентивних заходів у разі необхідності.

Тому важливо своєчасно надавати зрозумілі повідомлення про використання систем ШІ. Користувачі повинні отримувати повідомлення про використання автоматизованих систем заздалегідь. Пояснення повинно бути доступне разом із самим рішенням або невдовзі після нього. Повідомлення та пояснення можуть бути в різних форматах[48].

Один з документів, який вимагає забезпечувати цей принцип у роботі інтелектуальних систем, — це «Етичні настанови для надійного ШІ», розроблені Європейською комісією[49]. У ньому сформовані рекомендації щодо якісних і кількісних метрик, які дозволяють оцінювати прозорість систем ШІ. Також важливо розглядати концепцію права на пояснення, яка полягає у тому, що людина має право знати, яким чином система ШІ дійшла певного рішення, що може вплинути на її права та інтереси.

Звичайно, що абсолютна прозорість може бути недосяжною, оскільки вона залежить від функціональності конкретної системи. Також деякі деталі роботи алгоритмів можуть бути обмеженими в доступі з міркувань інтелектуальної власності або державної таємниці. Але це не означає, що не потрібно пояснювати, як працює ШІ, тоді в такому випадку лише певному колу суб'єктів, наприклад, контролюючим органам у цій сфері. Узагалі термін «прозорість» має багато визначень. У контексті цього принципу основна увага приділяється розкриттю інформації про те, як використовується ШІ. Прозорість не означає розкриття комерційної або іншої таємниці, що охороняється законом. Мова йде про те, що суспільство має знати загальну інформацію, як система ШІ використовується у відповідній галузі, щоб можна було зробити усвідомлений вибір і вберегти себе від можливих ризиків. Додатковий аспект прозорості стосується громадських консультацій та підвищення обізнаності населення щодо роботи ШІ. Такий підхід має підтримуватися в правовому суспільстві, де на першому місці стоїть людина, її права та свободи.[50]

Якщо за допомогою систем ШІ обробляються персональні дані, тоді пояснювати процес роботи з даними є юридичною вимогою. Обробка персональних даних має здійснюватися відкрито й прозоро із застосуванням засобів та у спосіб, що відповідають визначеним цілям. Тобто прозорість гарантує кожному отримання інформації про обробку своїх персональних даних і безпосередній доступ до них, адже людина має усвідомлювати не тільки потенційні вигоди від впровадження систем ШІ, а й власні ризики від його застосування. Володілець персональних даних зобов'язаний

47 **Валідація** — процес підтвердження відповідності (обґрунтованості) або надання законної сили.

48 Information Commissioner's Office «Guidance on AI and data protection». Режим доступу: https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/artificial-intelligence/guidance-on-ai-and-data-protection/

49 Ethics guidelines for trustworthy AI. Режим доступу: https://digital-strategy.ec.europa.eu/en/library/ethics-guidelines-trustworthy-ai

50 Blueprint for an AI Bill of Rights: A Vision for Protecting Our Civil Rights in the Algorithmic Age. Режим доступу: https://www.whitehouse.gov/ostp/news-updates/2022/10/04/blueprint-for-an-ai-bill-of-rightsa-vision-for-protecting-our-civil-rights-in-the-algorithmic-age/

пояснювати широкому загалу в доступній формі, для чого і яким чином ці дані отримує, як планує використовувати та кому вони можуть бути передані51.

Якщо подивитися на рекомендації державних регуляторів у країнах ЄС, то вимога до прозорості обробки персональних даних системами ШІ займає центральне місце. Зокрема у своїх перевірках ставлять питання до зацікавлених сторін ШІ: як забезпечується прозорість діяльності у використанні технологій? Наприклад, в Офісі інформаційного комісара Великої Британії (ICO) зосереджено увагу на тому:

- Де можна дізнатися інформацію про діяльність суб'єкта ШІ з питань обробки персональних даних?
- Яким чином інформація про обробку даних надається фізичним особам?
- Чи поінформовані суб'єкти персональних даних про свої права?[52]

Італійський орган захисту даних[53] зобов'язав інформувати людей про використання їхніх персональних даних у технологіях ШІ всіма можливими способами, зокрема за допомогою радіо, телебачення, газети та інтернету. Таке рішення стосувалося нової технології ChatGPT і змусило компанію-розробника OpenAI вжити перелік заходів щодо надійності, безпечності та захисту конфіденційної інформації в системі[54].

НЕУПЕРЕДЖЕНІСТЬ ТА НЕДИСКРИМІНАЦІЯ

Питання про створення неупереджених систем ШІ стало об'єктом численних дискусій і досліджень останніми роками. Важливо зазначити, що упередженість може бути як випадковою, так і навмисно внесеною в конкретну систему. Наприклад, випадки, коли відмовляють у кредитуванні, працевлаштуванні тощо людям похилого віку або самотнім вагітним жінкам. Наприклад, відома історія про міжнародну компанію Amazon, яка припинила використання ШІ для відбору персоналу через виявлену упередженість та помилки в алгоритмі, який базувався на шаблонах слів у резюме, неправильно обробляв інформацію.

Тому у системах ШІ має бути забезпечена можливість людського втручання. Для дотримання принципу недискримінації потрібно відповісти на такі питання: де та в якій формі необхідна присутність людської оцінки та аналізу? У яких випадках повністю автоматизоване ухвалення рішень є припустимим?[55] Якщо ШІ використовується для аналізу персональних даних, важливо гарантувати критичний підхід до вибору джерел, аналіз потенційних зміщень та оцінювання їх впливу на права людини. Це прямо відображено в законодавстві про захист персональних даних[56]. Тому для реалізації неупередженого використання ШІ слід підходити комплексно, аналізуючи усі стадії життєвого циклу системи, починаючи ще з етапу проєктування.[57]

МІНІМІЗАЦІЯ ДАНИХ

Принцип мінімізації даних полягає в тому, що обсяг інформації, особливо, яка містить персональні дані, потрібно зменшити до мінімального рівня. Можна збирати лише ті дані, які забезпечують досягнення цілей їх обробки[58]. З'ясувати,

51 Стаття 6 Закону України «Про захист персональних даних».

52 Generative AI: eight questions that developers and users need to ask. Режим доступу: https://ico.org.uk/about-the-ico/media-centre/blog-generative-ai-eight-questions-that-developers-and-users-need-to-ask/

53 *Garante* per la protezione dei dati personali.

54 Chat GPT : Garante privacy, limitazione provvisoria sospesa se OpenAI adotterà le misure richieste. L'Autorità ha dato tempo alla società fino al 30 aprile per mettersi in regola. Режим доступу: https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9874751#english

55 Blueprint for an AI Bill of Rights: A Vision for Protecting Our Civil Rights in the Algorithmic Age. Режим доступу: https://www.whitehouse.gov/ostp/news-updates/2022/10/04/blueprint-for-an-ai-bill-of-rightsa-vision-for-protecting-our-civil-rights-in-the-algorithmic-age/

56 Стаття 5 GDPR.

57 Information Commissioner's Office «Guidance on AI and data protection». Режим доступу: https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/artificial-intelligence/guidance-on-ai-and-data-protection/

58 Стаття 9 GDPR.

чи дотримано цей принцип, можна за допомогою таких питань:

- Чи дані збираються тільки для досягнення конкретних цілей (немає надлишкових даних)?
- Чи здійснюється аналіз обсягу даних?
- Чи існує процедура видалення надлишкових даних?

Наприклад, якщо формується база персональних даних (номери телефонів, електронні адреси тощо) для організації навчального курсу, автоматичної розсилки матеріалів та оцінки результатів, то не потрібно додатково збирати адреси місця реєстрації проживання людей. У разі, якщо така інформація збирається, це потрібно обґрунтувати. Іншими словами, принцип полягає в тому, що не варто збирати дані лише на випадок, що вони можуть стати в пригоді в майбутньому.

У контексті систем ШІ виникають певні виклики, пов'язані з принципом мінімізації даних, оскільки часто технології вимагають значного обсягу інформації. Серед можливих підходів для забезпечення відповідності цьому принципу в системах ШІ особливу увагу слід приділити плануванню обробки даних. Експерти з юридичної та технічної сфер повинні спільно визначати належні обсяги даних, враховуючи конкретний контекст подальшого їх використання. Системи ШІ здатні досягати більшої статистичної точності при використанні різних інформаційних джерел. Проте такий підхід одночасно може збільшувати ризик порушення приватності осіб. Тому важливо знаходити баланс між цими аспектами.

4. БЕЗПЕЧНІ ТА НАДІЙНІ ТЕХНОЛОГІЇ ШТУЧНОГО ІНТЕЛЕКТУ

У попередніх розділах було розглянуто питання щодо впливу новітніх технологій ШІ на права людини та міжнародні принципи, підходи та методи їх правового регулювання. Далі —буде зосереджено увагу на важливих заходах щодо управління інтелектуальною системою. Іншими словами, буде надано роз'яснення, які необхідно прийняти рішення, щоб технології ШІ були безпечними та відповідали вимогам законодавства.[59]

4.1. ПОПЕРЕДНІ КОНСУЛЬТАЦІЇ ТА ТЕСТУВАННЯ

Якщо мова йде про технології ШІ, які мають значний вплив на права людини, тоді на етапі розроблення, впровадження, розгортання або придбання системи варто проводити попередні консультації, які передбачають залучення експертів у різних сферах прав людини, зокрема з питань конфіденційності.

Звичайно, може постати питання про комерційну таємницю в приватному секторі або державну таємницю, що обмежує доступ до інформації широкому загалу. Але це не має означати, що технологію розробляють, впроваджують, а потім суспільство повинно вивчати наслідки. Розробники або ті, хто впроваджує ШІ, спочатку повинні переконатися, що інновації безпечні для суспільства. У разі виникнення негативних інцидентів довести, що отримали достатньо висновків зовнішніх експертів, що можна запускати такий проєкт. Тестування систем ШІ перш за все допомагає ідентифікувати ризики щодо порушення прав людини. Наприклад, дискримінацією або порушенням приватності. Під час аналізу системи впродовж тестування можна виявити проблеми та вжити заходи для їх виправлення ще перед впровадженням.

59 Комітети по всьому світу, наприклад Спеціальний комітет Ради Європи зі штучного інтелекту, нині працюють над створенням нормативної бази та кодексів етики для рішень на базі ШІ. Слід використовувати їхні висновки, а також інші відповідні керівні принципи щодо прав людини.

4.2. СИСТЕМНИЙ МОНІТОРИНГ Й АДАПТАЦІЯ

Після впровадження ШІ необхідно здійснювати системний моніторинг для виявлення проблем, що можуть виникнути в реальних умовах експлуатації. Зокрема, виявити ті ризики, які не були ідентифіковані під час тестування. Моніторинг повинен включати безперервне оцінювання шкоди, оновлення систем або перенавчання моделей машинного навчання за потреби. Варто враховувати продуктивність як технічних компонентів системи (алгоритм, а також будь-які апаратні компоненти, вхідні дані тощо), так і діяльність людини, яка, наприклад, виконує роль оператора системи.

Наприклад, компанія-розробник представила проєкт ідентифікації осіб за допомогою ШІ в системах відеоспостереження. Під час тестування система показала хороші результати, правильно розпізнавши обличчя в 99 % випадків. Проте після впровадження такої технології в реальному середовищі виявилося, що існують помилки за певними параметрами: погано освітлені обличчя або незвичайні кути огляду тощо. Попри високу точність у тестових даних, система може виявитися менш ефективною в реальних умовах через відмінності, які не були враховані під час навчання моделі.

4.3. АНАЛІЗ СТАТИСТИЧНОЇ ТОЧНОСТІ Й АКТУАЛЬНОСТІ ДАНИХ

Статистична точність належить до питань, які дані система ШІ вважає правильними або неправильними. Важливо зауважити, що слово «точність» має різне значення в контексті захисту персональних даних. Точність у законодавстві про захист даних визначається як один з фундаментальних принципів, який зобов'язує гарантувати, що персональні дані є точними та за потреби актуалізованими. Він вимагає вживання всіх розумних заходів, щоб переконатися, що персональні дані, які обробляються, не є «невірними або оманливими щодо будь-якого факту» і за потреби їх виправлено або видалено. У широкому сенсі точність у контексті ШІ (і загалом у статистичному моделюванні) стосується того, як часто система ШІ вгадує правильну відповідь, вимірювану на основі правильно позначених тестових даних. Тестові дані зазвичай відокремлюють від навчальних даних перед тренуванням або беруть з іншого джерела (або обох). Важливо, що в багатьох випадках відповіді, які дає система ШІ, будуть персональними даними. Отже, у цьому документі термін «точність» розуміється в контексті закону про захист даних; «статистична точність» — точності самої системи ШІ.

Покращення статистичної точності висновків системи ШІ є однією з важливих вимог для забезпечення дотримання принципу справедливості. Однак це не означає, що система ШІ повинна бути повністю статистично точною, щоб відповідати принципу точності. У багатьох випадках висновки системи ШІ не призначені для того, щоб їх розглядали як фактичну інформацію про особу. Натомість представляють статистично обґрунтовані припущення про те, що може бути правдою про особу зараз чи в майбутньому. Щоб уникнути неправильного тлумачення таких персональних даних як фактичних, потрібно забезпечити, щоб у записах (або внутрішніх документах) було вказано, що вони є статистично обґрунтованими припущеннями, а недостовірними фактами. Записи повинні містити інформацію про походження даних, а також систему ШІ, що використовувалася для генерації результату. Якщо висновок був заснований на неточних даних або система ШІ, використана для його створення, має статистичний дефект, це може вплинути на якість результату.[60]

Законодавство у сфері захисту даних, зокрема GDPR[61], визначає статистичну точність у контексті профілювання та автоматизованого ухвалення рішень. Тобто організації повинні застосовувати «відповідні математичні та статистичні процедури» для профілювання осіб як частину своїх технічних заходів і забезпечити виправлення будь-яких факторів, які можуть призвести до неточностей у персональних даних, щоб мінімізувати ризик помилок. Якщо системи ШІ використовуються для підготовки висновків про людей, тоді необхідно подбати, щоб система мала достатню статистичну точність для таких цілей. Загалом статистична точність як міра залежить від можливості порівняти результати висновків системи з деякою «реальною істиною». Скажімо, медичний діагностичний інструмент для виявлення певних видів захворювання може проводити оцінювання за допомогою якісних тестових даних, що містять відомі результати пацієнтів. У деяких інших галузях може бути недосяжна реальна істина, тому що немає якісних тестових даних або тому, що те, що було класифіковано, засновано на суб'єктивних судженнях (наприклад, який саме пост у соціальних медіа образливий тощо).

Неправильне розуміння статистичної точності може призвести до того, що ШІ будуть сприйматися як надзвичайно точні, хоча насправді вони просто відображають середні оцінки з набору людських міток, а не об'єктивну правду. Щоб уникнути цього, важливо відзначати, що висновки ШІ не повинні вважатися безапеляційною істиною. Навіть якщо система має високу статистичну точність щодо наявних даних, це не означає, що вона буде так само ефективно працювати, наприклад, якщо зміниться певні характеристики групи осіб або їх застосують до іншої групи в майбутньому. Робота ШІ може змінитися через різні чинники, і вона може стати менш статистично точною із часом.

Тому необхідно регулярно оцінювати такі «зміщення» та перенавчати модель на нових даних, якщо в цьому виникне потреба. Треба уникати «забруднення» системи застарілими, неточними або помилковими даними, які можуть викривлювати або погіршувати результати її роботи[62].

60 Under specification Presents Challenges for Credibility in Modern Machine Learning. Режим доступу: https://arxiv.org/pdf/2011.03395.pdf

61 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance). Режим доступу: https://eur-lex.europa.eu/eli/reg/2016/679/oj

62 Information Commissioner's Office «Guidance on AI and data protection». Режим доступу: https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/artificial-intelligence/guidance-on-ai-and-data-protection/

4.4. ПОШУК І ЗАБЕЗПЕЧЕННЯ ЯКОСТІ ДАНИХ

Важливо звернули увагу на джерела даних, які використовуються для навчання моделей ШІ, а також враховувати низку факторів, включаючи точність, репрезентативний характер і законність. У цьому контексті потрібно розглянути такі питання:

- Які джерела даних використовуються для навчання моделі ШІ?
- Як і від кого було отримано дані?
- Яку частку даних отримано із загальнодоступних джерел для навчання ШІ?
- На якій правовій підставі здійснюється збір і подальша обробка даних?
- Яким чином оцінюється зміст вихідних даних — вручну або автоматично?
- Чи вихідні дані є репрезентативними, неупередженими та забезпечено захист від несанкціонованого використання?

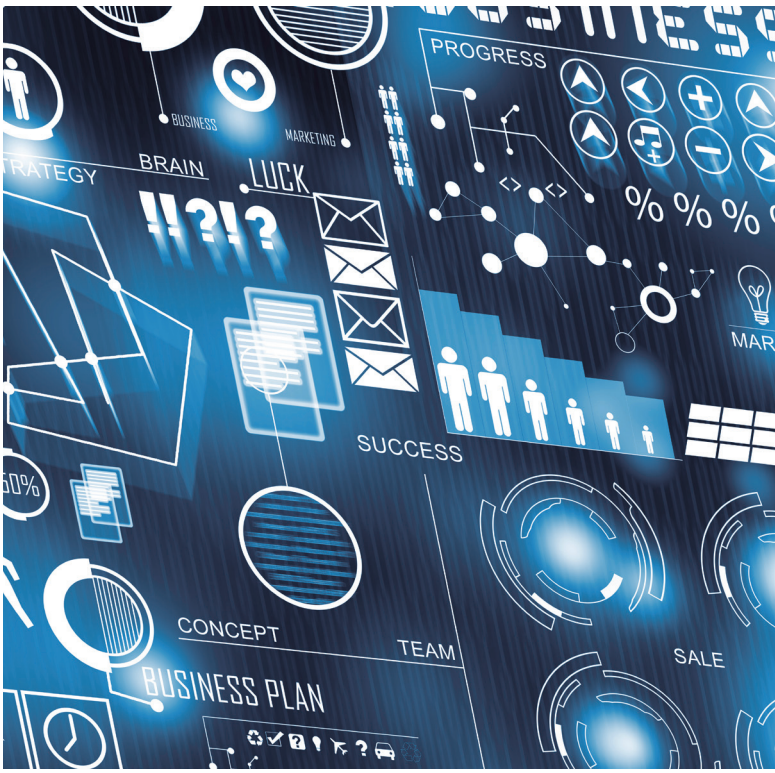
Наприклад, Комісія із захисту персональних даних Сінгапуру додатково рекомендує розглянути питання для кращого розуміння якості набору навчальних даних для підвищення точності та продуктивності моделі ШІ, а саме:

- Чи вихідні дані містять інформацію, захищену авторським правом?
- Чи вихідні дані містять особисту інформацію?63

Одним з ризиків при розробленні та використанні ШІ є ризик упередженості, який може бути викликаний попередньою конфігурацією алгоритму та якістю зібраних даних. Для того, щоб мінімізувати його, дані, які використовуються, повинні бути перевіреними та точними. Тому рекомендується:

- вести запис про походження даних;
- проводити аудит наборів даних, які використовуються при створенні алгоритмів;
- робити оцінювання якості наборів даних, які використовуються для навчання системи;
- регулярно оновлювати дані, які використовуються для навчання системи;
- мати окремі набори даних для навчання, тестування та перевірки процесу ухвалення рішень.

Водночас за можливості застосовувати інструменти анонімізації. Тобто визначати, чи необхідно, щоб дані, які використовуються, були пов'язані з конкретною особою. Якщо в цьому немає потреби, тоді краще використовувати анонімізовану інформацію, де особу не можна ідентифікувати. Таким чином, це дозволить зменшити ризики, пов'язані з обробкою та захистом персональних даних у проєктах і процесах ШІ[64].



63 Proposed advisory guidelines on use of personal data in ai recommendation and decision systems, 2023. Режим доступу: https://www.pdpc.gov.sg/-/media/files/pdpc/pdf-files/legislation-and-guidelines/public-consult-on-proposed-ag-on-use-of-pd-in-ai-recommendation-and-systems-2023-07-18-draft-advisory-guidelines.pdf

64 General Recommendations for the Processing of Personal Data in Artificial Intelligence. Document approved by the Entities member of the Ibero-American Data Protection Network in the 21 June 2019 session in Naucalpan de Juárez, Mexico.

4.5. СИСТЕМА ВІДПОВІДАЛЬНОСТІ

Якщо в автоматизованій системі стануться помилки, тоді це може призвести до компрометації, втрати або некоректної обробки інформації. Тому важливо мати чітку систему відповідальності для осіб, які розробляють, впроваджують або використовують системи ШІ. Наразі в Україні немає прямих положень у законодавстві, які б вимагали звітувати суб'єктів, відповідальних за розроблення або використання ШІ, як і механізму контролю за такими системами. Водночас варто розглянути міжнародну практику, оскільки законодавча регуляція може слугувати захистом інтересів громадян, бізнесу та держави, гарантуючи, що технології системи ШІ використовуються етично, прозоро та відповідально.

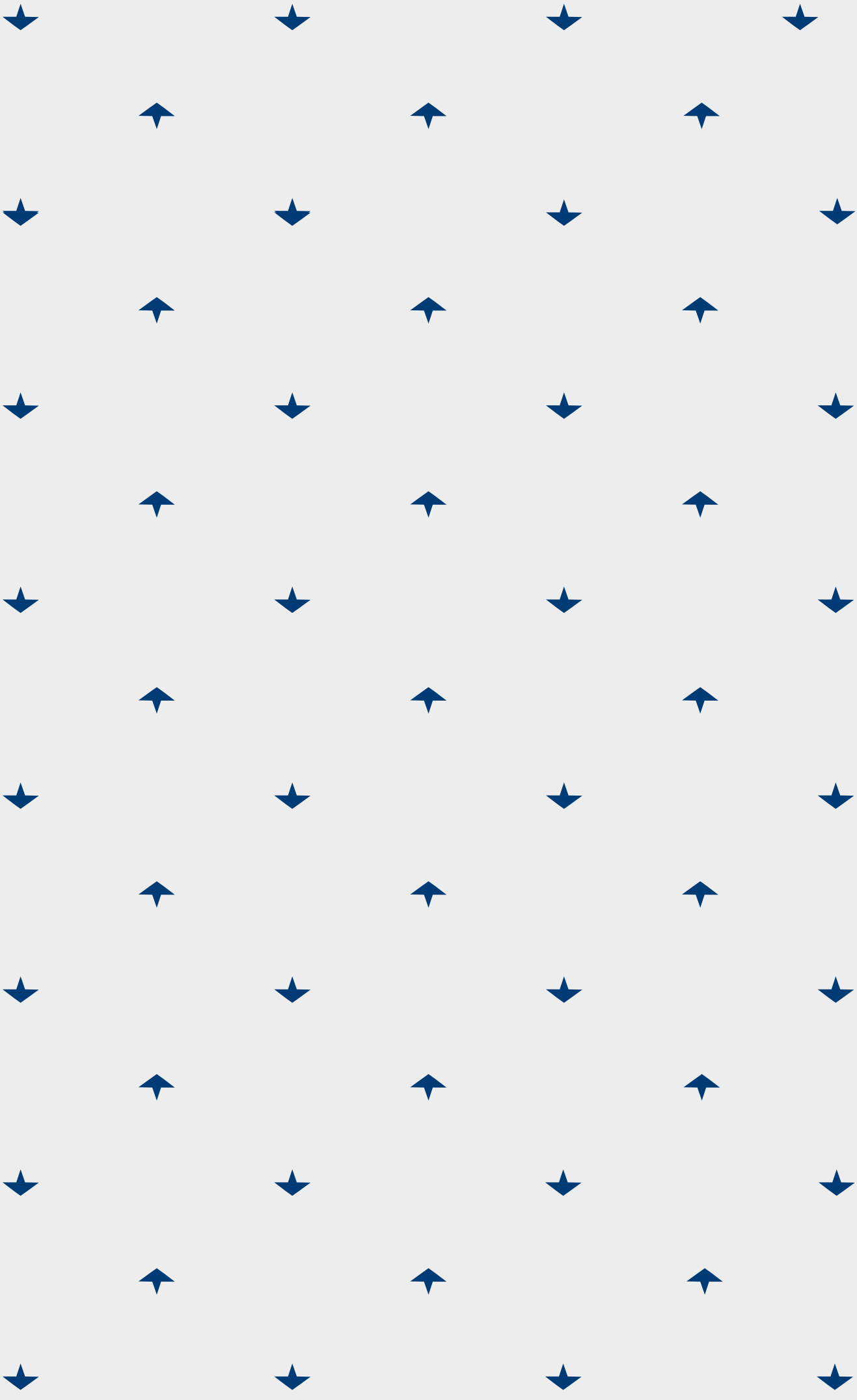
Серед поширених прикладів у контексті етичного та відповідального використання ШІ постає питання: хто буде нести відповідальність, якщо автономний автомобіль потрапить у ДТП і буде завдано шкоду пішоходу? Розробник автомобіля або програмного забезпечення, яке дало можливість ухвалювати рішення? Конструктор датчиків, які використовуються для сприйняття навколишнього середовища? Державна влада, яка дозволила пересування на дорогах такого транспортного засобу? Питання про відповідальність, якщо ШІ працює автономно, — найбільш дискусійне серед правників. Хтось вважає, якщо подія викликана дефектами конструкції, тоді питання до виробника. Якщо стався програмний збій — до розробника. Якщо так було запрограмовано від початку, тоді до тих, хто його навчив або запустив і так далі. Дехто вважає, що всі перелічені суб'єкти одночасно. У кожному разі має бути правова основа для розв'язання цього питання та вироблені відповідні підходи залежно від ступеня небезпеки й інших характеристик машини[65]. Те саме стосується систем, які працюють на основі персональних даних й ухвалюють рішення, які мають вплив на права людини.

У зв'язку із цим, важливо розглянути питання щодо юрисдикції, тобто визначення повноважень і компетенції судових або наглядових органів у розгляді справ, пов'язаних зі ШІ. Зокрема визначення *суб'єктів юрисдикції, наприклад* розробники, постачальники, користувачі систем тощо. *Сфери застосування* — види діяльності або ситуації. З огляду на транснаціональний характер сучасних технологій також важливо визначити, які законодавчі положення мають застосовуватися при розгляді справ, що мають міжнародний аспект або вплив.

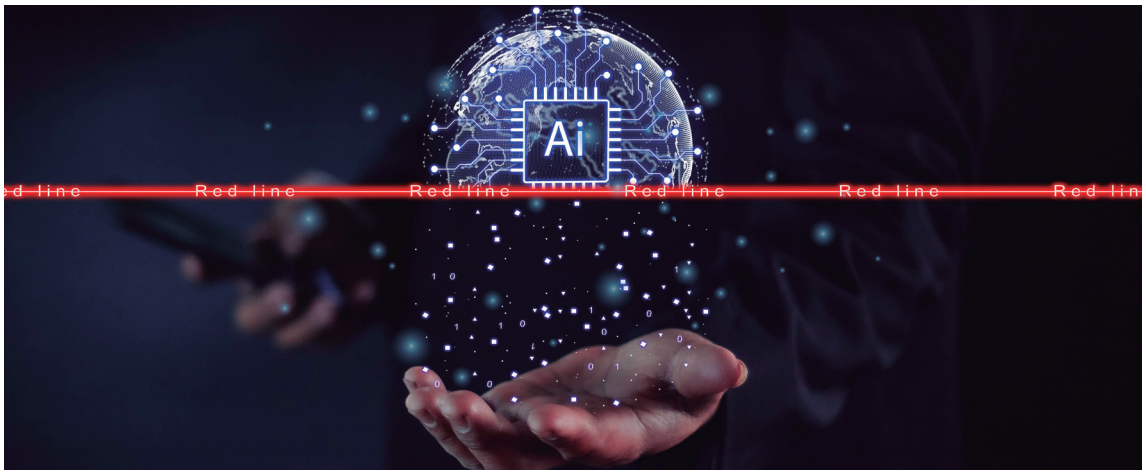
Отже, коли мова йде про безпеку й надійність систем ШІ, то необхідно мати відповіді на такі питання: що буде у разі непередбаченого сценарію? Надійність і безпека — це комплекс питань *«а що, якщо…?»*. Сценарії надійності, реакції механізму мають бути повністю опрацьовані й передбачені. Також важливо розуміти, яким чином людина зможе в разі потреби втрутитися в систему. Надійність системи ШІ повинна бути доведена протягом усього її життєвого циклу за допомогою аудитів.[66]

65 Several initiatives are aiming at proposing guidelines and principles for the ethical and responsible development and use of AI (see e. g. IEEE Ethically Aligned Design, the Asilomar principles, the UNI Global Union reflection on the future of work, the Barcelona declaration, or the EESC opinion, just to cite a few).

66 Blueprint for an AI Bill of Rights: A Vision for Protecting Our Civil Rights in the Algorithmic Age. Режим доступу: https://www.whitehouse.gov/ostp/news-updates/2022/10/04/blueprint-for-an-ai-bill-of-rightsa-vision-for-protecting-our-civil-rights-in-the-algorithmic-age/



5. ЗАБЕЗПЕЧЕННЯ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ



Як вже було зазначено раніше, більшість сучасних технологій ШІ передбачають обробку персональних даних. Це означає, що один із серйозних ризиків полягає в порушенні права людини на приватність. Неправомірна або помилкова обробка конфіденційної інформації про фізичну особу в системах ШІ може призвести до негативних для неї наслідків.

Тому зацікавлені сторони, включаючи організації чи окремих осіб, які розробляють, розгортають або використовують ШІ, повинні забезпечити захист персональних даних протягом усього його життєвого циклу системи[67]. Зокрема, зберігати справедливий баланс між інтересами, через які була створена інтелектуальна система, і правами та свободами осіб, на чиї дані ця система впливає.

67 Забезпечити право людини на повагу до приватного та сімейного життя відповідно до статті 8 Європейської конвенції з прав людини і основоположних свобод.

5.1. ПРОЄКТУВАННЯ СИСТЕМИ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ

Усі суб'єкти, що обробляють персональні дані, повинні спроєктувати належну систему їх захисту — privacy by design і privacy by default. Терміни *privacy by design*[68] і *privacy by default*[69] розробила екскомісарка з питань інформації та

68 *Privacy by design* (дизайн приватності) — означає, що особа, яка збирає дані, зобов'язана вбудувати систему їх захисту в усі процеси своєї діяльності ще на ранньому етапі їх проєктування і повинна підтримувати таку систему безперервно й надалі. По суті, у законі робиться акцент на превенції всіх можливих ризиків, наприклад витоку даних.

69 *Privacy by default* (конфіденційність за замовчуванням) — означає, що особам, чиї дані обробляються, не потрібно вживати жодних дій для захисту своєї конфіденційності, бо це має бути забезпечено за замовчуванням. Тобто в діяльність організацій повинні бути імплементовані відповідні технічні та організаційні заходи безпеки інформації. Тут доречно згадати принцип мінімізації даних: що менше даних організація збирає й обробляє, то менший ризик порушення закону.

конфіденційності провінції Онтаріо[70] Енн Кавукян[71]. У 2009 році вона опублікувала документ, де пояснила, що «вбудована конфіденційність» означає, що компанії повинні активно розглядати питання захисту даних протягом усього циклу їх обробки (full lifecycle protection): від збору інформації до її видалення. Починати роботу потрібно ще на етапі проєктування, гарантувавши, що всі дані надійно зберігаються, а потім своєчасно знищуються. Принципи privacy by design і privacy by default ухвалені більшістю країн як стандарт у сфері захисту даних. Так, у статті 25 GDPR визначено:

> *«Зважаючи на сучасний рівень розвитку, витрати на реалізацію, специфіку, обсяг, контекст і цілі обробки, а також ризики різної ймовірності та тяжкості для прав і свобод фізичних осіб, які може спричинити обробка, контролер повинен, у момент визначення засобів обробки та в момент власне обробки, вжити необхідних технічних і організаційних заходів, таких як використання псевдонімів, призначених для результативної реалізації принципів захисту даних, зокрема, мінімізації даних, і включення необхідних гарантій до обробки для досягнення відповідності вимогам цього Регламенту та забезпечення захисту прав суб'єктів даних. Контролер повинен вжити відповідних технічних і організаційних заходів для гарантування того, що за замовчуванням буде здійснювати обробку лише тих персональних даних, які є необхідними для кожної спеціальної цілі обробки. Такий обов'язок застосовують до кількості зібраних персональних даних, ступеня їхньої обробки, періоду їхнього зберігання та їхньої доступності».*

Наприклад, генеративний ШІ у вигляді чат-ботів пропонує можливість швидко та легко створювати різний контент. Відомі великі мовні моделі (LLM) — це ChatGPT, Luminous або Bard. У багатьох установах такі інструменти тепер стали частиною повсякденного робочого процесу, але часто їх використання не врегульовано. Той факт, що мовні моделі зазвичай працюють у хмарі, несе різні ризики порушення захисту персональних даних. Тому Комісар з питань захисту даних і свободи інформації у Гамбурзі опублікував[72] у листопаді 2023 року контрольний список питань щодо використання чат-ботів на основі великих мовних моделей (LLM) відповідно до вимог законодавства про захист персональних даних. У цьому документі виділено ключові аспекти, які необхідно враховувати при використанні чат-ботів на базі LLM, у тому числі:

- формулювання чітких внутрішніх інструкцій про те, коли та за яких умов слід використовувати генеративні інструменти ШІ;
- залучення спеціаліста із захисту даних (DPO) для розробки внутрішніх інструкцій, організації відповідних процесів з оцінки впливу на захист даних (DPIA);
- забезпечення конфіденційності даних у результатах роботи ШІ;
- усунення ризиків щодо витоків даних, упередженості та дискримінації у результатах роботи ШІ тощо.

Отже, законодавство, зокрема GDPR, зобов'язує забезпечити право людини на захист персональних даних на кожному етапі їх обробки, починаючи з проєктування продукту або послуги ШІ. Підхід «конфіденційність за допомогою дизайну» використовується скоріше для запобігання ризикам, а не усунення наслідків. Іншими словами, люди не повинні доводити своє право на недоторканість приватного життя, воно повинно захищатися за замовчуванням.[73]

70 Онтаріо — провінція на центральному сході Канади.

71 Ann Cavoukian, Ph.D. Privacy by Design. The 7 Foundational Principles. Режим доступу: https://www.ipc.on.ca/wp-content/uploads/resources/7foundationalprinciples.pdf

72 Checklist for the use of LLM-based chatbots. Режим доступу: https://datenschutz-hamburg.de/fileadmin/user_upload/HmbBfDI/Datenschutz/Informationen/20231113_Checklist_LLM_Chatbots_EN.pdf

73 Посібник «Аналіз ризиків під час обробки персональних даних: що важливо знати?». Детальніше з методологією оцінювання ризиків можна ознайомитися за посиланням: https://decentralization.gov.ua/uploads/library/file/774/Posibnyk_ocinka-ryzykiv-ZPD.pdf

5.2. ОЦІНЮВАННЯ РИЗИКІВ

Оцінювання ризиків — важлива складова проєктування системи захисту персональних даних та процесу обробки інформації за допомогою ШІ. Мова йде як про технічний захист систем, суті роботи *(уточ. для чого використовується ШІ)*, так і дотримання положень законодавства про захист персональних даних. Відповідно до міжнародних положень[74] фізичні або юридичні особи, які здійснюють обробку персональних даних, повинні проводити оцінювання ризиків[75], щоб передбачити ситуації, які можуть нести загрози для прав і свобод людини ще до початку їх настання.

Цей процес може відбуватися різними способами й стосуватися як технічної частини роботи системи *(див. Розділ 4)*, так і організаційних процесів. Наприклад, у європейському законодавстві оцінювання впливу на захист персональних даних, або Data Protection Impact Assessment (далі — DPIA), — це процедура, передбачена статтею 35 GDPR, а також іншими документами, які визначають міжнародні стандарти безпеки даних[76]. DPIA — це процес, покликаний допомогти аналізувати, виявляти й мінімізувати ризики для персональних даних під час їх обробки. Невиконання DPIA, коли це обов'язково, може призвести до притягнення до відповідальності. Наприклад, пунктом 84 GDPR визначено, що *«...контролер повинен нести відповідальність за проведення оцінювання впливу на захист даних з метою визначення, зокрема, походження, специфіки, особливості та ступеня тяжкості такого ризику. Необхідно враховувати результати оцінювання під час визначення належних заходів, яких необхідно вжити для підтвердження того, що опрацювання персональних даних відповідає цьому Регламенту»*[77].

Іншими словами, законодавець наголошує, що DPIA — це систематичний процес, який має бути інтегрований на постійній основі. Тобто кожна установа чи організація повинна розробити свою методологію, яка буде враховувати специфіку її діяльності та потреби в оцінюванні ризиків. Загалом головна мета цього процесу — відповісти на питання:

- Які існують загрози?
- Які джерела їх виникнення?
- Які наслідки можуть настати?
- Що потрібно зробити, щоб їх усунути?

Оцінювання потрібно робити, якщо запускається новий проєкт, з'являються нові цілі та збирається інший вид даних, зокрема, яка належить до спеціальної категорії; змінюється програмне забезпечення за допомогою якого здійснювалася обробка інформації тощо. Окрім цього, провести оцінювання варто в таких ситуаціях:

- Об'єднання декількох баз даних в одну (що не рекомендовано робити, оскільки агрегація баз даних може нести багато загроз).
- Створення нових баз даних або впровадження нових процесів обробки інформації.
- Залучення нових сторін. Наприклад, реалізація проєктів з використанням сторонніх постачальників.
- Додавання нових функцій у наявний продукт або послугу.

У чинному українському законодавстві немає зобов'язань щодо типів обробки, які підлягають оцінюванню, але європейські стандарти, на які має орієнтуватися Україна, такий перелік містять. Так, наприклад, у статті 35 (3) GDPR визначено три типи обробки, для яких завжди потрібно DPIA:

Систематичне й масштабне профілювання фізичних осіб: *(А)* **«***систематичного та масштабного*

74 Standards ISO-29134 «Guidelines for privacy impact assessment», ISO-31000 «Risk management. Principles and guidelines», ISO-31010 «Risk management. Risk assessment techniques».

75 Під поняттям «ризик» мається на увазі сценарій, що описує подію, її причини та наслідки, а також оцінюється з погляду складності та ймовірності.

76 «The Practical Guide for Data Protection Impact Assessments subject to the GDPR» published by the AEPD. Standards ISO-29134 «Guidelines for privacy impact assessment», ISO-31000 «Risk management. Principles and guidelines» and ISO-31010 «Risk management. Risk assessment techniques».

77 Офіційний переклад Регламенту Європейського парламенту і Ради (ЄС) 2016/679 про захист фізичних осіб у зв'язку з опрацюванням персональних даних і про вільний рух таких даних, та про скасування Директиви 95/46/ЄС.

оцінювання персональних аспектів, що стосуються фізичних осіб, яке ґрунтується на автоматизованому опрацюванні, в тому числі профайлінгу, та на якому ґрунтуються рішення, що мають юридичні наслідки щодо фізичної особи чи подібним чином істотно впливають на фізичну особу».

- Широкомасштабного опрацювання спеціальних категорій даних**:** *(B) «широкомасштабного опрацювання спеціальних категорій даних, вказаних у статті 9 (1), та персональних даних про судимості і кримінальні злочини, вказані в статті 10».*
- Громадський моніторинг: (C) «систематичного та широкомасштабного моніторингу зони, що знаходиться у відкритому доступі»78.

Відповідно до статті 29 GDPR особа, що збирає дані, встановлює відповідні інструкції для їх обробки та захисту. Робоча група органів ЄС у сфері захисту персональних даних опублікувала[79] керівні принципи, які можуть виступати індикаторами обробки з високим ступенем ризику, наприклад, коли:

- Обробка персональних даних здійснюється за допомогою інноваційних технологій, зокрема ШІ.
- Застосовується автоматизоване ухвалення рішень.
- Обробка медичних, біометричних або генетичних даних (окрім випадків, коли це здійснюється медичними працівниками для надання допомоги людині).
- Обробка, яка включає відстеження геолокації або поведінки людини, включаючи, окрім іншого, онлайн-середовище.
- Обробка персональних даних дитини, зокрема в маркетингових цілях.
- Якщо обробка даних має такий характер, що витік цієї інформації може нести загрозу для здоров'я або фізичної безпеки людей[80].
- Застосовується масштабне профілювання людей[81].

Згідно із Законом про цифрові послуги (Digital Services Act, DSA), який у 2022 році набув чинності в ЄС, передбачені спеціальні положення для великих онлайн-платформ або пошукових систем — Very Large Online Platforms (VLOP) та Very Large Search Engines (VLSE), що налічують понад 45 мільйонів користувачів. Такі суб'єкти зобов'язані щороку проводити широкомасштабне оцінювання ризиків можливого негативного впливу їхніх сервісів, наприклад, щодо доступу до нелегальних товарів, контенту чи поширення дезінформації. Окрім того, VLOP і VLSE повинні проводити всеосяжний аналіз загроз для основоположних прав людини і громадянина. Наприклад, у зв'язку із цим у компанії Google заявили, що внесли низку змін до своєї політики. Зокрема, розширено доступ [регуляторів] до даних, що стосуються ведення адресних рекламних кампаній, а також розкрито більше інформації про модерування сервісів і пошукових систем. У компанії Meta повідомили про те, що Facebook та Instagram припинили вести рекламні кампанії, націлені на підлітків.

Разом з тим, якщо проаналізувати рекомендації державних регуляторів у сфері захисту персональних даних у європейських країнах, то більшість з них наголошує, що навіть якщо обробка даних за допомогою систем ШІ не належить до категорій високого ризику, де закон зобов'язує здійснювати DPIA, з урахування розвитку технологій й того, що ще немає остаточного розуміння реального впливу на права і свободи

78 Офіційний переклад Регламенту Європейського парламенту і Ради (ЄС) 2016/679 про захист фізичних осіб у зв'язку з опрацюванням персональних даних і про вільний рух таких даних, та про скасування Директиви 95/46/ЄС.

79 Guidelines on Data Protection Impact Assessment (DPIA) (wp248rev.01). Режим доступу: https://ec.europa.eu/newsroom/article29/items/611236

80 Приклади операцій, що вимагають DPIA, та які критерії є високим ризиком в поєднанні з іншими, що «можуть призвести до високого ризику». Режим доступу: https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/accountability-and-governance/data-protection-impact-assessments-dpias/examples-of-processing-likely-to-result-in-high-risk/

81 Профілювання означає будь-яку форму автоматизованої обробки персональних даних, що складається з використання особистої інформації людини для оцінювання певних аспектів, наприклад, що стосуються її роботи, соціального статусу, здоров'я, особистих уподобань, місцезнаходження, переміщення тощо.

людини, усе одно варто робити оцінювання ризиків[82].

Процес оцінювання ризиків можна здійснювати в декілька етапів. Наприклад, спочатку — проаналізувати напрями роботи у сфері обробки персональних даних загалом. Далі — визначити, для чого потрібно проводити цю процедуру, адже від мети аналізу буде залежати сценарій і зміст його методології, а також те, скільки треба часу, ресурсів і який очікуваний результат. Для початку треба скласти методологію оцінювання, сконцентровану саме цій діяльності. Коли є детальний профіль суб'єкта *(тобто конкретної організації)*, визначена ціль і методологія аналізу, настає етап оцінювання ризиків[83]. Оскільки проєкти використання ШІ дуже різні, у тому числі різні цілі та процеси обробки персональних даних, має бути складена індивідуальна адаптована методологія оцінювання ризиків, з розбивкою на етапи застосування технології. Для виконання цього процесу можна залучати сторонніх експертів, які мають відповідну кваліфікацію в цій сфері. З огляду на складний і динамічний характер ШІ, це не тільки допоможе ефективно долати виклики у сфері захисту даних, а ще й може слугувати конкурентною перевагою.

82 Information Commissioner's Office «Guidance on AI and data protection». Режим доступу: https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/artificial-intelligence/guidance-on-ai-and-data-protection/

83 Посібник «Аналіз ризиків під час обробки персональних даних: що важливо знати?». Детальніше з методологією оцінювання ризиків можна ознайомитися за посиланням: https://decentralization.gov.ua/uploads/library/file/774/Posibnyk_ocinka-ryzykiv-ZPD.pdf

5.3. ВИЗНАЧЕННЯ ПІДСТАВ ДЛЯ ОБРОБКИ ПЕРСОНАЛЬНИХ ДАНИХ

Якщо система ШІ передбачає обробку персональних даних, то така діяльність повинна бути обґрунтованою згідно із законом. Тобто має бути правова основа. У статті 11 Закону України «Про захист персональних даних» визначені підстави для обробки персональних даних:

1. згода суб'єкта персональних даних на обробку його персональних даних;
2. дозвіл на обробку персональних даних, наданий володільцю персональних даних відповідно до закону виключно для здійснення його повноважень;
3. укладення та виконання правочину, стороною якого є суб'єкт персональних даних або який укладено на користь суб'єкта персональних даних чи для здійснення заходів, що передують укладенню правочину на вимогу суб'єкта персональних даних;
4. захист життєво важливих інтересів суб'єкта персональних даних;
5. необхідність виконання обов'язку володільця персональних даних, який передбачений законом;
6. необхідність захисту законних інтересів володільця персональних даних або третьої особи, якій передаються персональні дані, крім випадків, коли потреби захисту основоположних прав і свобод суб'єкта персональних даних у зв'язку з обробкою його даних переважають такі інтереси.

Хоча використання ШІ принципово не відрізняється від іншої обробки даних, але все-таки існують деякі особливості. Наприклад, системи, засновані на машинному навчанні, потребують використання даних для навчання, перш ніж вони будуть застосовуватися на етапі роботи. За умови, що цей етап навчання дуже відрізняється від етапу оперативного впровадження системи ШІ. Його виняткова мета — підвищення продуктивності системи ШІ. Водночас важливо зазначити, що правова підстава як «наукові дослідження» сама собою не може бути правовою основою для обробки. Тільки ті правові основи, що прямо перелічені в законі.[84]

Важливо звернути увагу, якщо системи ШІ впроваджує суб'єкт владних повноважень, то відповідно до статті 19 Конституції України його посадові особи зобов'язані діяти лише на підставі, у межах повноважень і в спосіб, що передбачені Конституцією та законами України. З огляду на це положення, наприклад, органи державної влади або місцева влада, може здійснювати обробку персональних даних (будь-яка дія або сукупність дій) лише за наявності повноважень, законної підстави й обґрунтованої мети та в спосіб, передбачений законом. Тобто не потрібно отримувати згоду суб'єкта персональних даних у тих випадках, коли дозвіл на збір інформації прямо передбачений законом. Водночас недостатньо мати повноваження, має бути обґрунтована мета та чітка процедура.

У європейському законодавстві правові підстави для обробки персональних даних викладені в статті 6 GDPR:

1. суб'єкт даних надав згоду на обробку своїх персональних даних для однієї чи декількох спеціальних цілей;

84 Національна комісія з інформаційних технологій та громадянських свобод Франції (CNIL). Режим доступу: https://www.cnil.fr/fr/intelligence-artificielle/ia-comment-etre-en-conformite-avec-le-rgpd

2. для виконання контракту, стороною якого є суб'єкт даних, або для вжиття дій на запит суб'єкта даних до укладення договору;
3. для дотримання встановленого законом зобов'язання, яке поширюється на контролера[85];
4. для того, щоб захистити життєво важливі інтереси суб'єкта даних або іншої фізичної особи;
5. для виконання завдання в суспільних інтересах або здійснення офіційних повноважень, покладених на контролера;
6. для цілей законних інтересів контролера або третьої сторони, окрім випадків, коли над такими інтересами переважають інтереси фундаментальних прав і свобод суб'єкта даних, що вимагають охорони персональних даних, особливо, якщо суб'єктом даних є дитина[86].

Як вирішити, коли застосовується законна підстава? Це залежить від конкретних цілей і контексту обробки. Водночас досить часто застосовуються декілька підстав, усе залежить від конкретного випадку обробки даних. Жодна з перелічених основ не може вважатися кращою або важливішою, ніж інші. Перед тим, як впроваджувати технології на основі персональних даних, варто подумати про так званий триетапний тест, де потрібно:

- визначити правову підставу;
- переконатися, що обробка необхідна для досягнення конкретної мети;
- збалансувати з інтересами, правами та свободами особи[87].

85 Контролер означає фізичну чи юридичну особу, орган публічної влади, агентство чи інший орган, який самостійно чи спільно з іншими визначає цілі та засоби опрацювання персональних даних; якщо цілі та засоби такого опрацювання визначаються законодавством Союзу чи держави-члена, контролер або спеціальні критерії його призначення можуть бути передбачені законодавством Союзу чи держави-члена (стаття 4 GDPR).

86 Офіційний переклад Регламенту європейського Парламенту і Ради (ЄС) 2016/679 від 27 квітня 2016 року про захист фізичних осіб у зв'язку з опрацюванням персональних даних і про вільний рух таких даних, та про скасування Директиви 95/46/ЄС (Загальний регламент про захист даних (GDPR). Режим доступу: https://zakon.rada.gov.ua/laws/show/984_008-16#Text

87 Information Commissioner's Office «Guidance on AI and data protection». Режим доступу: https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/artificial-intelligence/guidance-on-ai-and-data-protection/

5.4. ВИЗНАЧЕННЯ ЦІЛЕЙ ДЛЯ ОБРОБКИ ПЕРСОНАЛЬНИХ ДАНИХ

Система ШІ, заснована на використанні персональних даних, завжди має розроблятися, навчатися та розгортатися із чітко визначеною метою (цілями). Її потрібно встановити ще до розроблення проєкту (продукту чи послуги). Чітке усвідомлення того, навіщо здійснюється обробка конкретної інформації, необхідна для реалізації принципу *«обмеження мети»* та забезпечення справедливості, законності й прозорості обробки персональних даних, зокрема визначення необхідного рівня їх захисту.

Згідно з принципом *«обмеження мети»* потрібно заздалегідь визначити, обґрунтувати та документально закріпити реальні підстави й мету збору даних, адже надалі це стане запобіжником проти їх використання в незаконних цілях. Наприклад, перш ніж встановити системи відеоспостереження з технологіями ШІ, необхідно визначити мету й переконатися, що вона є законною. А також те, що досягнення цієї мети неможливе іншим способом, який передбачає меншу ступінь втручання у приватність. Неоднозначні або загальні описи на кшталт «для кращого виконання покладених завдань» недостатні. Окрім того, слід переконатися, що персональні дані згодом не будуть використані для непередбачених цілей або неправомірно передані третім особам, що не мають санкціонованого доступу.

Персональні дані можуть оброблятися для досягнення визначених реальних цілей, при цьому такі цілі мають бути максимально конкретизованими, досяжними та викладеними у внутрішніх документах (політиках), що регулюють роботу в цій сфері. Використання даних для реалізації додаткових чи нових завдань можливе, якщо:

1. Нова мета обробки персональних даних сумісна з метою первинною.

У такому випадку нова правова підстава для роботи з даними не потрібна, проте оцінювання того, чи справді оновлена мета сумісна з початковою, має бути об'єктивним. Для цього необхідно взяти до уваги такі фактори:

- наскільки первинна мета пов'язана з новою;
- контекст, у якому початково оброблялися персональні дані;
- специфіку та характер даних (наприклад, чи відносяться вони до особливої категорії тощо);
- вірогідність настання негативних наслідків для осіб, чиї дані обробляються;
- можливість гарантування належного рівня захисту обробки нової інформації.

Наприклад, впровадження системи ШІ на основі машинного навчання здійснюється поетапно. Спочатку відбувається навчання, що передбачає проєктування, розроблення системи ШІ. Далі — оперативне розгортання системи ШІ, отриманої на першому етапі. З погляду захисту персональних даних ці два кроки не відповідають одній й тій самій цілі й тому мають бути розділені. У двох випадках цілі обробки персональних даних мають бути окремо визначені, бути чіткими та мати законні підстави[88]. Скажімо, системи розпізнавання обличчя можна використовувати для багатьох цілей, таких як запобігання злочинності, або ж аутентифікація та позначення осіб у соціальних мережах. Кожне із цих застосувань може вимагати іншої законної підстави.

2. З'явилася правова норма, яка вимагає чи дозволяє обробку даних з новою метою.

Наприклад, через відповідні зміни в законодавстві повноваження органу збільшені, і він отримав право виконувати додаткові функції, пов'язані з обробкою персональних даних.

88 Таку ж позицію офіційно опублікувала Національна комісія з інформаційних технологій та громадянських свобод Франції (CNIL). Режим доступу: https://www.cnil.fr/fr/intelligence-artificielle/ia-comment-etre-en-conformite-avec-le-rgpd

5.5. ВИЗНАЧЕННЯ РОЛІ ПІД ЧАС ОБРОБКИ ПЕРСОНАЛЬНИХ ДАНИХ

Розуміння ролі зацікавлених сторін ШІ у процесі обробки персональних даних необхідне для визначення обсягу їх прав та обов'язків. Наприклад, з огляду на міжнародну практику, велика увага зосереджена на рішеннях, які має ухвалити саме володілець даних[89]. Зокрема про:

- джерело та характер даних, що використовуються для навчання моделі ШІ;
- цільовий результат моделі (що передбачається або класифікується);
- загальні види алгоритмів машинного навчання, які будуть використовуватися для створення моделей з даних (наприклад, нейронні мережі);
- вибір ознак, які можуть використовуватися в кожній моделі;
- ключові параметри моделі (наприклад, наскільки складним може бути дерево рішень або скільки моделей буде включено в життєвий цикл);
- те, яким чином моделі будуть тестуватися та оновлюватися: як часто, з використанням яких видів даних, як буде оцінюватися постійна продуктивність тощо[90].

Коли системи ШІ залучають кілька організацій до обробки даних, визначити ролі може бути складно. Можуть виникнути питання про типи сценаріїв, коли організація чи установа стане володільцем даних. Наприклад, організація надає хмарний сервіс для зберігання даних, а також набір загальних інструментів для машинного навчання. Особи, які використовують цей сервіс, за логікою закону будуть вважатися володільцями (контролером) даних, оскільки вони вирішують, які дані й моделі використовувати, параметри моделей і процеси їх оцінювання,

89 Володілець персональних даних (або згідно з GDPR — контролер даних) — фізична або юридична особа, яка збирає дані, визначає мету, встановлює спосіб та порядок їх обробки та має у власності відповідне технічне обладнання. Це можуть бути підприємства, установи й організації всіх форм власності, органи державної влади чи органи місцевого самоврядування, а також фізичні особи-підприємці.

90 Information Commissioner's Office «Guidance on AI and data protection». Режим доступу: https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/artificial-intelligence/guidance-on-ai-and-data-protection/

тестування, оновлення тощо. Проте організація, що надає сервіс, імовірно, є розпорядником (процесором), оскільки вона лише визначає технічні аспекти, конфігурацію зберігання та архітектуру хмари тощо. Інший приклад, коли постачальник (розпорядник даних) запропонував інструмент для скринінгу резюме для оцінювання та відбору кандидатів на роботу й для цього почав вимагати від володільця даних багато інформації про кожного кандидата. Якщо володілець закуповує таку систему, тоді потрібно розглянути, чи можна виправдати збір такого обсягу персональних даних від кандидатів, і якщо ні, запросити постачальника змінити свою систему або знайти іншого. Ці приклади вказують на складність визначення ролей, особливо коли залучено декілька суб'єктів ШІ. Це підкреслює потребу чіткого розуміння відповідальності кожної сторони в межах законодавства про захист персональних даних, а також додаткового дослідження цього питання на конкретних практичних прикладах.

5.6. ЗАБЕЗПЕЧЕННЯ ПРАВ СУБ'ЄКТІВ ПЕРСОНАЛЬНИХ ДАНИХ

Проєктування системи захисту персональних даних в технологіях ШІ вимагає чіткого розуміння та дотримання інформаційних прав людини. Згідно закону кожна фізична особа має особисті немайнові права на свої персональні дані. Зокрема[91]:

1. знати про джерела збирання, місцезнаходження своїх персональних даних, мету їх обробки, місцезнаходження або місце проживання (перебування) володільця чи розпорядника персональних даних або дати відповідне доручення про отримання цієї інформації уповноваженим ним особам, окрім випадків, встановлених законом;
2. отримувати інформацію про умови надання доступу до персональних даних, зокрема інформацію про третіх осіб, яким передаються її персональні дані;

91 Стаття 8 Закону України «Про захист персональних даних».

3. на доступ до своїх персональних даних;
4. отримувати не пізніше як за тридцять календарних днів з дня надходження запиту, окрім випадків, передбачених законом, відповідь про те, чи обробляються її персональні дані, а також отримувати зміст таких персональних даних;
5. пред'являти вмотивовану вимогу володільцю персональних даних із запереченням проти обробки своїх персональних даних;
6. пред'являти вмотивовану вимогу щодо зміни або знищення своїх персональних даних будь-яким володільцем і розпорядником персональних даних, якщо ці дані обробляються незаконно чи є недостовірними;
7. на захист своїх персональних даних від незаконної обробки та випадкової втрати, знищення, пошкодження у зв'язку з умисним приховуванням, ненаданням чи несвоєчасним їх наданням, а також на захист від надання відомостей, що є недостовірними чи ганьблять честь, гідність та ділову репутацію фізичної особи;
8. звертатися зі скаргами на обробку своїх персональних даних до Уповноваженого або до суду;
9. застосовувати засоби правового захисту в разі порушення законодавства про захист персональних даних;
10. вносити застереження стосовно обмеження права на обробку своїх персональних даних під час надання згоди;
11. відкликати згоду на обробку персональних даних;
12. знати механізм автоматичної обробки персональних даних;
13. на захист від автоматизованого рішення, яке має для нього правові наслідки.

Розглянемо детальніше декілька із них.

ПРАВО НА ІНФОРМАЦІЮ ТА ДОСТУП ДО ДАНИХ

Це право передбачає можливість особи звернутися із запитом, щоб уточнити,

- чи обробляє володілець або розпорядник (контролер чи процесор) її персональні дані;
- які саме дані обробляє (категорія та види);
- на яких правових підставах та з якою метою здійснюється обробка[92].

Також питання можуть стосуватися інших технічних та організаційних процесів обробки даних: внутрішні політики, система безпеки, термін зберігання та видання, передача третім особам тощо). Якщо дані такої людини не обробляються, необхідно повідомити про це (залишати запит без відповіді не можна). Якщо обробляються дані суб'єкта, тоді потрібно це підтвердити.

Якщо особа виявила бажання отримати доступ до своїх даних, то такий запит треба задовольнити, окрім випадків визначених законом. Закон України «Про захист персональних даних» не тільки гарантує право на доступ до своїх персональних даних, а й визначає такі засади отримання доступу, як *безоплатність (стаття 19 Закону)* та *невідкладність (стаття 17 Закону)*. Отже, кожна особа за своїм бажанням повинна отримати можливість безперешкодно переглянути інформацію про себе, при цьому плата за це не береться. У такому випадку може виникнути питання про обсяг даних. Це завжди варто уточнювати. Важливо звернути увагу, що такий запит може сприйматися як опис даних, тобто того, яка інформація збирається. Згідно із законом потрібно надати саме персональні дані як такі. Якщо це були заповнені анкети, наприклад для отримання дисконтної карти магазину, тоді саме їх. Якщо виконати запит надто складно, треба про це повідомити особу, вказавши причини неможливості виконання запиту та про будь-які альтернативні можливості. Тому важливо дотримуватися концепції проєктування дизайну приватності ще на стадії розроблення моделі. Тоді спеціалісти з питань конфіденційності інформації можуть передбачити такий законодавчий аспект, як дотримання права людини на інформацію та доступ до своїх даних, окрім випадків, визначених законом. Зокрема, розробити політики та інші внутрішні інструкції, які забезпечать доступ особи до інформації про:

- цілі обробки;
- види та категорії персональних даних;

92 Право доступу суб'єкта персональних даних закріплено в статті 15 GDPR.

- про одержувачів чи категорії одержувачів, яким були або будуть розкриті дані;
- термін зберігання даних або критерії для визначення зазначеного періоду;
- права особи, зокрема на виправлення чи видалення своїх даних, обмеження або заперечення проти їх обробки;
- право подання скарги до наглядового органу;
- джерело персональних даних, якщо вони були отримані не від суб'єкта даних;
- наявність процесу автоматизованого ухвалення рішення[93], у тому числі на якому етапі обробки даних воно застосовується;
- умови та засоби захисту передачі даних, якщо персональні дані передаються до третьої країни або міжнародної організації[94].

ПРАВО НА ВИДАЛЕННЯ

Право на видалення, відоме також як «право бути забутим». Згідно зі статтею 8 Закону України «Про захист персональних даних» особа має право пред'являти вмотивовану вимогу із запереченням проти обробки своїх персональних даних, а також щодо їх знищення, якщо ці дані обробляються незаконно чи є недостовірними. Згідно зі статтею 17 GDPR особа має право вимагати видалення своїх персональних даних, якщо, зокрема, дані більше не потрібні для цілей, для яких вони були зібрані, суб'єкт відкликає свою згоду на обробку даних або дані обробляються незаконно, окрім випадків, визначених законом.

У системах ШІ, які використовують персональні дані для навчання та функціонування, забезпечення права на видалення вимагає впровадження технічних та організаційних заходів. Вони повинні гарантувати можливість видалення даних на запит особи та виконання цього запиту в розумний строк. При цьому важливо забезпечити, щоб видалення не порушувало цілі та функції ШІ, які можуть включати, наприклад, виявлення патернів, навчання моделей чи інші завдання. Такі процедури повинні враховувати особливості роботи системи ШІ та можливість видалення або анонімізації даних з різних джерел і баз даних.[95]

ПРАВО НА ЗАХИСТ ВІД АВТОМАТИЗОВАНОГО УХВАЛЕННЯ РІШЕННЯ

Будь-яка сучасна технологія може зазнавати збою, помилки, кібератаки тощо, що в результаті може мати непередбачені наслідки як для окремих осіб, так і суспільства загалом. Відповідно до національного[96] та міжнародного законодавства особа має право не підлягати рішенню, що ґрунтується виняткова на автоматизованій обробці, у тому числі профайлінгу, що породжує правові наслідки, окрім випадків, визначених законом[97].

Законодавство не перешкоджає використовувати ШІ для автоматизованого ухвалення рішень, якщо ці рішення мають правові підстави та реалізуються в законний спосіб. Тобто мають бути встановлені певні гарантії такої обробки інформації[98]. Зокрема, воно зобов'язує враховувати «специфічні обставини та контекст» і впроваджувати технічні та організаційні заходи, щоб забезпечити її «справедливість та прозорість». Ці заходи повинні:

- забезпечити обробку персональних даних таким чином, щоб враховувати ризики для прав та інтересів осіб *(див. п. 5.2. Оцінювання ризиків)*;
- запобігти дискримінаційним впливам на основі спеціальної категорії даних.

Також слід передбачити можливість відмовитися від автоматизованих систем, де це доречно. Згідно зі статтею 8 Закону України «Про захист персональних даних» і статтею 13 (2)(f) та 14 (2)(g) GDPR необхідно повідомити особам, чиї дані обробляються, про використання автоматизованих систем, зокрема надати «змістовну інформацію

93 Згідно зі статтями 22(1) і (4) GDPR.
94 Згідно зі статтею 46 GDPR.
95 Guidelines on Personal Data Processing Using Artificial Intelligence Technologies, FIIAPP.
96 Стаття 8 Закону України «Про захист персональних даних».
97 Стаття 22 GDPR.
98 Преамбула 71 GDPR надає більше ясності стосовно статті 22.

про логіку ухвалення автоматизованих рішень, а також про можливі наслідки» такої обробки для них. Потрібно забезпечити своєчасний людський контроль і втручання, якщо автоматизована система дає збій, помилку або на вимогу суб'єкта даних тощо.

Існує багато причин, чому люди не хочуть користуватися автоматизованою системою: вона може призвести до непередбачуваних результатів; вона може посилювати упередження чи бути недоступною; може просто бути незручною; а може замінити паперовий або ручний процес, до якого вже звикли. Однак люди часто стикаються з відсутністю альтернативи. Це неправильний підхід з погляду забезпечення юридичних гарантій захисту. Людина повинна мати право вибору або ж заперечити проти використання автоматизованої обробки, окрім випадків, коли така система встановлена відповідно до вимог закону, в інтересах національної безпеки, економічного добробуту. Але в кожному разі потрібно зробити так, щоб не допустити негативних наслідків для людини.

На практиці може виникнути питання: яка обробка розглядається як автоматизована[99]? Системи ШІ виконують різні ролі, тобто це означає, що можуть брати участь у різних етапах процесу ухвалення рішень. Коли ШІ ухвалює рішення, яке має юридичні наслідки для осіб, варто поставити такі питання:

- Який це вид рішення (чи воно лише автоматизоване)?
- Коли ухвалюється це рішення?
- У якому контексті система ухвалює рішення?
- Які кроки призводять до цього рішення?

Як зазначено вище, законодавство вимагає забезпечити заходи безпеки під час обробки персональних даних для здійснення автоматизованих рішень, які мають юридичний або подібний за значущістю вплив на осіб. Ці заходи охоплюють право осіб:

- запросити втручання людини;
- висловити свою точку зору;

99 Зокрема, підпадає під статтю 22 GDPR.

- оскаржити рішення, ухвалене стосовно них;
- отримати пояснення логіки рішення[100].

Втручання людини повинно передбачати аналіз рішення незалежно від того, обробка повністю автоматизована або частково[101]. Тому також слід:

- розглянути вимоги системи, необхідні для забезпечення змістовного перегляду людини ще з фази проєктування;
- розробити й забезпечити відповідну професійну підготовку для людей, які переглядають рішення.

Варто інформувати про специфіку автоматизованого рішення, зокрема стосовно джерел даних, що використовуються для його ухвалення. Наприклад, якщо надаються результати рішення через вебсайт, на сторінці має бути посилання або чітка інформація, що дозволить особі зв'язатися зі співробітником, який може здійснити втручання, без зайвих затримок або ускладнень. Усі записи про ухвалені системою ШІ рішення, а також інформацію про те, чи фізична особа зверталася з проханням про втручання людини, висловлювала свої погляди, оскаржувала рішення, чи змінювалося рішення в результаті цього, рекомендується зберігати протягом певного періоду часу[102]. Також потрібно врахувати й додаткові аспекти в контексті складних систем ШІ:

- Автоматичне упередження (automation bias). Термін «автоматичне упередження», або «упередження, спричинене автоматизацією», позначає стан, коли користувачі системи підтримки ухвалення рішень довіряють результатам, згенерованим системою, і перестають застосовувати свої власні судження або не запитують про можливі помилки в її висновках. Уявімо ситуацію, наприклад, коли особі було відмовлено в отриманні засобів для зменшення болю через те, що медичне програмне забезпечення змішало її анамнез з даними іншого пацієнта. Або установа впровадила автоматизовану систему оцінювання роботи, у результаті чого деяких працівників звільнили на основі рішень, ухвалених програмою, не надаючи їм можливості для оскарження[103]. Тому важливе вручання людини для перевірки усіх даних.
- Відсутність можливості інтерпретації. Деякі види ШІ можуть забезпечити результати, які складно інтерпретувати для людини, наприклад ті, що базуються на складних моделях глибокого навчання. Якщо результати ШІ не можуть бути легко інтерпретовані й інші засоби пояснення виявляються недостатньо доступними або ненадійними, існує ризик того, що людина не зможе належним чином оцінити результати та врахувати їх при ухваленні власних рішень.

Отже, потрібно розуміти ризикові аспекти, пов'язані з кожною опцією та забезпечити чіткі сфери відповідальності й ефективні політики з управління ризиками.[104]

100 The Alan Turing guidance on 'Explaining decisions made with Artificial Intelligence.

101 Додаткова інформація: Європейська рада із захисту даних Європейська рада із захисту даних (EDPB), яка замінила Робочу групу зі статті 29 (WP29), включає представників органів із захисту даних кожної країни-члена ЄС. WP29 опублікував рекомендації щодо автоматизованого індивідуального ухвалення рішень та профілювання, які можуть надати корисні вказівки з певних питань. Режим доступу: https://ec.europa.eu/newsroom/article29/items/612053

102 Інструкція з документації «Європейські рекомендації щодо автоматизованого ухвалення рішень та профілювання». Режим доступу: https://ec.europa.eu/newsroom/article29/items/612053

103 Умовні приклади, які поширені у світі.

104 Information Commissioner's Office «Guidance on AI and data protection». Режим доступу: https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/artificial-intelligence/guidance-on-ai-and-data-protection/

Омбудсман України
Ombudsman of Ukraine

Фінансується
Європейським Союзом

FIIAPP
COOPERACIÓN ESPAÑOLA

Міністерство
цифрової трансформації
України