AMERICANBARASSOCIATION

Лабораторія Цифрової Безпеки

Без обмежень:

як Україна регулює збір навчальних даних для тренування штучного інтелекту?

Анна Людва
Тетяна Авдєєва

2023

Зміст

У сучасному цифровізованому світі, який заполонили нові технології, штучний інтелект (ШІ) продовжує революціонізувати різні галузі та сфери життя. Будучи невід'ємною частиною індустрії, економіки та робочої сили, ШІ лише збільшуватиме свій вплив протягом років: статистика демонструє, що з 2023 по 2030 рік темпи зростання ШІ становитимуть 37,3%. У свою чергу, розробка нових систем ШІ потребує тренування моделей машинного навчання, яке здійснюється за допомогою навчальних даних. Як основа машинного навчання та ШІ, навчальні дані є необхідними для того, аби навчити алгоритми розпізнавати закономірності та тенденції, робити прогнози, а також передбачати новий набір даних. Потреба у навчальних даних є постійною – кількість опрацьованих та використаних даних напряму залежить від точності результатів, виданих системою ШІ. Розробники систем ШІ обирають різні шляхи збору відповідних даних, які будуть використовуватися для навчання алгоритму машинних моделей. У цьому випадку дані можуть отримуватися за допомогою скрапінгу веб-сайтів (“website scraping”), використання систем відкритих даних або синтетичних даних, а також ручного введення даних в базу даних.

Слідуючи світовим трендам, Україна не є винятком та використовує ШІ в різних галузях. Втім, незважаючи на відкритість України до впровадження машинних технологій, відсутність належного законодавчого регулювання щодо збору навчальних даних фактично “зв'язує руки” розробникам індустрії. Станом на сьогодні українське законодавство не встигає за стрімким розвитком ШІ, а тому не передбачає чітких механізмів збору та обробки навчальних даних для тренування моделей машинного навчання. З огляду на це, Лабораторія цифрової безпеки вирішила проаналізувати не лише українське законодавство у сфері ШІ та захисту даних для виокремлення основних проблем, з якими стикається індустрія під час своїх розробок, а й іноземні практики щодо легітимної обробки та збору навчальних даних. Результатом правового аналізу стануть рекомендації, які будуть містити прийнятну модель механізму дій для українських законотворців, яка не лише захищатиме персональні дані користувачів, але й не “перекриватиме повітря” індустрії ШІ.

І. Погоня за розвитком ШІ, або українські спроби врегулювати нові технології

Незважаючи на те, що Україна бере активну участь у розробці нових технологій ШІ, регулювання в цьому полі є досить застарілим та недосконалим. З огляду на відсутність уніфікованого законодавства, яке адресує питання збору даних для тренування систем ШІ, необхідно звертатися до галузевих законів, що регулюють окремі пов'язані сфери. Одним із таких законів є Закон України "Про захист персональних даних". Прийнятий у 2010 році, Закон окреслює здебільшого загальні положення та гарантії щодо збору та обробки персональних даних, фактично не фокусуючись на положеннях автоматизованого збору даних або алгоритмах машинного навчання. Втім Закон встановлює обмеження щодо збору та обробки окремих категорій даних. Практика демонструє, що для тренування моделей машинного навчання збору підлягають фактично всі види даних, серед яких і біометричні дані. Останні є формою чутливих даних, обробка яких є здебільшого забороненою за винятком окремих випадків, які визнають дії з біометричними даними легітимними. Закон передбачає перелік таких винятків, проте не включає у список можливість збору даних для цілей створення ШІ.

> Натомість Закон дозволяє обробку біометричних даних, якщо вона, зокрема:
>
> - здійснюється за умови надання суб'єктом персональних даних однозначної згоди на обробку таких даних;
> - необхідна для здійснення прав та виконання обов'язків володільця у сфері трудових правовідносин із забезпеченням відповідного захисту;
> - необхідна для захисту життєво важливих інтересів суб'єкта персональних даних або іншої особи у разі недієздатності або обмеження цивільної дієздатності суб'єкта персональних даних;
> - необхідна в цілях охорони здоров'я;
> - стосується даних, які були явно оприлюднені суб'єктом персональних даних (що часто використовується розробниками систем ШІ).

Як вже було зазначено, однією з технік збору даних для тренування є скрапінг відкритих даних, тобто даних, що знаходяться у вільному доступі в Інтернеті. Оскільки оприлюднені дані відносяться до відкритих даних, можна припустити, що Закон фактично дозволяє збір таких даних для тренування машинних моделей. Як буде продемонстровано у подальших розділах, така політика не є найбільш безпечною для індустрії та може призвести до судових проваджень, відкритих проти розробників моделей ШІ (наприклад, позови проти OpenAI).

Говорячи про законодавчі ініціативи, варто згадати Проект Закону про захист персональних даних, що знаходиться на розгляді Верховної Ради з жовтня 2022 року. На відміну від Закону, законопроект має на меті наблизити законодавство щодо захисту даних до європейських стандартів, адресуючи вже нагальні питання цифрової сфери та розвитку нових технологій. Проте і в такому випадку проект залишається недосконалим в питаннях ШІ та доступу до даних. Хоча положення проекту акцентують увагу на автоматизованій обробці персональних даних, вони обмежуються виключно цим. Крім того, проект збільшує перелік винятків, які дозволяють обробку біометричних даних, додаючи обробку, необхідну *“в цілях архівування в суспільних інтересах, цілей наукового чи історичного дослідження або статистичних цілей”*. У цьому випадку проект фактично дозволяє збір навчальних даних, здійснений без мети прибутку.

Оскільки збору навчальних даних можуть підлягати і авторські роботи, у контексті безпеки даних особи варто також згадати Закон України “Про авторське право і суміжні права”. Згідно з Законом, об'єкти авторського права включають бази даних (компіляції даних), якщо вони за добором або упорядкуванням їх складових частин є результатом інтелектуальної діяльності. При цьому логічні схеми, алгоритми і мови програмування, не охороняються авторським правом. З огляду на це, Закон не передбачає механізму авторизації доступу до авторських матеріалів для їх використання з метою тренування систем ШІ.

II. Що не так з чинним регулюванням?

Очевидно, що неврегульованість сфери ШІ призводить до негативних наслідків, які мають вплив не лише на саму індустрію, але і на суб'єктів даних, чия інформація підлягає використанню. Серед найбільш проблематичних аспектів варто виокремити відсутність регуляторної бази, загроза конфіденційності та безпеці даних, а також порушення авторського права.

Відсутність регуляторної бази. Найбільш нагальну проблему, що постає перед розробниками ШІ, наразі становить вимушене порушення закону задля створення та тренування систем ШІ з огляду на відсутність законодавчої підстави для збору персональних даних. Оскільки чинне законодавство не передбачає жодних легітимних шляхів для збору даних та їх обробки, а також не містить вказівок чи політики щодо використання таких даних, у розробників залишається два варіанти дій: зупинити свою діяльність або ж переступати закон задля розвитку системи. Практика демонструє, що розробники зазвичай схиляються до другого варіанту, виправдовуючи таке рішення метою запуску нових технологій та цифровізації держави.

Недосконаліть чинного законодавства було підтверджено і у Концепції розвитку штучного інтелекту в Україні, розробленої КМУ. Серед пріоритетних напрямів реалізації було виокремлено приведення законодавства у галузі використання технологій ШІ у відповідність із міжнародними нормативно-правовими актами. Враховуючи, що імплементація положень запланована до 2030 року, на жаль, зміни законодавства доведеться чекати нескоро.

Загроза конфіденційності та безпеці даних. Практика демонструє, що збір навчальних даних здебільшого відбувається без попередньої згоди чи повідомлення користувачів, оскільки їх дані перебувають у відкритому доступі. А це, у свою чергу, піднімає питання конфіденційності та безпеки даних, які підлягають подальшому використанню. Яскравим прикладом є Google, який було звинувачено у зборі даних із Google Docs для навчання ШІ. Спочатку компанія заявляла, що без дозволу користувача не збирає даних користувачів, що перебувають у відкритому доступі, використовуючи анонімізовані дані, проте пізніше визнала, що використовує скрапінг для тренування систем Bard та Cloud AI.

Більше того, публікація особою даних звісно ж уможливлює їх використання в різних цілях – проте які цілі легальні і етичні? Наприклад, компанія використовує дані з відкритих джерел для тренування систем, що створюють синтетичні медіа (діпфейки) для поширення порнографії (яка легалізована в багатьох державах). Чи справді особа, публікуючи фото у профайлі на Facebook усвідомлює, що її персональні дані можуть використовуватися і для створення таких систем? Жодних законодавчих обмежень з цього приводу немає. Тож питання залишається відкритим.

Порушення авторського права. Інша проблема, на яку варто звернути увагу, є поширеною не лише в українських реаліях, але й на міжнародному полі. Як вже було згадано, для тренування систем ШІ необхідні чималі обсяги даних, більшість з яких збирається з відкритого онлайн-простору. Для створення “людського” контенту (тобто оригінального контенту, згенерованого живою особою замість машини) розробники збирають інформацію з соцмереж, пошукових систем, цифрових бібліотек, статистичних банків тощо. Оскільки дані є оприлюдненими, розробники презюмують, що їх збирання є легітимним. Проте часто трапляється, що навчальні дані становлять предмет авторського права окремих осіб, особливо коли йдеться про розробку моделей, спрямованих на створення людського продукту (наприклад, системи, спрямовані на створення мистецтва або перекладачі). Варто підкреслити, що практика збору предметів авторського права для цілей тренування ШІ є досить суперечливою та регулюється на рівні кожної держави по-різному. Втім, наразі можна спостерігати чималу кількість позовів, які було подано проти розробників систем ШІ авторами контенту, зібраного без попереднього дозволу:

- Передусім варто згадати скандал між New York Times та OpenAI, що є розробником ChatGPT. Автори газети звинуватили розробників у використанні газетних звітів медіа для тренування ШІ без дозволу авторів. Основне занепокоєння NY Times полягало у тому, що OpenAI фактично стане прямим конкурентом газети, адже може генерувати аналогічні статті. З огляду на це Times планували подачу судового позову проти розробників системи, задоволення якого могло б призвести до фатальних наслідків для індустрії ШІ: суд міг би наказати OpenAI видалити весь нелегально зібраний матеріал. Проте до суду справа не дійшла – пізніше New York Times оновили власну політику використання даних, заборонивши використання контенту газети для тренування моделей ШІ.
- Примітно, що у контексті вищезгаданої ситуації існує прецедент зі схожими фактами справи. Так, справа *Authors Guild v. Google, Inc.* пов'язана зі скаргою автора щодо неправомірного використання цифрових копій його книг для системи Google Books. Федеральний апеляційний суд США встановив, що сканування книг не порушує авторського права заявника з огляду на доктрину "добросовісного користування" (яка буде розкрита у наступному розділі), а сама система не становить конкуренції на ринку книг та автору.
- Крім того, варто згадати позов, поданий Getty Images проти компанії Stability AI, що є розробником генератора зображень. Getty Images вимагають 1,8 трильйонів доларів компенсації за ймовірно 12 мільйонів зображень, які було використано без погодження.

III. "Зроби сам": як іноземні країни розробляють стандарти для регулювання ШІ?

Незважаючи на те, що багато країн вже імплементували положення щодо регулювання механізму використання ШІ, проблема щодо збору та обробки навчальних даних залишається поширеною і серед міжнародної спільноти. Це зумовлено як відсутністю уніфікованих стандартів, так і фрагментацією національних правил. У цьому випадку можна виокремити декілька країн та їх спроби законодавчо врегулювати проблему та віднайти баланс між потребою розвитку технологій ШІ (у контексті навчання та тренування моделей) та захистом прав людини (у контексті безпеки персональних даних та авторського права).

Рівень ЄС. У контексті доступу розробників ШІ до даних варто звернутися до Положення ЄС про узгоджені правила справедливого доступу до даних

та їх використання (Акт про дані). Акт встановлює правила щодо того, хто може використовувати або отримувати доступ до даних у всіх секторах економіки в ЄС. Встановлюючи вимоги щодо обміну даними, Акт поширюється на різних акторів, серед яких органи державної влади, надавачі цифрових послуг, а також розробників девайсів (що включають і розробників систем ШІ). Акт про дані надає як окремим особам, так і компаніям більше контролю над своїми даними через право на перенесення, копіювання або передачу даних з різних служб, де дані генеруються за допомогою розумних об'єктів, машин та пристроїв. Так, користувачі підключених пристроїв, (починаючи від розумних побутових приладів і закінчуючи інтелектуальним промисловим обладнанням), можуть отримувати доступ до даних, створених у результаті їх використання, які часто збираються виключно розробниками та постачальниками послуг. Крім того, Акт передбачає створення ринків даних ("data markets"). У цьому випадку виробникам або користувачам дозволяється монетизувати згенеровані дані шляхом обміну, продажу або ліцензування їх іншим компаніям, як-от стартапам. Акт також встановлює обмеження щодо доступу третіх осіб до спільних даних, які передбачають заходи щодо захисту конфіденційності, приватності та комерційної таємниці, а також обмеження на використання даних ринковими конкурентами власника даних.

За своїми положеннями Акт є компліментарним документом до Європейського Акту про управління даними, який сприяє обміну даними між секторами та країнами ЄС, а також розвитку інноваційних продуктів та послуг. Передусім Акт передбачає механізм щодо повторного використання (для комерційних та некомерційних цілей) певних даних державного сектору, які не можуть бути доступні як відкриті дані. Йдеться про дані, захищені комерційною таємницею, статистичною конфіденційністю, авторським правом, а також захистом персональних даних. У цьому випадку Акт встановлює вимоги щодо повторного використання даних, серед яких їх попередня анонімізація або модифікація, дотримання вимог авторського права, попередження щодо передачі даних третім особам тощо. Крім того, Акт передбачає положення щодо альтруїзму даних ("data altruism"), що фактично відображає доктрину добросовісного використання, дозволяючи добровільний механізм обміну даними на основі згоди осіб для цілей загального інтересу. Для досягнення цієї мети, а також полегшення збору даних, Акт запроваджує універсальну європейську форму згоди на альтруїзм даних, що передбачає як надання, так і подальше відкликання згоди. Така форма слугує своєрідним гарантом для дослідників та компаній, що мають на меті використання відповідних даних. У цьому контексті Акт також вимагає від держав-членів ЄС створення національних Публічних реєстрів щодо визнаних організацій альтруїзму даних, які повинні відповідати ряду вимог.

Практика Німеччини. Будучи державою-членом ЄС, німецьке законодавство фактично віддзеркалює європейські стандарти у сфері захисту персональних даних під час їх збору та обробки. Німеччина не містить уніфікованого законодавства щодо регулювання ШІ, обмежуючись спеціальними законами та внутрішніми актами.

Здебільшого практика доступу та збору даних для тренування ШІ може підпадати під регулювання Закону Німеччини про авторське право ("German Copyright Act" або "Urheberrechtsgesetz (UrhG)"). Закон також імплементував Директиву ЄС 2019/790 щодо авторського права та суміжних прав та її положення щодо аналізу тексту та даних (*"text and data mining"*). За Директивою, аналіз тексту та даних означає будь-який автоматизований аналітичний метод, спрямований на аналіз тексту та даних у цифровій формі з метою генерування інформації, який включає, але не обмежується зразками, трендами та кореляціями. Враховуючи вимоги Директиви, німецький Закон дозволяє відтворення матеріалів для їх автоматизованого аналізу з метою отримання інформації про зразки, тренди та кореляції лише у випадку, якщо доступ до таких матеріалів є легітимним. При цьому автор має право не надавати доступ до своїх матеріалів. Як виняток Закон дозволяє неавторизоване відтворення авторських робіт лише для некомерційних цілей. Наприклад, дослідницькі інститути мають необмежене право аналізувати авторський контент, оскільки вони вже мають до нього доступ. Задля уникнення порушень кримінальне законодавство Німеччини вимагає встановлення спеціального захисту проти неавторизованого доступу за допомогою технічних або організаційних засобів. Більше того, кримінальний закон ("StGB") встановлює відповідальність за неавторизований доступ до авторських робіт, спеціально захищених від несанкціонованого доступу.

Таким чином, німецьке законодавство прямо не забороняє збір навчальних даних для цілей ШІ за умови дотримання правил щодо захисту персональних даних. У цьому контексті Німеччина звертається до вимог Загального регламенту захисту даних, а саме: (1) наявність легальної бази для обробки персональних даних (здебільшого явна згода суб'єкта даних) та (2) наявність чіткого попередження щодо такої обробки. Німецька цільова група ШІ зауважила, що більшість позовів проти ChatGPT було подано саме через відсутність законодавчої бази, оскільки було невідомо, звідки надходять дані. Крім того, національний Закон Німеччини про захист даних ("BDSG") вказує, що дані для тренування ШІ повинні бути "значними", тобто якщо такі дані отримані за допомогою *"науково визнаної математично-статистичної процедури"*.

Практика США. Американське регулювання значно відрізняється від європейського у тому аспекті, що розробники ШІ мають набагато ширше поле

можливостей для тренування машинних моделей з огляду на пом'якшені вимоги у сфері захисту авторського права. Наприклад, згідно з Законом США про авторське право, відтворення будь-яких матеріалів зазвичай відбувається за явної згоди автора, проте легітимність такого відтворення залежить від винятків, передбачених законом. Одним із таких винятків є так зване "добросовісне використання" ("fair use"), на яке найчастіше посилаються розробники технологій ШІ. Добросовісне використання – це доктрина, яка дозволяє обмежене використання (включаючи тренування ШІ) авторського матеріалу без попереднього дозволу автора. Для визначення добросовісності використання матеріалу в будь-якому конкретному випадку, Закон виокремлює врахування чотирьох факторів:

1) мета та характер використання, включно з тим, чи здійснено таке використання комерційною або з неприбутковою освітньою метою;
2) характер твору, захищеного авторським правом;
3) кількість та істотність використаної частини по відношенню до захищеного авторським правом матеріалу в цілому; та
4) вплив використання на потенційний ринок або вартість захищеного авторським правом матеріалу.

Основний аргумент компаній ШІ полягає у тому, що їх моделі не використовують авторський матеріал, а трансформують оригінальну роботу, що і кваліфікує діяльність машинних моделей як "добросовісне використання". Водночас, у національній справі *Andy Warhol Foundation for the Visual Arts v. Goldsmith*, що стосується несанкціонованого використання фотографій заявника, суд вказав, що таке використання було недобросовісним, оскільки переслідувало комерційну мету. У цьому випадку американська практика нагадує європейську, здебільшого дозволяючи тренування моделей ШІ для неприбуткових цілей. Втім, наскільки багато компаній насправді є некомерційними?

IV. Пошук законодавчих лазівок або легітимні способи збору навчальних даних

З огляду на недосконале регулювання як розробники, так і користувачі ШІ намагаються знайти шляхи збору навчальних даних, які були легітимними і при цьому не порушували чинне законодавство. У цьому контексті варто виокремити декілька способів отримання таких даних, поширених у міжнародному полі.

Анонімізація даних. Найпоширенішим способом використання даних для тренування ШІ без законодавчих наслідків для індустрії є анонімізування таких

даних. Анонімізація – це процес маніпулювання даними, за якого отримана інформація позбавляється будь-яких елементів, які могли б ідентифікувати суб'єктів даних. Після застосування методів анонімізації зазвичай стає неможливо ідентифікувати конкретну особу або виокремити чутливі дані, пов'язані з суб'єком даних. Методи анонімізації різняться залежно від того, скільки інформації планується приховати: у цьому випадку також може бути застосована рандомізація (зміна достовірності даних - як-от заміна одного імені іншим) чи генералізація (приховування ідентифікаторів) даних. Анонімізація значно спрощує зобов'язання розробників ШІ: застосування таких методів автоматично виключає застосовність регулювання з боку ЄС. Крім того, анонімні дані є корисними і для самої індустрії, оскільки видалення особистої інформації з даних, які всебічно репрезентують населення, перед їх використанням для навчання ШІ гарантує, що несвідомі упередження не потраплять в алгоритм, а персональні дані будуть захищені.

У контексті неможливості ідентифікації особи варто також звернути увагу на використання синтетичних даних. Синтетичні дані – це інформація, створена штучно комп'ютерними програмами, а не на основі реальних подій. Деякі провайдери надають в користування такі бази даних, що створюються на основі наявних даних, переважно через їх незначні варіації. Використання синтетичних даних для навчання ШІ значно мінімізує загрози щодо конфіденційності та безпеки персональних даних, оскільки вони не генеруються на основі реальних подій. Втім, розробники машинних моделей частіше звертаються до "людських" даних, які включають біометричні та чутливі дані, задля отримання найефективніших результатів з боку ШІ.

Передача відкритих даних. Поширеним є також надання у користування даних, що були зібрані дослідниками та науковцями. Так, академічні інституції та приватні дослідники створюють попередньо заповнені бази даних для типових проблем алгоритму машинного навчання, що можуть бути використані і для навчання моделей. Наприклад, Університет Каліфорнії в Ірвайні наразі підтримує 413 баз даних, відкритих для використання в алгоритмах машинного навчання.

Ліцензія на доступ до даних. Практика щодо укладення ліцензійної угоди на навчальні дані ШІ (або ліцензування ШІ) є досить поширеною в американській індустрії. За умовами угоди особа або компанія погоджується надати базу даних для цілей тренування моделей ШІ. Ліцензія у свою чергу надає дозвіл компанії або особі використовувати інтелектуальну власність іншої сторони за певну плату. Зазвичай ліцензійна угода містить умови щодо власності матеріалів авторського права та суміжних прав, а також доступу до біометричних даних та їх видалення після закінчення тренування. Крім того, ліцензування також може використовуватися для вирішення питань

конфіденційності, міркувань використання або обмежень, а також проблем навчання та інших питань, які часто можуть бути автоматизованими у зв'язку зі збором, використанням і розкриттям даних. Наприклад, деякі вебсайти або платформи надають доступ до їх даних через Інтерфейси Прикладного Програмування ("Application Programming Interfaces (APIs)"), що регулюються окремими ліцензійними угодами. Такі угоди виокремлюють дозволене та обмежене використання даних. У цьому випадку не існує проблем з порушенням авторського права, оскільки дозвіл було завчасно погоджено з власниками даних.

V. Рекомендації змін до законодавства України

Як і багато інших держав, Україна все ще знаходиться на шляху до вдосконалення законодавства щодо регулювання ШІ. З огляду на відсутність українського уніфікованого законодавства, Лабораторія цифрової безпеки передусім рекомендує розробити спеціальний Кодекс поведінки щодо регулювання ШІ (на рівні саморегулювання індустрії за моделлю Сполученого Королівства), який передбачатиме механізм збору та обробки навчальних даних для тренування ШІ, а також права суб'ктів даних, чия інформація підлягає збору, та відповідні зобов'язання, які несуть розробники систем ШІ. У контексті прийнятних законодавчих змін, Лабораторія цифрової безпеки рекомендує імплементувати європейську модель, оскільки більшість українських законів вже базується на стандартах ЄС, а Україна має зобов'язання по євроінтеграційному треку через статус кандидата на членство в ЄС. З огляду на це, рекомендується внести зміни до окремих законів України, як-от:

1) **Розробка державних політик:**

- запустити регуляторні сендбокси ("sandboxes") (за моделлю Акту ЄС про штучний інтелект) для розробки та тестування інноваційних технологій ШІ протягом визначеного часового періоду, а також механізм контролю, згідно з яким ці системи будуть розміщені на ринку або іншим чином введені в експлуатацію;
- уповноважити академічні інституції або приватних дослідників на створення відкритих баз даних, спрямованих на навчання машинних моделей, а також надання в користування розробникам ШІ навчальних даних;
- дозволити розробникам ШІ повторно використовувати дані державного сектору, які не можуть бути доступні як відкриті дані (за моделлю Європейського акту про управління даними), передбачивши

категорії таких даних, механізм їх анонімізації або модифікації перед використанням, а також захист авторського права користувачів та їх персональних даних.

2) **У Законі України “Про захист персональних даних”:**

- передбачити створення державних баз даних (з попередньо отриманою згодою від суб'єктів даних та авторів матеріалів) для надання в користування розробникам ШІ відкритих навчальних даних для цілей тренування машинних моделей;
- встановити явну згоду користувачів на збір та обробку їх біометричних даних, а також їх попереднього повідомлення про те, як ці дані будуть використовуватися, як обов'язкові вимоги для збору розробниками навчальних даних для цілей ШІ;
- встановити можливість форм анонімізації або псевдонімізації даних за вимогою суб'єкта даних;
- встановити механізм видалення навчальних даних (в тому числі і з відповідних державних баз даних) при закінченні тренування системи ШІ за вимогою суб'єкта даних.

3) **У Законі України “Про авторське право та суміжні права”:**

- поза державними базами даних та ліцензіями, які дозволяють вільне використання авторських матеріалів, встановити явну згоду авторів на збір та обробку їх матеріалів як обов'язкову вимогу для отримання розробниками ШІ навчальних даних;
- дозволити збір авторських робіт для цілей тренування ШІ, якщо подальше використання таких робіт здійснюється без мети отримання прибутку.

Аналітичний звіт підготовлено в рамках програми “Сприяння Інтернет свободі в Україні”, яку реалізує Американська Асоціація Юристів в Україні / Ініціатива верховенства права.

Лабораторія цифрової безпеки — громадська організація, що працює над створенням сприятливого середовища для реалізації цифрових прав людини через проведення аналізу та розробку рекомендацій щодо державної політики у сфері інтернет свобод та врядування, а також надає підтримку з цифрової безпеки правозахисникам, журналістам, медійним та іншим організаціям громадянського суспільства в Україні та Східній Європі.

Лабораторія Цифрової Безпеки

2023