ТРИБУНА ДОКТОРАНТА І АСПІРАНТА

DOI: 10.31359/2079-6242-2024-47-186
УДК 340.12:341.231.14

О. П. Андрущенко, аспірантка кафедри філософії Національного юридичного університету імені Ярослава Мудрого
ORCID: 0009-0004-1759-1166

ЗАХИСТ ПРАВ ЛЮДИНИ В УМОВАХ РОЗВИТКУ ШТУЧНОГО ІНТЕЛЕКТУ

Постановка проблеми. У наш час штучний інтелект (далі – ШІ) дедалі глибше проникає у повсякденне життя, змінюючи способи, способи і форми нашого спілкування і життєдіяльності у цілому. Його потенційний вплив на права людини та проблеми злочинності викликає серйозні обговорення і зацікавленість. Хоча ШІ може відкривати нові можливості для захисту прав та забезпечення безпеки, він також вносить загрози для приватності та стимулює виникнення нових видів кіберзлочинності. Отже, проблема впливу штучного інтелекту на права людини та злочинність стає надзвичайно актуальною. Розуміння цього впливу та розробка його ефективних форм і методів є ключовими завданнями для забезпечення гармонійного розвитку сучасного суспільства. З розвитком штучного інтелекту виникають нові можливості та загрози для прав людини, а також нові виклики у боротьбі зі злочинністю, які потребують адаптивних стратегій.

Аналіз останніх досліджень і публікацій. З огляду на надзвичайно швидкий розвиток технологій штучного інтелекту та їх широке застосування в різних сферах життя актуальність досліджень та публікацій із цієї тематики очевидна. Публікації, використані в статті, надають цікавий погляд на проблеми, що виникають у зв'язку з упровадженням та розвитком штучного інтелекту і його правового регулювання. О. П. Дзьобань у роботі «Цифрова людина як філософська проблема»[1] висвітлює цифрову людину як новий феномен, що виникає на основі конвергенції технологій, котрі включають ШІ та машинне навчання, та підкреслює важливість розвитку нових моральних цінностей у цифровій епосі й усвідомлення людиною віртуальної реальності.

А. Клян[2] у своїй статті звертає увагу на широке використання штучного інтелекту у різних сферах життя та виклики, які виникають у зв'язку із цим, висвітлює значення правового регулювання штучного інтелекту з метою забезпечення ефективності та етичності його застосування.

С. Р. Корнеєва[3] аналізує різні підходи до правового регулювання штучного інтелекту та наслідки цього, а також звертається до проблеми визначення статусу ШІ як об'єкта або суб'єкта правових відносин.

У статті Г. К. Авдєєвої «Системи штучного інтелекту у протидії злочинності»[4] розглядається широкий спектр застосування систем ШІ в різних сферах, включаючи правоохоронну діяльність, боротьбу зі злочинністю та підвищення рівня громадської безпеки.

---

[1] Дзьобань О. П. 'Цифрова людина як філософська проблема' (2021) 2(37) Інформація і право 9–21 <https://doi.org/10.37750/2616–6798.2021.2(37).238330/> (дата звернення: 10.03.2024).

[2] Клян А. 'Правове регулювання штучного інтелекту в Україні та світі' (GOLAW, 03 лютого 2022) <https://golaw.ua/ua/insights/publication/pravove-regulyuvannya-shtuchnogo-intelektu-v-ukrayini-ta-sviti/> (дата звернення: 10.03.2024).

[3] Корнеєва С. Р. 'Теоретичні підходи до визначення поняття та правового регулювання штучного інтелекту' (2021) 66 Науковий вісник Ужгородського національного університету 50–55. <https://doi.org/10.24144/2307–3322.2021.66.9> (дата звернення: 10.03.2024).

[4] Авдєєва Г. К. 'Системи штучного інтелекту у протидії злочинності' *Роль та місце правоохоронних органів у розбудові демократичної правової держави*: матеріали XV міжнар. наук.-практ. конф. (22 березня 2023 р., м. Одеса) 5–8

Загалом останні дослідження та публікації у сфері правового регулювання ШІ вказують на актуальність та складність проблеми, а також на необхідність подальших досліджень для розробки ефективних стратегій та політик у цій царині. Так, потребує більш глибокого філософсько-правового дослідження проблема впливу штучного інтелекту на права людини.

Метою статті є дослідження з філософських позицій впливу штучного інтелекту на права людини, прогнозування майбутніх розвиткових тенденцій у цій сфері та виявлення проблем, пов'язаних зі злочинністю, що виникають у контексті широкомасштабного застосування ШІ.

Виклад основного матеріалу. Застосування ШІ у сфері прав людини відкриває нові можливості і виклики. ШІ може допомагати в автоматизації обробки правової інформації, може використовуватися для прогнозування можливих порушень прав людини тощо. Алгоритми машинного навчання можуть аналізувати великі обсяги даних, щоб виявляти ознаки можливих порушень прав людини, такі як дискримінація, насильство чи порушення прав жінок, дітей, меншин чи біженців. ШІ може автоматизувати деякі рутинні процеси у сфері прав людини, такі як обробка запитів, складання звітів або ведення обліку правопорушень. У цілому застосування ШІ у сфері прав людини може забезпечити покращення доступу до правосуддя та підвищення ефективності правоохоронних органів, але потребує посилення уваги до етичних, приватних та безпекових питань.

Слід зазначити, що прогрес торкнувся й правоохоронної практики, особливо у частині опрацювання великих та надвеликих обсягів накопичених криміногенних даних із метою пошуку закономірностей, патернів, тенденцій, місць концентрації кримінальної активності тощо. Застосування зарубіжних сучасних методик і можливостей комп'ютерно-програмного забезпечення на рівні ШІ дозволяє суттєво удосконалити процес опрацювання таких даних, що у підсумку дозволяє вивести правоохоронну діяльність із прогнозування на якісно новий рівень. Органи та підрозділи поліції різних країн світу використовують прогнозування переважно з профілактичною метою. Такі знання є інструментом націлювання зусиль та ресурсів поліції для позитивного впливу на стан криміногенної ситуації. Аналітичні системи можуть виявляти та аналізувати такі випадки, допомагаючи швидше реагувати та захищати права тих, хто постраждав. Більше того, за допомогою штучного інтелекту може створюватися система раннього попередження порушень прав людини, що дозволить уникнути негативних наслідків та своєчасно здійснювати заходи для їх запобігання.

У США інформаційні системи працюють з метою розшуку злочинців, профайлінгу і виявлення можливих правопорушників. Інформаційні служби кримінального правосуддя (далі – CJIS) керують кількома національними системами інформації про злочини, які використовуються органами громадської безпеки як для кримінально-правових, так і соціальних цілей. Системи CJIS доступні для учасників кримінального правосуддя, включаючи правоохоронні органи, в'язниці, прокуратуру, суди, а також служби пробації та досудового розслідування. Системи CJIS також доступні органам некримінальної юстиції для спеціально дозволених цивільних цілей, таких як перевірка влаштування дитини, працевлаштування особи, житла та ліцензування[1].

Інформаційні методики та системи застосовуються у США також на регіональному рівні. Так, Департамент поліції Нью-Йорка спільно з Microsoft розробив Domain Awareness System (DAS)[2] – систему, яка агрегує й аналізує інформацію про громадську безпеку зі звітів, камер спостереження, спостережень очевидців тощо. Приблизно у такий самий спосіб працює ShotSpotter[3] – акустична система спостереження, яка фіксує постріли зі зброї та оповіщає про це поліцію. Сенсори ShotSpotter дозволяють визначити місце, де стався інцидент, із точністю до двох футів. Увесь процес – з моменту, коли постріл був зафіксований, до відправки інформації поліції – займає близько 40 секунд. Дана технологія використовується вже в 75 містах США. Програма PreCrime Observation System[4] обчислює ймовірність скоєння злочинів, ґрунтуючись на статистиці попередніх

[1] 'Criminal Justice Information Services (CJIS)' (An official website of the United States government, Department of Justice) <https://www.fbi.gov/services/cjis> (дата звернення: 10.03.2024).

[2] 'NYPD. Technology' <https://www1.nyc.gov/site/nypd/about/about-nypd/equipment-tech/technology.page> (дата звернення: 10.03.2024).

[3] 'Criminal Intelligence – Manual for Analysts' (Vienna: United Nations Publication, 2011) <https://www.unodc.org/documents/organized-crime/Law-Enforcement/Criminal_Intelligence_for_Analysts.pdf> (дата звернення: 10.03.2024).

[4] 'Precrime' <https://www.pre-crime.eu/> (дата звернення: 10.03.2024).

правопорушень. Отже, США мають розвинену мережу інформаційних систем, які дозволяють оперативно отримувати інформацію про стан злочинності в країні для формування відповідних напрямів кримінологічної політики.

Також одним із найбільш часто використовуваних інструментів підготовки прогнозів є Predictive Policing (PredPol). PredPol – це компанія, що здійснює діяльність із передбачення злочинів за допомогою прогнозової аналітики. Починаючи з 2020 року, алгоритм PredPol є найбільш часто вживаним алгоритмом моделі здійснення правоохоронної діяльності на основі прогнозів у поліції США. Відділам поліції, які використовують PredPol, видаються роздруківки карт юрисдикції, на яких позначають райони, де передбачається, що злочин може мати місце протягом найближчого дня. Використовуючи для прогнозування лише три типи даних – тип інциденту, дата / час інциденту та місце його прояву, технологія PredPol допомагає правоохоронним органам значно зменшити рівень злочинності в юрисдикціях усіх видів та розмірів, як у США, так і за кордоном[1]. Цінність прогнозів проактивної моделі правоохоронної діяльності Predictive Policing полягає також і в тому, що вони використовуються під час визначення ймовірності виникнення ризиків та оцінювання рівня їх впливу на стан криміногенної ситуації, що має важливе значення для обґрунтування розподілу ресурсів та прийняття рішень стосовно вирішення відповідних проблем[2]. Проте важливо пам'ятати про потенційні ризики, які супроводжують застосування штучного інтелекту у сфері прав людини. Наприклад, системи виявляються вразливими до алгоритмічного упередження, яке може призвести до некоректного виявлення порушень або підтримки системних нерівностей. Тому необхідно ретельно контролювати процеси розробки та впровадження штучного інтелекту, забезпечуючи їх прозорість та відповідність принципам справедливості й недискримінації. Також потрібно забезпечити конфіденційність особистої інформації та її захист від можливих кібератак, щоб уникнути порушення приватності, а також інших прав людини у контексті використання штучного інтелекту.

Можна констатувати, що здійснення правоохоронної діяльності на основі прогнозів межує з низкою проблем, які впливають на її ефективність. Як зазначають Е. Рижков та Я. Дзех, проблемою, яка потребує вирішення під час функціонування підрозділів інформаційно-аналітичної підтримки, є осучаснення матеріально-технічної бази та належне фінансування для придбання техніки і ліцензійного програмного забезпечення[3]. Інша комплексна проблема, що впливає на функцію прогнозування у діяльності поліції, є те, що зазначена проактивна модель покладається на аналіз, який проводиться шляхом усвідомленого опрацювання кримінальними аналітиками, у тому числі з використанням комп'ютерного програмного забезпечення, наявних вхідних даних для ідентифікації шаблонів, тенденцій, закономірностей тощо. У першу чергу, якість прогнозів напряму залежатиме від точності даних, які містяться у системах інформаційно-аналітичного забезпечення та базах даних поліції й інших базах даних, котрі використовують співробітники правоохоронних органів. Також вирішальне значення матиме вміння кримінальними аналітикам трактувати наявні дані та формувати з них релевантні прогнози про розвиток подій у майбутньому, яким має бути властивий високий ступінь вірогідності. Як перша складова (якість, точність та повнота даних), так і друга складова проблеми (трактування та підготовка прогнозів) можуть призвести до упереджених результатів (об'єктом посиленої роботи поліції можуть стати окремі (наприклад, незабезпечені) прошарки суспільства. Також слід зазначити, що у практиці діяльності поліції різних країн світу існує тенденція маніпуляції із відомостями, які підлягають реєстрації, що у підсумку призведе до помилкових та неточних прогнозів. Таким чином, необхідно забезпечити захист приватності осіб, які стануть об'єктом аналізу та моніторингу, і уникнути можливості зловживання зібраними даними. Також потрібно уникати потенційного використовування штучного інтелекту для підтримки або спрощення систем, які порушують

[1] 'Predpol. Proven Crime Reduction Results' <https://www.predpol.com/schedule-a-demo> (дата звернення: 10.03.2024).

[2] 'Predictive Policing. The Role of Crime Forecasting in Law Enforcement Operations' <https://www.rand.org/pubs/research_reports/RR233.html> (дата звернення: 10.03.2024).

[3] Рижков Е. В., Дзех Я. С. 'Проблемні питання інформаційно-аналітичного забезпечення в системі органів Національної поліції та проблемні питання щодо захисту інформації під час виконання службових обов'язків' *Проблеми застосування інформаційних технологій правоохоронними структурами України та закладами вищої освіти зі специфічними умовами навчання* : збірник наукових статей за матеріалами доповідей Всеукраїнської науково-практичної конференції (21 грудня 2018 року, м. Львів) 83

права людини, наприклад, у випадках систем масового спостереження або систем соціального контролю.

Як слушно зазначає Г. К. Авдєєва, системи ШІ ефективно вирішують завдання щодо ідентифікації осіб за фотознімками, відеозаписами та пробами ДНК. Зокрема, американська система розпізнавання осіб Clearview AI використовує базу даних із 10 млрд фотопортретів і показує свою ефективність на практиці. Однак через можливі порушення прав людини парламент ЄС запропонував заборонити збирання фотозображень осіб до приватних систем розпізнавання (у тому числі Clearview)[1]. Як справедливо зазначає О. П. Дзьобань, «Віртуальний світ, створений новітніми інформаційними технологіями, включає людину у процес сприйняття цілком і відразу. Виникає багатоликість створюваного віртуального світу, нескінченне павутиння ходів користувача інформаційно-комунікаційних засобів. Залежно від ситуації один і той же контекст може бути розглянуто під різними кутами зору, і це вже накладає певний відбиток на створюваний віртуальний потік»[2].

У жовтні 2022 року Національна комісія Франції з питань інформатики та свобод оштрафувала компанію Clearview AI на 20 млн євро за порушення конфіденційності французьких користувачів. Національна комісія з питань інформатики та свободи (CNIL) видала наказ Clearview AI не обробляти дані осіб, які перебувають у Франції, якщо для цього відсутні законні підстави і видалити всі вже зібрані дані[3]. Цей приклад демонструє важливість етичного та законного використання інформації у цифровому середовищі, а також потребу ефективного регулювання цих процесів для захисту приватності користувачів.

Також існують й інші негативні результати використання систем ШІ. Зокрема, в США з 2013 р. по 2016 р. у поліції проходила тестування система Watson компанії IBM, яка автоматично складала стандартні звіти і процесуальні документи після усного повідомлення інформації електронному помічникові. Через низьку якість отриманих документів та, як наслідок, суттєве зниження якості роботи, поліцейські надали негативну оцінку системі Watson та припинили її використання[4]. Таким чином, використання ШІ може призвести до збору великих обсягів особистих даних, що може порушити приватність користувачів, особливо якщо ці дані використовуються без їх згоди, а недостатньо точні або неправильно налаштовані алгоритми можуть сприяти формулюванню неправильних чи дискримінаційних висновків, що може порушити права людини.

Фундаментальні технології штучного інтелекту покликані сприяти трансформуванню економіки, ринку праці, державних установ і, як результат, – суспільства загалом. Використання таких технологій відкриває неосяжні можливості в різних сферах соціально-економічного життя (підвищення ефективності виробництва, зменшення витрат, поліпшення якості товарів і послуг та ін.)[5].

Водночас, незважаючи на сприйняття ШІ як успішної й популярної цифрової технології, її застосування в різних сферах суспільного життя має відповідати основним правам людини, закріпленим у міжнародних документах. Це пов'язано з наявністю певного конфлікту між інтересами суб'єктів (що прагнуть економічного зростання, автоматизації та кадрових змін) і дотриманням прав, свобод та інтересів людини в разі застосування технологій штучного інтелекту.

Розвиток ШІ призводить до значних змін у правовому середовищі, тому передбачити всі аспекти цих змін складно. Отже, питання правового регулювання сфери ШІ та його впливу на реалізацію й захист прав людини перебувають на етапі активних наукових обговорень та новітніх розробок. У таких умовах фундаментальні права людини, які гарантовані основними законами більшості країн, зокрема, свобода та недоторканність, невтручання в приватне життя, свобода думки і слова, набувають розширеного змісту.

[1] Авдєєва Г. К. 'Системи штучного інтелекту у протидії злочинності' *Роль та місце правоохоронних органів у розбудові демократичної правової держави*: матеріали XV міжнар. наук.-практ. конф. (22 березня 2023 р., м. Одеса) 6

[2] Дзьобань О. П. 'Цифрова людина як філософська проблема' (2021) 2(37) Інформація і право 14 <https://doi.org/10.37750/2616–6798.2021.2(37).238330/> (дата звернення: 10.03.2024).

[3] 'France sees global A. I. regulation ideas by the end of this year, wants to work with U. S. on tech laws' <https://www.cnbc.com/2023/06/15/ai-regulation-france-sees-ideas-on-global-laws-by-end-of-year.html> (дата звернення: 10.03.2024).

[4] Авдєєва Г. К. 'Системи штучного інтелекту у протидії злочинності' *Роль та місце правоохоронних органів у розбудові демократичної правової держави*: матеріали XV міжнар. наук.-практ. конф. (22 березня 2023 р., м. Одеса) 6

[5] Kosilova O. I., Rozghon O. V., Solodovnikova C. K., Stolbovyi V. M., Barabash O. O. 'Observance of Human Rights in the Use of AI as Technology' (2022) 14(2) Law, State and Telecommunications Review 38–67 <DOI: 10.26512/lstr.v14i2.41558> (дата звернення: 10.03.2024).

В Європейському Союзі перші спроби регламентування ШІ, зокрема роботів, були ухвалені Резолюцією Європарламенту від 16 лютого 2017 р. У галузі цивільного права для врегулювання питань, пов'язаних із робототехнікою, ухвалені такі механізми: створення системи реєстрації роботів і спеціального фонду страхування цивільної відповідальності, пропорційна відповідальність розробників і власників роботів. Надалі, ускладнення таких технологій вимагатиме переходу до нової, більш складної, схеми правового регулювання[1].

Загалом мета Європейського Союзу – сприяти розвитку надійного, етичного ШІ, який відповідає нормам законодавства. Із цією метою ЄС працює над адаптацією законодавства, розробляє етичні принципи та правові норми, що стосуються використання ШІ. Зокрема, починаючи з 2021 року в рамках ЄС розробляється перший у світі Закон про ШІ – Artificial Intelligence Act. Саме в проекті цього Акта вперше надано розгорнуте правове визначення ШІ в ЄС: «Штучний інтелект – це машинна система, яка розроблена для роботи з різним рівнем автономності та яка може, для явних або прихованих цілей, генерувати результати, такі як прогнози, рекомендації або рішення, що впливають на фізичне або віртуальне середовище»[2].

Окрім того, корисним та цікавим в аналізованій сфері є досвід Великої Британії, адже ця країна розробила та затвердила базові стандарти з державного регулювання процесами, пов'язаними з упровадженням технологій ШІ. Ці стандарти були викладені у Національній Стратегії штучного інтелекту, підготовленій урядом Великої Британії та опублікованій 22 вересня 2021 р., а так само у координаційному документі під назвою «Створення інноваційного підходу до регулювання штучного інтелекту», представленому урядом 18 липня 2022 р.[3]

Зрештою, розвиток ШІ впливає на багато аспектів правового середовища. Тому важливо вносити відповідні зміни в законодавство та практику, щоб забезпечити його ефективність, справедливість та відповідність основним правам людини.

Сучасна злочинність постійно еволюціонує, а злочинці швидко адаптуються до нових технологій і методів. Тому існує потреба у постійному вдосконаленні правових інструментів, щоб вони відповідали новим викликам і загрозам. Сучасний глобалізований світ зазнав кардинальних соціальних і технологічних трансформацій. Кіберзлочини стають ще більш складними та заплутаними. Основою, на якій будуються суспільства та підприємства, сьогодні є онлайн-світ, цифрові пристрої та технології.

Для досягнення очікуваних результатів у розслідуванні кіберзлочинів, потрібно посилити оперативну спроможність правоохоронних та/або судових органів для розслідування кібератак і кіберзлочинів, а також надати нові методи розслідування та інструменти (зокрема, для цифрової криміналістики), щоб зосередитись на сферах із найбільшою загрозою. До такого інструментарію належать: цифрова криміналістика (наприклад, криміналістика мобільних пристроїв, комп'ютерів, мереж, Інтернету речей і транспортних засобів); візуальний аналіз даних; аналіз шкідливих програм і можливості зворотного проектування; аналіз та арешт криптовалют; ефективне зберігання, обробка, аналіз і передача великих даних; розуміння та використання метаданих і «розвідки про загрози»; моніторинг Dark Web[4]. Тому поява нових форм злочинності вимагає вдосконалення технологій та правового регулювання для ефективного захисту від них, включаючи розробку нових методів виявлення та протидії.

Можна констатувати, що розробка стратегій і рекомендацій для захисту прав людини та боротьби зі злочинністю в контексті штучного інтелекту вимагає комплексного підходу, що об'єднує правове регулювання, технологічні інновації та співпрацю між різними зацікавленими сторонами.

---

[1] Корнеєва С. Р. 'Теоретичні підходи до визначення поняття та правового регулювання штучного інтелекту' (2021) 66 Науковий вісник Ужгородського національного університету 50–55 <https://doi.org/10.24144/2307–3322.2021.66.9> (дата звернення: 10.03.2024).

[2] European Parliament resolution of 16 February 2017 with recommendations to the Commission on Civil Law Rules on Robotics (2015/2103(INL)). Official Journal of the European Union. 18.7.2018. <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX-:52017IP0051&rid=9> (дата звернення: 10.03.2024).

[3] Клян А. 'Правове регулювання штучного інтелекту в Україні та світі' (GOLAW, 03 лютого 2022) <https://golaw.ua/ua/insights/publication/pravove-regulyuvannya-shtuchnogo-intelektu-v-ukrayini-ta-sviti/> (дата звернення: 10.03.2024).

[4] Staniforth A. 'Cybercrime innovation: Transforming digital investigation tools, techniques, and technologies' (Policing Insight. 13th August 2022) <https://policinginsight.com/feature/analysis/cybercrime-innovation-transforming-digital-investigation-tools-techniques-and-technologies/> (дата звернення: 10.03.2024).

Що стосується правового регулювання, законодавчі органи повинні розробляти та впроваджувати нормативно-правові акти, що будуть в повній мірі регулювати використання штучного інтелекту в сфері прав людини та боротьби зі злочинністю. Вони мають включати в себе правила щодо захисту приватності, заборони дискримінації, етичного використання алгоритмів тощо. Закони повинні вимагати від компаній, що використовують ШІ, надавати прозору та доступну інформацію про алгоритми, дані та вплив ШІ на права людини. Також мають створюватися групи для моніторингу за дотриманням прав людини та боротьби зі злочинністю в контексті ШІ.

Технологічна складова майбутніх інновацій повинна містити механізм етичних алгоритмів, які будуть відповідати принципам справедливості та прозорості. Розробникам слід використовувати технології шифрування та анонімізації для захисту особистих даних, а також розробляти системи контролю доступу та автентифікації з метою обмеження доступу до чутливої інформації. Крім того, потрібно встановлювати механізми відповідальності за можливі порушення прав людини, щоб стимулювати розробників та операторів до дотримання етичних і правових стандартів.

Так само слід відмітити, що ефективна боротьба з порушеннями прав людини та злочинністю в контексті ШІ вимагає співпраці між різними секторами суспільства. Урядові органи, громадські організації та приватні компанії повинні спільно працювати над розробкою та виконанням стратегій і заходів із забезпечення прав людини та боротьби зі злочинністю з огляду на інструменти ШІ. Усі заходи щодо захисту прав людини та боротьби зі злочинністю мають ґрунтуватися на принципах доступності та рівноправ'я, тобто необхідно враховувати потреби й інтереси різних груп населення, у тому числі осіб з інвалідністю, етнічних та мовних меншин.

Крім цього, стратегії та рекомендації повинні постійно оновлюватися й адаптуватися до швидкого розвитку технологій ШІ та змін у соціальному, економічному і політичному середовищі.

Висновки. Із розвитком ШІ з'являються як нові можливості, так й виклики у сфері боротьби зі злочинністю та захисту прав людини. Нові технології можуть використовуватися як для запобігання злочинності, так і для вчинення злочинів, включаючи кіберзлочини й порушення приватності. Захист прав людини в умовах розвитку штучного інтелекту потребує комплексного підходу, що об'єднує правове регулювання, технологічні інновації та співпрацю між різними зацікавленими сторонами. Реалізація вищевказаних стратегій та рекомендацій допоможе забезпечити баланс між розвитком ШІ та захистом прав людини, зменшити ризики використання ШІ для злочинних цілей і збільшити довіру громадськості до цих технологій.

REFERENCES

List of legal documents

Legislation

1. European Parliament resolution of 16 February 2017 with recommendations to the Commission on Civil Law Rules on Robotics (2015/2103(INL)). Official Journal of the European Union 18.7.2018 <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX-:52017IP0051&rid=9>

Bibliography

Journal articles

1. Dzoban O. P. 'Tsyfrova liudyna yak filosofska problema' [Digital man as a philosophical problem] (2021) 2 (37) Informatsiia i pravo 9–21 <DOI https://doi.org/10.37750/2616–6798.2021.2(37).238330/> (in Ukrainian)
2. Korneieva S. R. 'Teoretychni pidkhody do vyznachennia poniattia ta pravovoho rehuliuvannia shtuchnoho intelektu' [Theoretical approaches to the definition of the concept and legal regulation of artificial intelligence] (2021) 66 Naukovyi visnyk Uzhhorodskoho natsionalnoho universytetu 50–55 (in Ukrainian)
3. Kosilova O. I., Rozghon O. V., Solodovnikova C. K., Stolbovyi V. M., Barabash O. O. 'Observance of Human Rights in the Use of AI as Technology' (2022) 14 (2) Law, State and Telecommunications Review 38–67 <DOI 10.26512/lstr.v14i2.41558> (in English)

Conference paper

4. Avdieieva H. K. 'Systemy shtuchnoho intelektu u protydii zlochynnosti' [Artificial intelligence systems in the fight against crime] *Rol ta mistse pravookhoronnykh orhaniv u rozbudovi demokratychnoi pravovoi derzhavy*: materialy XV mizhnar. nauk.-prakt. konf. (22 bereznia 2023 r., m. Odesa) 5–8 (in Ukrainian)

5. Ryzhkov E. V., Dzekh Ya. S. 'Problemni pytannia informatsiino-analitychnoho zabezpechennia v systemi orhaniv Natsionalnoi politsii ta problemni pytannia shchodo zakhystu informatsii pid chas vykonannia sluzhbovykh oboviazkiv.' [Problematic issues of information and analytical support in the system of the National Police bodies and problematic issues regarding the protection of information during the performance of official duties] *Problemy zastosuvannia informatsiinykh tekhnolohii pravookhoronnymy strukturamy Ukrainy ta zakladamy vyshchoi osvity zi spetsyfichnymy umovamy navchannia* : zbirnyk naukovykh statei za materialamy dopovidei Vseukrainskoi naukovo-praktychnoi konferentsii (21 hrudnia 2018 r., m. Lviv) 83–86 (in Ukrainian)

Websites

6. 'Criminal Intelligence – Manual for Analysts' (Vienna: United Nations Publication, 2011) <https://www.unodc.org/documents/organized-crime/Law-Enforcement/Criminal_Intelligence_for_Analysts.pdf> (in English)
7. 'Criminal Justice Information Services (CJIS)' (An official website of the United States government, Department of Justice) <https://www.fbi.gov/services/cjis> (in English)
8. 'France sees global A. I. regulation ideas by the end of this year, wants to work with U. S. on tech laws' <https://www. cnbc.com/2023/06/15/ai-regulation-france-sees-ideas-on-global-laws-by-end-of-year.html> (in English)
9. Klian A. 'Pravove rehuliuvannia shtuchnoho intelektu v Ukraini ta sviti' [Legal regulation of artificial intelligence in Ukraine and the world] (GOLAW 03 Liutoho 2022) <https://golaw.ua/ua/insights/publication/pravove-regulyuvannya-shtuchnogo-intelektu-v-ukrayini-ta-sviti/> (in Ukrainian)
10. 'NYPD. Technology' <https://www1.nyc.gov/site/nypd/about/about-nypd/equipment-tech/technology.page> (in English)
11. Staniforth A. 'Cybercrime innovation: Transforming digital investigation tools, techniques, and technologies' (Policing Insight. 13th August 2022) <https://policinginsight.com/feature/analysis/cybercrime-innovation-transforming-digital-investigation-tools-techniques-and-technologies> (in English)
12. 'Precrime' <https://www.pre-crime.eu/> (in English)
13. 'Predictive Policing. The Role of Crime Forecasting in Law Enforcement Operations' <https://www.rand.org/pubs/research_reports/RR233.html> (in English)
14. 'Predpol. Proven Crime Reduction Results' <https://www.predpol.com/schedule-a-demo> (in English)

Андрущенко О. П.

Вплив штучного інтелекту на захист прав людини: проблеми, прогнози та перспективи боротьби зі злочинністю

Стаття присвячена уточненню окремих аспектів філософсько-правової рефлексії впливу штучного інтелекту на забезпечення прав людини та виявлення пов'язаних з конкретними аспектами використання цієї технології способів боротьби зі злочинністю в цьому контексті. Висвітлено проблеми та перспективи використання штучного інтелекту в сучасному суспільстві, зокрема його впливу на правове середовище та захист прав людини. Зазначається необхідність етичних алгоритмів технологічної складової майбутніх інновацій, застосування шифрування та анонімізації для захисту даних та механізмів відповідальності для розробників. Наголошується на важливості співпраці між секторами суспільства та постійного оновлення стратегій у зв'язку зі швидким розвитком технологій штучного інтелекту. Проаналізовані тенденції у сфері прав людини та розвитку штучного інтелекту, на підставі чого окреслені шляхи боротьби із проблемами, що з'являються.

Ключові слова: *права людини, штучний інтелект, правове регулювання, захист прав людини.*

Andrushchenko O. P.

The Impact of Artificial Intelligence on Human Rights Protection: Problems, Forecasts and Prospects for Combating Crime

The article is devoted to clarifying certain aspects of the philosophical and legal reflection on the impact of artificial intelligence on human rights and identifying the ways of combating crime in this context related to specific aspects of the use of this technology. The author highlights the problems and prospects of using artificial intelligence in modern society, in particular, its impact on the legal environment and human rights protection. The author points out the need for ethical algorithms for the technological component of future innovations, the use of encryption and anonymisation to protect

data, and accountability mechanisms for developers. The author emphasises the importance of cooperation between sectors of society and constant updating of strategies due to the rapid development of artificial intelligence technologies. Trends in human rights and the development of artificial intelligence are analysed, and ways to combat emerging problems are outlined.

Keywords: *human rights, artificial intelligence, legal regulation, human rights protection.*

Стаття надійшла до редакції:15.04.2024 р.
Прийнята до друку: 20.05.2024 р.