

УДК 342.72/.73:519

КОСІЛОВА О.І., кандидат політичних наук, доцент, науковий співробітник
Київського національного університету імені Тараса Шевченка,
Інститут права.
ORCID: <https://orcid.org/0000-0002-5574-3771>.

СОЛОДОВНИКОВА Х.К., кандидат психологічних наук, юрист, Київський
національний університет імені Тараса Шевченка,
Інститут права.
ORCID: <https://orcid.org/0000-0002-9169-9026>.

ПРАВА І СВОБОДИ ЛЮДИНИ І ГРОМАДЯНИНА V.S. ШТУЧНИЙ ІНТЕЛЕКТ: ПРОБЛЕМНІ АСПЕКТИ

Анотація. В статті аналізуються актуальні проблеми забезпечення та порушень основоположних прав і свобод людини і громадянина у зв'язку з застосуванням технологій штучного інтелекту. Здійснено спробу комплексного аналізу впливу штучного інтелекту на права і свободи особи, проаналізовано окремі факти порушень прав і свобод, визначені виклики та загрози, а також правові методи захисту прав і свобод. Здійснено аналіз поточного стану нормативно-правового регулювання правовідносин, пов'язаних з використанням штучного інтелекту в Україні, визначено прогалини правового регулювання.

Ключові слова: права людини, штучний інтелект, захист прав і свобод, нормативне регулювання, загрози, виклики, інформаційні технології, Інтернет речей, електронна особа, кібербезпека.

Summary. The article analyzes the current problems of ensuring and violations of fundamental human and civil rights and freedoms in connection with the use of artificial intelligence technologies. An attempt was made to comprehensively analyze the impact of artificial intelligence on the rights and freedoms of the individual, analyzed some facts of violations of rights and freedoms, identified challenges and threats, as well as legal methods of protection of rights and freedoms. An analysis of the current state of legal regulation of legal relations related to the use of artificial intelligence in Ukraine, identified gaps in legal regulation.

Keywords: human rights, artificial intelligence, protection of rights and freedoms, legal regulation, threats, challenges, information technologies, Internet of things, electronic person, cybersecurity.

Аннотация. В статье анализируются актуальные проблемы обеспечения и нарушений основных прав и свобод человека и гражданина в связи с применением технологий искусственного интеллекта. Предпринята попытка комплексного анализа влияния искусственного интеллекта на права и свободы человека, проанализированы отдельные факты нарушений прав и свобод, некоторые вызовы и угрозы, а также правовые методы защиты прав и свобод. Осуществлен анализ текущего состояния нормативно-правового регулирования правоотношений связанных с использованием искусственного интеллекта в Украине, определены пробелы правового регулирования.

Ключевые слова: права человека, искусственный интеллект, защита прав и свобод, нормативное регулирование, угрозы, вызовы, информационные технологии, Интернет-вещей, электронная личность, кибербезопасность.

Постановка проблеми. Сучасний світ сьогодні переживає четверту промислову революцію, “постінформаційні” реалії задають нові тренди в контексті захисту і дотримання основоположних прав людини. Внаслідок розширення сфери застосування

технологій штучного інтелекту виникає низка загроз та викликів правам і свободам особи. Проте в Україні ці питання розглядаються переважно в межах розв'язання проблем захисту персональних даних. Інші аспекти порушення прав і свобод на сьогоднішній день ще не стали деталізованим предметом наукових досліджень. Новизною в даній роботі є спроба системного підходу щодо можливих загроз і викликів правам та свободам особи та, відповідно, аналіз правових методів захисту прав та свобод людини і громадянина в цих умовах.

Результати аналізу наукових публікацій. Дослідження у галузі розвитку та застосування штучного інтелекту в Україні є предметом міждисциплінарних досліджень та тільки набувають свого розвитку. Зокрема, серед українських дослідників, кримінально-правовий аспект штучного інтелекту досліджує Радутний О.Е., відповідальність суб'єктів інформаційних відносин за умов подальшого розвитку автономних роботів і штучного інтелекту – Кохановська О.В., правосуб'єктність штучного інтелекту – Кошелева К.О., нормативно-правове регулювання застосування технологій штучного інтелекту – Власюк В.В., Мудриєвська Л., правове регулювання Інтернету речей – Баранов О.А., Брайчевський С.М., Гребенюк М., проблеми приватності, конфіденційності, охорони, захисту та безпеки персональних даних в умовах застосування новітніх технологій – Брижко В.М. та інші.

Проте на сьогодні в Україні недостатньо уваги приділяється комплексному аналізу штучного інтелекту з позицій дотримання та захисту основоположних прав і свобод людини і громадянина.

Метою статті є розкрити актуальні питання прав і свобод людини і громадянина у взаємодії зі штучним інтелектом.

Відповідно меті сформовано такі завдання: дослідження окремих загроз порушень деяких основоположних прав і свобод людини внаслідок застосування штучного інтелекту; аналіз стану нормативно-правового регулювання правовідносин пов'язаних з використанням штучного інтелекту; виявлення прогалин правового врегулювання, аналіз діючих механізмів захисту порушених прав та свобод.

Виклад основного матеріалу. Вступ України до Ради Європи, з одного боку, став суттєвим кроком нашої держави на шляху до європейської інтеграції, а з другого – засвідчив прийняття Україною на себе цілої низки міжнародно-правових зобов'язань, насамперед, щодо поваги та захисту прав людини. Чільне місце серед виконаних зобов'язань перед Радою Європи займає ратифікація Україною Конвенції про захист прав і основоположних свобод людини у 1997 р. [1], з визнанням юрисдикції Європейського суду з прав людини. Як зазначають численні дослідники, Україні необхідно адаптувати та гармонізувати своє законодавство в даній сфері з законодавством Європейського Союзу.

Бостром Н., у книзі “Штучний інтелект”, пише, що людство не просто на порозі відкриття “надрозуму”, а й може просто вже опинитися перед обличчям загрози, яка полягає в жорсткій конкуренції між людиною та штучним інтелектом, і останній стрімко завойовує усі сфери буття людини, що, на думку вченого, є серйозною загрозою основоположним правам людини. У зв'язку з цим дослідник наголошує, що людина потребує всебічного захисту вже, в тому числі й юридично-правового [2]. Через стрімке поширення та розвиток технологій штучного інтелекту за кордоном вже давно ведуться численні наукові дискусії серед “скептиків та оптимістів” в різних галузях наук, починаючи від філософії, економіки і права, не кажучи вже про науки, пов'язані з комп'ютерами.

Так, Законодавство ЄС включає 515 актів європейського права, які використовують термін “Internet of Things” (*All EU law*). Можна класифікувати їх за різними критеріями, а саме: за джерелами, роками видання. Так, за суб'єктами правотворчості: European

Commission (224); Council of the European Union (172); European Economic and Social Committee (61); Directorate-General for Communications Networks, Content and Technology (59); European Parliament (48) тощо; за роками видання: 2019 – 77; 2018 – 149; 2017 – 107; 2016 – 83; 2015 – 15 тощо [3].

На відміну від європейських країн стан законодавства в нашій державі знаходиться лише на початковому етапі на шляху до унормування нового типу правовідносин за умови застосування технологій штучного інтелекту у різні сфери та потребує його удосконалення та гармонізації з європейським у цій сфері.

Регулювання питань щодо застосування штучного інтелекту має здійснюватися відповідно до норм міжнародних договорів та конвенцій, що ратифіковані більшістю (європейських) держав. Зокрема, відповідно до спеціалізованих міжнародних договорів у сфері розвитку штучного інтелекту: Конвенції Ради Європи про кіберзлочинність, також відома як Будапештська конвенція [4]; Етичної хартії по використанню штучного інтелекту у судовій системі та її середовищі (*European ethical Charter on the use of Artificial Intelligence in judicial systems and their environment*), Загального Регламенту захисту даних (ЄС) 2016/679 від 27.04.16 р. (*General Data Protection Regulation*) [5].

Україна вже використовує досвід провідних європейських держав (зокрема Естонії) у сфері застосування технологій штучного інтелекту у публічне адміністрування та рухається в напрямку створення е-України. Так, Міністерством цифрової трансформації України (далі – Мінцифри України) було розроблено Концепцію розвитку штучного інтелекту в Україні [6]. Як зазначила заступник міністра цифрової трансформації Іонан В.: “Наша головна мета – сприяння розвитку штучного інтелекту й інтеграція його в економічно важливі сектори. Таким чином ми збільшимо частку інтелектуально ємних продуктів і значно зміцнимо позиції України на світовому ринку. Особливу увагу планується приділяти використанню штучного інтелекту в сфері кібербезпеки й оборони. Також дуже важливо мати правильний баланс між штучним інтелектом, розробленим сторонніми постачальниками і національними” [6].

28 січня 1981 року було прийнято першу міжнародну угоду в сфері персональних даних – Конвенцію Ради Європи “Про захист осіб у зв’язку з автоматизованою обробкою персональних даних” (відома як Конвенція РЄ № 108, згідно з порядком у серії Європейських договорів). Відповідно цієї Конвенції сторони зобов’язані вжити необхідних заходів у своєму внутрішньому законодавстві для застосування принципів, які вона встановлює, для забезпечення поваги на своїй території основних прав людини всіх осіб щодо обробки персональних даних. У липня 2010 року Україна ратифікувала Конвенцію РЄ № 108.

Консультативний комітет Ради Європи, створений відповідно до Конвенції РЄ № 108, який працює над захистом фізичних осіб у сфері автоматизованої обробки персональних даних, у січні 2019 р. прийняв Керівні принципи щодо штучного інтелекту та захисту даних. В цьому документі Комітет визнав, що штучний інтелект є корисним інструментом під час прийняття рішень, зокрема щоб підтримати науково обґрунтовані та інклюзивні політики та наголосити на необхідності розвитку й використання штучного інтелекту з усвідомленням права на повагу до приватного життя та захист персональних даних.

Документ ґрунтується на переконанні, що використання штучного інтелекту в жодному разі не має загрожувати людській гідності, правам людини та основоположним свободам, зокрема в тому, що стосується права на захист даних, оскільки це закріплено в Європейській конвенції про права людини та в модернізованій Конвенції РЄ № 108.

У травні 2018 року Рада Європи прийняла Протокол CETS № 223, яким було внесено зміни до Конвенції РЄ № 108. Модернізована Конвенція РЄ № 108+ враховує більшість викликів, спричинених розвитком інформаційних і комунікаційних технологій та посилює вимоги щодо її імплементації. Таким чином перед Україною постало питання ратифікації Протоколу, яким було внесено зміни до Конвенції РЄ № 108. Це дозволить покращити ситуацію з дотриманням прав людини у сфері захисту персональних даних.

Концепція, яку розробили в Мінцифри України, передбачає розвиток людського капіталу та акцент на освіті розробників у сфері штучного інтелекту, розвиток підприємств з використанням штучного інтелекту, активне впровадження технологій штучного інтелекту в держсекторі й основних індустріях країни. Також вона передбачає необхідність дотримання права на конфіденційність і приватність людини (в міністерстві планують розробити Етичний Кодекс використання штучного інтелекту “враховуючи європейський досвід”). У Мінцифри України вже створили експертний комітет з питань штучного інтелекту [7]. В останні дні вересня цього року міністерство презентувало концепцію держави в смартфоні – онлайн платформу “Дія”. За планом до 2024 року 100 % держпослуг будуть доступні українцям онлайн [8].

Протягом тривалого часу в Україні не існувало законодавства, яке врегульовувало б питання забезпечення безпеки як в інформаційному, так і в кіберпросторі. Першою спробою врегулювати це питання був проект Закону України “Про засади інформаційної безпеки України”, яким пропонувалося розмежування інформаційної та кібербезпеки. Отже, основною вимогою є те, що зібрані особисті відомості мають бути достатньо захищеними, персональні дані повинні збиратися, використовуватися та надаватися зі знанням та згодою особи, а також особа повинна мати доступ до особистих відомостей, що збираються про неї, включаючи можливість виправлення або видалення неправильних даних. Для тих, хто незаконно збирає, зберігає, знищує та поширює конфіденційну інформацію про особу передбачена стаття 182 (Порушення недоторканності приватного життя) Кримінального кодексу України (далі – КК України) [9]. Покарання за таку діяльність становить від 8500 до 17000 гривень, а за повторні злочини – навіть позбавлення волі на строк від 3 до 5 років [10].

В порівнянні з іншими злочинами проти особи ця стаття має достатньо невеликий відсоток вироків суду, крім того, що виключно за повторне вчинення дій передбачено покарання у вигляді позбавлення волі. В цілому законодавець передбачив достатньо м’яке покарання з порівняно невеликою сумою штрафу.

Це судження стає справедливим, особливо якщо врахувати, що в Україні порушення даної статті КК України відбувається, згідно проаналізованих даних, в основному в через витоки на широкий загал (в мережу Інтернет) персональних даних клієнтів банків, на другому місці – витоки інформації з закладів, що надають медичні послуги.

Право на приватність, конфіденційність та захист персональних даних є старим основоположним правом людини, яке отримало нову та особливу актуальність з поширенням і розвитком інформаційних технологій. Саме це право нам гарантує Закон “Про захист персональних даних” [11]. Відповідно до статті 5 вказаного закону, основними суб’єктами загального забезпечення кібербезпеки у межах всієї держави є: Президент України, який здійснює координацію діяльності у сфері кібербезпеки як складової національної безпеки України, через очолювану ним Раду національної безпеки і оборони України; Національний координаційний центр кібербезпеки, як робочий орган Ради національної безпеки і оборони; Кабінет Міністрів України.

Суб'єктами, які безпосередньо здійснюють у межах своєї компетенції заходи із забезпечення кібербезпеки, є: міністерства та інші центральні органи виконавчої влади; місцеві державні адміністрації; органи місцевого самоврядування; правоохоронні, розвідувальні і контррозвідувальні органи, суб'єкти оперативно-розшукової діяльності; Збройні Сили України, інші військові формування, утворені відповідно до закону; Національний банк України; підприємства, установи та організації, віднесені до об'єктів критичної інфраструктури; суб'єкти господарювання, громадяни України та об'єднання громадян, інші особи, які провадять діяльність та/або надають послуги, пов'язані з національними інформаційними ресурсами, інформаційними електронними послугами, здійсненням електронних правочинів, електронними комунікаціями, захистом інформації та кіберзахистом.

В Україні функцію зі захисту персональних даних покладено на Уповноваженого Верховної Ради України з прав людини (Омбудсмена). У структурі Секретаріату Уповноваженого Верховної Ради України з прав людини було створено окремий Департамент у сфері захисту персональних даних [12]. До повноважень Уповноваженого, відповідно до статті 23 Закону “Про захист персональних даних”, відноситься, проведення перевірок, видання приписів про запобігання або усунення порушень законодавства про захист персональних даних, надання рекомендацій щодо практичного застосування законодавства про захист персональних даних, складання протоколів про притягнення до адміністративної відповідальності та направлення їх до суду. Відповідно до визначених законом компетенцій, Уповноважений є медіатором, а не каральним органом і не може безпосередньо накладати санкції. На підставі проведених перевірок рішення про накладання санкцій ухвалюють суди, що значно уповільнює процес. У той же час швидкість розповсюдження інформації, зокрема і персональної, в Інтернеті є такою, що для захисту порушених прав вкрай необхідним є оперативне реагування. Іноді Офіс Уповноваженого дійсно реагує на порушення досить швидко, проте охопити увагою всі кричущі порушення, на жаль, він не в змозі. Відтак, необхідним є вдосконалення законодавства України з метою підвищення ефективності правового регулювання суспільних взаємовідносин в даній сфері суспільного життя. А саме, внесення необхідних системних змін у статті Конституції України, КК України та інші нормативно-правові акти.

Зокрема, якщо проаналізувати вже існуючі нормативно-правові акти, то можемо побачити, що, за порушення законодавства у сфері захисту персональних даних українське законодавство передбачає штрафи, які цілком можна назвати символічними – до двох тисяч неоподатковуваних мінімумів доходів громадян, тобто 34 тисяч гривень (ст. 188-39 Кодексу про адміністративні правопорушення) [13]. Такі суми є зовсім незначними для великих компаній, а отже – навряд чи можуть бути стримуючим від порушення фактором.

Загальновідомим є факт, що найпоширенішою сферою яка опиняється під серйозною загрозою порушення основоположних прав людини у зв'язку з застосуванням штучного інтелекту є сфера приватного життя, а саме право на приватність. Право на приватність визначено в стаття 12 Загальної декларації прав людини (далі – ЗДПЛ): “Ніхто не може зазнавати безпідставного втручання у його особисте і сімейне життя, безпідставного посягання на недоторканність його житла, тайну його кореспонденції або на його честь і репутацію” [14]; в Європейській Конвенції з прав людини (далі – ЄКПЛ) цьому присвячено статтю 8 “Право на повагу до приватного і сімейного життя” [1]. У ЄКПЛ акцентовано, що сферу захисту обмежено втручанням в приватне життя з боку держави.

В контексті порушення права на приватність, зазвичай говорять про порушення ще двох прав людини – право на свободу висловлення (ст. 19 ЗДПЛ та ст. 10 ЄКПЛ) та право мирних зборів (ст. ЗДПЛ 20 та ст. 11. ЄКПЛ). Людина, яка знає, що за нею можуть слідкувати, скоріш за все буде більш обережною у висловлюваннях та буде брати менш активну участь у громадському житті. Зокрема, право на свободу висловлення порушується через тимчасове або постійне припинення дії акаунтів у соцмережах за допомогою фільтрів, які відслідковують дописи, які штучний інтелект визначає як такі, що порушують права інших людей: несуть загрозу, булінг, дискримінацію за національністю, релігією тощо. В Україні за допомогою Big Data (укр. – “Великі Дані”) та штучного інтелекту неодноразово викривали в такий спосіб великі ботоферми (нешодавній випадок у Фейсбук з ботофермою, що провадила агітаційну підтримку на користь одного з політиків), а також піддавалися реальному кримінальному переслідуванню люди, які в соцмережах закликали до дій, що КК України кваліфіковано як “сепаратизм” та “тероризм”.

Виходячи з відомих на сьогодні випадків використання Великих Даних та взаємозв'язків, що виникають в мережі, до цього списку також можна додати свободу пересування (ст. 13 ЗДПЛ), право володіти майном (ст. 17 ЗДПЛ), право на демократію (ст. 21 ЗДПЛ), а також різні форми дискримінації (ст. 14 ЄКПЛ), які виникають в результаті застосування моделей, що спираються на Big Data та конвергенцію новітніх технологій [15].

На підтвердження вищесказаного можемо навести приклад деяких порушень прав людини. Зокрема, технології, що впроваджено з метою якісного покращення в повсякденний побут людини передбачають такі заходи як збір персональної інформації про користувачів Інтернету. В подальшому використання результатів аналізу цієї інформації для таргетування осіб та груп осіб відповідно до їх уподобань та психологічних особливостей. Внаслідок чого людина піддається в тому числі нав'язливому тиску контекстної реклами, що зокрема відображається й у технології, використовуваній Google Maps, а саме фізичне перебування людини у певний момент часу використовується для того, щоб вчасно надсилати пропозиції з метою вплинути на її вибір при покупці або виборі ресторану, відвідуванні музею тощо [16].

Найяскравішим прикладом обмеження свободи пересування виступає Китай, де запровадження системи соціальних рейтингів, механіка дій яких реалізована в першу чергу на використанні Big Data та штучного інтелекту, призвело до того, що несплата або несвоєчасна сплата аліментів, податків, різних штрафів, скоєння дрібних правопорушень тощо – це все впливає на зниження соціального рейтингу, а поєднання декількох з таких причин призводить до внесення в чорний список, блокування державою реалізації більшості основоположних прав, в тому числі й через заборону доступу до банківських операцій, використання віртуальних грошей, і, як наслідок, люди з чорного списку не можуть купувати квитки на транспорт [17].

Право володіти майном включає в себе право володіння та розпорядження ним в межах закону. Тут доречно згадати ситуації з Apple в 2016 році, яка під час оновлення програмного забезпечення ненавмисно заблокувала значну кількість смартфонів, що ремонтувалися не в авторизованих сервісах компанії. А також електронних пристроїв для читання Kindle (2009), коли з е-книжок Kindle без відома їх володільців зникли раніше завантажені книжки Орвелла через відсутність права інтелектуальної власності видавця, який розмістив їх на платформі. Тому компанія Amazon видалила її, повернувши покупцям гроші [18].

Крім вищезгаданих проблем, слід зазначити також, що вітчизняні науковці починають говорити про штучний інтелект як реальність яку необхідно вичленувати з вже існуючих юридично-правових категорій для вдосконалення можливостей її введення

в правове поле та, відповідно, здійснити її правове регулювання. Так, зокрема, Радутний О.Е. слідом за іншими науковцями зазначає, що необхідно вводити нову категорію, крім фізичної та юридичної осіб, а саме “електронна особа” [19]. Зокрема, розмірковуючи над ознаками суб’єкта злочину, дослідник застерігає, що штучний інтелект за більшістю ознак є схожим на “фізичну особу”. Будуючи свої аргументи, вчений виходить з положень, запропонованих Європейським парламентом. Останній прийняв на розгляд проект Резолюції про правовий статус роботів як “електронної особи” [20]. Проект Резолюції передбачає наділення роботів статусом “електронної особи”, яка має специфічні права та обов’язки. Вказана Резолюція має на меті регулювання правового статусу роботів у суспільстві людей [21]. Дослідник, аналізуючи пояснювальну записку до цієї Резолюції зазначає актуальне положення: “дедалі складніше буде визначати особу (сьогодні це поки що розробник або користувач певного об’єкту робототехніки), яка повинна нести відповідальність за дії з боку штучного інтелекту, наприклад, щодо програмного забезпечення з відкритим початковим кодом (коли його розробниками, або тими, хто його вдосконалює, є невизначена кількість осіб), або відносно штучного інтелекту, який сам себе усвідомлює, наділений здатністю до роздумів про себе та оточуючий світ, самонавчання та самовдосконалення, дбає про власне самозбереження та отримання необхідних ресурсів, має здібності до творчої діяльності, приймає самостійні виважені рішення тощо” [19].

Інші дослідники питань взаємодії особи з штучним інтелектом, аналізуючи дану Резолюцію, приділяють увагу більш конкретним проблемам етики та безпеки. Зокрема, Каткова Т.Г. акцентує увагу на тому, що “Резолюція встановлює загальні етичні принципи розвитку галузі робототехніки і штучного інтелекту для використання в громадянському суспільстві, які мають бути враховані при соціальному, екологічному впливі й впливі на здоров’я людей робототехніки і могли б забезпечити відповідність дій роботів правовим, етичним стандартам і стандартам безпеки. Наприклад, стосовно питань безпеки Резолюція передбачає зобов’язання для розробників роботів інтегрувати в механізм аварійний вимикач з метою їх миттєвого відключення в надзвичайних ситуаціях” [22].

У світі вже створені компанії, які управляються і успішно працюють за допомогою самовиконуваних розумних контрактів (*smart contracts*), без традиційних органів на кшталт генерального директора чи ради директорів. Наприклад, DAO (*Decentralized Autonomous Organizations*) є однією з перших компаній, яка була створена за допомогою контракту-програми, яка регулює прийом криптовалюти, що використовується для фінансування та діяльності організації, а також конвертацію прийнятої криптовалюти в токени (аналог акцій в традиційній компанії) [23]. Тому замість того, щоб розташувати штучний інтелект серед вже відомих категорій (фізичні особи, юридичні особи, тварини, речі та інші суб’єкти та об’єкти), пропонується створення нової категорії “електронних осіб” як більш доцільної [24].

В Україні стрімкого поширення набуває наукова дискусія щодо проблем врегулювання взаємодії людини із штучним інтелектом в контексті подальшого розвитку і розширення методів та засобів такої взаємодії в глобальній мережі Інтернет. Так, в різних сферах науки і практики набуває поширення стале словосполучення “Інтернет речей” (скорочено ІР, англ. – Internet of Things (IoT)). Що розглядається як “мережа різних об’єктів, що розширюється, – від промислових пристроїв до споживацьких товарів, які можуть обмінюватися інформацією і виконувати свої завдання, поки людина працює, спить або займається спортом. Інтернет речей складається з мільйонів датчиків і різних

пристроїв, що генерують безперервні потоки даних, які можна використовувати для поліпшення як життя взагалі, так і для підвищення ефективності бізнесу зокрема” [25].

Як зазначає Гребенюк М., аналізуючи сучасний стан наукових розвідок в даній сфері, українські науковці, зокрема Литвинов Є.П., пропонують шляхи вдосконалення правового регулювання даної сфери шляхом впровадження інноваційної галузі Інтернет-права. Вчений розглядає його як сукупність юридичних норм, які вивчають всесвітній кіберпростір та його особливості [26, с. 158]. Підтримуючи і продовжуючи цю ідею, Л. Мудриєвська наполягає на необхідності прийняти окремий законодавчий акт “Про Інтернет”, з метою впорядкування правових основ використання глобальної мережі, де не тільки були б визначені термінологічні засади діяльності, але й Інтернет розглядався б як багатоманітне явище, а саме як форма діяльності, засіб комунікації, спосіб суспільного життя і свідомості [27, с. 71].

Таким чином Гребенюк М. пропонує визначити що “основними об’єктами, з приводу яких виникають суспільні відносини в кіберпросторі, є: 1) програмно-технічні комплекси, інформаційні системи, інформаційно-телекомунікаційні технології як засіб формування інформаційної інфраструктури, засоби зв’язку і телекомунікацій, що забезпечують здійснення інформаційних процесів (апаратна безпека, безпека додатків та серверів зв’язку); 2) інформація, інформаційні ресурси, інформаційні продукти, інформаційні послуги (контентна безпека); 3) доменні імена; 4) інформаційні права і свободи; 5) інтереси особи, суспільства, держави в кіберпросторі” [25]. І далі виокремлюється “дві основні групи відносин, які пов’язані з Інтернетом: безпосередньо з мережею Інтернет як телекомунікаційною мережею; з використанням мережі Інтернет, Інтернет-технологій для реалізації різних видів діяльності”.

Відтак, виходячи з вищевикладеного, є підстави стверджувати, що на сьогодні в Україні основні принципи захисту прав людини в постіндустріальну, епоху четвертої революції задекларовано, але їх імплементація стикається з багатьма перешкодами. А саме, проблема встановлення юрисдикції. Запровадження системи IP-адрес та геолокації змінило Інтернет і він більше не є світом без кордонів, ці кордони є прозорими для ймовірних порушників. Причинами є те, що поки що відсутні технічні інструменти контролю трафіку: досі не вдосконалено законодавство, яке врегульовувало б інструменти контролю та самі мережі, на яких їх може бути встановлено, оскільки останні здебільшого знаходяться у приватних руках; а також через відсутність технічної можливості заблокувати певну діяльність.

Як приклад, можемо навести ситуацію, коли в умовах збройної агресії Російської Федерації, Україна технічно не в змозі завадити встановленню на смартфони громадянами України мобільного додатку, розробленого російським банком для онлайн платежів. Встановлення ж цього додатку надає доступ його розробнику до приватних даних користувача, що зберігаються в його смартфоні або продукуються ним у процесі користування. Внаслідок чого відбувається порушення права на приватність. Крім того, слід зазначити, що держава часто не має доступу до алгоритмів, які використовуються для обробки даних, якщо це робиться приватними компаніями, оскільки ці алгоритми часто є комерційною таємницею, а їх застосування може призводити до навмисної або ненавмисної дискримінації.

Висновки.

Стрімкий розвиток технологій штучного інтелекту та впровадження їх у різні сфери життєдіяльності людини а також застосування їх як інструментів реалізації владних повноважень окремих державних органів має низку переваг, але водночас і недоліків. Якщо переваги застосування штучного інтелекту очевидні (полягають у підвищенні

ефективності роботи державних структур, можливості швидкої обробки значних за обсягом матеріалів тощо), то недоліки мають прихований характер та пов'язані з можливими ризиками, викликами та загрозами окремим правам і свободам особи.

В Україні одним з найбільш явних порушень у зв'язку з застосуванням технологій штучного інтелекту є порушення права на приватність, зокрема, доступ до баз персональних даних. Проблема захисту прав людини в мережі додатково ускладнюється недовірою громадян до правоохоронної системи.

На нашу думку, застосування сучасних передових технологій штучного інтелекту не повинно суперечити правам людини, громадянським свободам, принципам верховенства права. Важливо усвідомлювати, що принцип верховенства права охоплює не лише змістовний аспект (правових відносин між людиною і державою на засадах визнання людини вищою соціальною цінністю), але й процедурний аспект, який базується на вимогах відповідності правотворчої та правозастосовної практики певним стандартам, як-от: заборона зворотної дії закону, вимога ясності та несуперечності закону; вимога щодо однакового застосування закону; застосування покарання виключно на підставі закону тощо, тобто відповідати практиці ЄСПЛ.

При цьому потрібно враховувати концептуальну правову проблему майбутнього. Традиційна правова доктрина стверджує, що правові норми регулюють суспільні відносини між людьми. Але на сучасному етапі правова наука в Україні не готова надати відповідь про те, яким чином будуть регулювати суспільні відносини, що пов'язані з штучним інтелектом.

Вищевказані проблеми дозволяють говорити про те, що на сьогодні Україна здійснює недостатній контроль за порушеннями в сфері витоку інформації та інших сферах взаємодії із штучним інтелектом. На нашу думку, це пов'язано з тим, що законодавство не встигає за розвитком цієї сфери, оскільки багато злочинів, передбачених в ЄС, в Україні залишаються нечітко артикульованими, а отже, не врегульованими.

У зв'язку з цим, з метою недопущення порушення фундаментальних прав людини, які зазначені у Конвенції про захист прав людини і основоположних свобод, безконтрольного розвитку та використання штучного інтелекту у суспільстві, державні органи, на які покладено законотворчий процес, мають розробити проекти законів та інших нормативно-правових актів, що стосуються прав і свобод людини, які пов'язані із використанням штучного інтелекту. Уряд держави має забезпечувати підготовку відповідних документів та представляти інтереси держави в ЄСПЛ під час розгляду справ про порушення прав людини в Україні задля дотримання прав і свобод людини і громадянина.

Використана література

1. Про захист прав людини і основоположних свобод: Конвенція РЄ від 1950 р.: Закон України від 17.07.97 р. № 475/97-ВР. URL: https://zakon.rada.gov.ua/laws/show/995_004#Text (дата звернення: 9.10.2020).

2. Бостром Н. *Искусственный интеллект. Этапы. Угрозы. Стратегии*. Москва: Манн, Иванов и Фербер. 2016. 496 с.

3. База даних EUR-Lex. URL: <https://eur-lex.europa.eu/homepage.html> (дата звернення: 5.11.2020).

4. Convention on Cybercrime. Budapest, 23.XI.2001. URL: <https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=0900001680081561> (дата звернення: 9.10.2020).

5. Сучасні правові стандарти Євросоюзу у сфері захисту персональних даних: / І. Майстренко – перекл. з англ.; В. Брижко – перекл. та редагування тексту. – (Науково-дослідний інститут інформатики і права Національної академії правових наук України). Київ: ТОВ “Видавничий дім “АртЕк”, 2018. 177 с.

What is the GDPR? The EU’s new data protection law. URL: <https://gdpr.eu/what-is-gdpr> (дата звернення: 09.10.2020).

6. Про проведення публічного громадського обговорення проєкту розпорядження Кабінету Міністрів України “Про схвалення Концепції розвитку штучного інтелекту в Україні”: – (повідомлення). URL: https://thedigital.gov.ua/regulations/povidomlennya-pro-provedennya-publichnogo-gromadskogo-obgovorennya-proyektu-rozporyadzhennya-kabinetu-ministriv-ukrayini-pro-shvalennya-konceptsiyi-rozvitku-shtuchnogo-intelektu-v-ukrayini?fbclid=IwAR1HLjfo5WtmAnNboi7HVksyvlO069tKFH6__SfPBdci_sXRfolKqWUsGi0 (дата звернення: 19.06.2020)

7. Міністерство цифрової трансформації України розробило концепцію розвитку сфери штучного інтелекту, яка посприяє просуванню таких технологій в Україні та їх інтеграції в основні галузі. URL: <https://deps.ua/ua/news/novosti-rynka/8118.html> (дата звернення: 19.06.2020).

8. Воронков О. Чи буде безпечною Україна в смартфоні. Чотири кроки захисту даних. URL: <https://nv.ua/ukr/biz/experts/bezpeka-danih-ukrajinciv-derzhava-v-smartfoni-yak-ce-bude-pracyuvati-50049227.html> (дата звернення: 17.09.2020).

9. Кримінальний кодекс України: Закон України від 05.04.01 р. № 2341-III. (ред. від 25.09.20). URL: <https://zakon.rada.gov.ua/laws/show/2341-14#Text> (дата звернення: 19.09.2020).

10. Захист особистих та персональних даних в Інтернеті: проблеми законодавчого врегулювання. URL: https://ukrainepravo.com/scientific-thought/legal_analyst/zakhist-osobistikh-ta-personalnikh-danikh-v-interneti-problemi-zakonodavchogo-vregulyuvannya/?fbc (дата звернення: 19.10.2020).

11. Про захист персональних даних: Закон України від 01.06.10 р. № 2297-VI. URL: <https://zakon.rada.gov.ua/laws/show/2297-17#Text> (дата звернення: 19.09.20).

12. Правдиченко А. Персональні дані онлайн: проблеми регулювання та перспективи захисту. URL: <https://cedem.org.ua/articles/personalni-dani-onlajn> (дата звернення: 19.06.2020).

13. Кодекс України про адміністративні правопорушення: Закон України від 07.12.84 р. № 8073-X. (редакція від 13.08.20). URL: <https://zakon.rada.gov.ua/laws/show/80731-10#Text> (дата звернення: 19.06.2020).

14. Загальна декларація прав людини URL: https://zakon.rada.gov.ua/laws/show/995_015?lang=uk#Text (дата звернення: 5.11.2020).

15. Брижко В.М. Конвергенція новітніх технологій: стан і перспективи змін у інформаційних відносинах / Брижко В.М., Фурашев В.Н. *Інформація і право*. № 1(20)/2017. С. 51-67.

16. Hill, Thomas “How to Target Customers With Location-Based Marketing”. 26 June 2018. URL: <https://business.tutsplus.com/tutorials/how-to-target-customers-with-location-based-marketing--cms-21507> (дата звернення: 5.11.2020).

17. Zhong, Rui “In China, social credit is just a more invasive form of social media”. 31 October 2019. URL: <https://www.codastory.com/authoritarian-tech/china-social-credit> (дата звернення: 13.11.2020).

18. Stone, Brad “Amazon Erases Orwell Books From Kindle”, July 17, 2009. URL: <https://www.nytimes.com/2009/07/18/technology/companies/18amazon.html> (дата звернення: 05.11.2020).

19. Радутний О.Е. Штучний інтелект як суб’єкт злочину. *Інформація і право*. № 4(23)/2017. С. 106-115.

20. Wakefield J. MEPs vote on robots’ legal status – and if a kill switch is required. URL: <http://www.bbc.com/news/technology-38583360> (дата звернення: 19.06.2020).

21. Коваль М. Электронная личность: зачем ЕС обсуждает права роботов. URL: <http://www.eurointegration.com.ua/rus/experts/2017/01/24/7060539> (дата звернення: 05.11.2020).

22. Каткова Т.Г. Законы про роботов: сучасний стан та перспективи розвитку. *IT-право: проблеми та перспективи розвитку в Україні*: зб. матеріалів II Міжнародної науково-практичної конференції, м. Львів, 17 лист. 2017 р. Львів. 2017. С. 99-105.

23. Вашкевич А. Електронна особа. URL: <https://zbruc.eu/node/51750> (дата звернення: 11.11.2020).

24. Хель И. Права роботов: когда разумную машину можно считать “личностью”. URL: <https://hi-news.ru/robots/prava-robotov-kogda-razumnuyu-mashinu-mozhno-schitat-lichnostyu.html> (дата звернення: 11.11.2020).

25. Гребенюк М. Проблеми правового регулювання застосування технологій ІОТ. *Інтернет речей: проблеми правового регулювання та впровадження*. 2019. С. 48.

26. Литвинов Є.П. Місце Інтернет-права в системі права та в системі юридичних наук *Адміністративне право і процес*. 2013. № 4(6). С. 155-162.

27. Мудриєвська Л.М. Правове регулювання діяльності Інтернету та його значення у формуванні інформаційного суспільства в Україні. *Актуальні проблеми вітчизняної юриспруденції*. 2013. № 4. С. 63-71.

~~~~~ \* \* \* ~~~~~

---