УДК 34:004.8
DOI https://doi.org/10.32782/2524-0374/2022-12/68

ПРАВОВІ АСПЕКТИ ЗАХИСТУ ПРИВАТНОСТІ ЖИТТЯ ЛЮДИНИ В КОНТЕКСТІ ВИКОРИСТАННЯ ШТУЧНОГО ІНТЕЛЕКТУ

LEGAL ASPECTS OF HUMAN PRIVACY PROTECTION IN THE CONTEXT OF THE USE OF ARTIFICIAL INTELLIGENCE

Кронівець Т.М., к.ю.н.,
завідувач кафедри фундаментальних і приватно-правових дисциплін
Вінницький державний педагогічний університет імені Михайла Коцюбинського

Тимошенко Є.А., асистентка кафедри права
Вінницький національний аграрний університет
аспірантка
Державна наукова установа «Інститут інформації, безпеки і права Національної академії правових наук України»

У статті аналізуються актуальні проблеми захисту приватності життя людини в контексті використання штучного інтелекту (далі – ШІ) Здійснено спробу комплексного аналізу впливу штучного інтелекту на захист персональних даних. Здійснено аналіз поточного стану нормативно-правового регулювання правовідносин, пов'язаних з використанням штучного інтелекту в Україні, а саме Закон України «Про інформацію», Закон України «Про захист персональних даних», визначено прогалини правового регулювання.

У зв'язку з розширенням сфери застосування штучного інтелекту, виникла низка загроз щодо розповсюдження, незаконної обробки та збору інформації, яка може бути конфінденційною.

Обсяг даних у мережі щодня збільшується. Закон Мура говорить нам, що інформація збільшується вдвоє кожні 2 роки, про що свідчить інформаційний вибух, який стався за останні 50 років. Інформації стає все більше, вона різноманітна та переміщається все більш швидше. Швидкість передачі інформації полегшує її збір та обробку, завдяки чому пришвидшується її аналіз та створення нових алгоритмів. Потоки даних із наших мобільних телефонів та інших підключених до мережі пристроїв розширюють обсяг і різноманітність інформації про кожен аспект нашого життя та виставляють конфіденційність у центр уваги як проблему глобальної державної політики.

Штучний інтелект прискорює цю тенденцію. Більшість сучасного аналізу даних, які є найбільш чутливими до конфіденційності, як-от алгоритми пошуку, механізми рекомендацій і мережі рекламних технологій, керуються машинним навчанням і прописаними алгоритмами. У міру розвитку штучного інтелекту він розширює можливості використання особистої інформації у спосіб, який може порушити інтереси конфіденційності, підвищуючи потужність і швидкість аналізу особистої інформації.

Ключові слова: штучний інтелект, захист персональних даних, конфіденційна інформація, персональні дані.

The article analyzes the actual problems of protecting the privacy of human life in the context of the use of artificial intelligence (hereinafter – AI). An attempt was made to comprehensively analyze the impact of artificial intelligence on the protection of personal data. An analysis of the current state of legal regulation of legal relations related to the use of artificial intelligence in Ukraine, namely the Law of Ukraine "On Information", the Law of Ukraine "On Protection of Personal Data", identified gaps in legal regulation.

In connection with the expansion of the scope of application of artificial intelligence, a number of threats have arisen regarding the distribution, illegal processing and collection of information that may be confidential.

The amount of data on the network is increasing every day. Moore's Law tells us that information doubles every 2 years, the amount of information explosion that has occurred in the last 50 years. Information is becoming more and more diverse and moving faster. The speed of information transmission facilitates its collection and processing, thanks to its analysis and the creation of new algorithms. Data streams from our mobile phones and other networked devices are expanding the volume and variety of information about every aspect of our lives and bringing privacy into the spotlight as a global public policy issue.

Artificial intelligence is accelerating this trend. Most of today's most privacy-sensitive data analytics, such as search algorithms, recommendation engines, and ad networks, are driven by machine learning and prescriptive algorithms. As artificial intelligence advances, it expands the ability to use personal information in ways that may violate privacy interests by increasing the power and speed of analysis of personal information.

Key words: artificial intelligence, personal data protection, confidential information, personal data.

Застосування технології штучного інтелекту в реальному світі вже є частиною нашого повсякденного життя, але багато людей про це не підозрюють. Однією з особливостей штучного інтелекту є те, що як тільки ця технологія починає активно використовуватись, вона більше не називається штучним інтелектом, а стає звичайним обчисленням та виведенням алгоритмів. Ці системи ШІ стають частиною нашого життя, такі як розпізнавання мовлення, обробка природної мови та прогнозна аналітика.

Штучний інтелект може багатьма способами збагатити наше життя. Підвищення ефективності та зниження витрат, значно покращене охорона здоров'я та дослідження, підвищена безпека транспортних засобів і загальна зручність – це лише деякі з обіцянок ШІ. Однак, як і будь-яка нова технологія, перспективи штучного інтелекту пов'язані з багатьма проблемами для суспільства та законодавства.

Нові технології майже завжди приносять із собою важливі міркування щодо конфіденційності, але масштаб і застосування ШІ створює унікальне та безпрецедентне середовище викликів. У певному сенсі наслідки штучного інтелекту можна розглядати як розширення тих, які створюють великі дані, але технологія штучного інтелекту приносить із собою не лише можливість обробляти величезні обсяги даних, але й використовувати їх для навчання, розробки адаптивних моделей і робити дієві прогнози – багато з цього без прозорих, зрозумілих процесів.

Розвиток технології штучного інтелекту несе в собі значний ризик того, що припущення та упередження осіб і компаній, які її створюють, впливають на результати ШІ. Непередбачені наслідки, спричинені упередженнями та непрозорими результатами використання нейронних мереж, створюють проблеми для урядових організацій, які бажають використовувати цю технологію для прийняття рішень. Існує можливість дискримінації та «грою» конфіденційними даними.

Ключовим моментом відмінності між ШІ та існуючими технологіями аналітики є потенціал автоматизації всіх цих сфер. Там, де люди історично мали змогу здійснювати максимальний контроль над обробкою даних, збільшення використання штучного інтелекту означає, що цього

більше не буде. Крім того, застосування штучного інтелекту до існуючих технологій суттєво змінить їх поточне використання та міркування конфіденційності. Наприклад, використання камер відеоспостереження в громадських місцях є відносно поширеною практикою, яка вважається виправданою в сучасному суспільстві, особливо в концепції «Смарт сіті» [7]. Однак у поєднанні з використанням програмного забезпечення для розпізнавання обличь мережу камер можна перетворити на інструмент, який набагато більше порушує конфіденційність. Саме через це у багатьох штатах Америки використання технології розпізнавання заборонено, навіть з міркувань безпеки.

ШІ також може змінити спосіб взаємодії людей із машинами. Наприклад, багато ШІ вже втілюють людські риси. Використання антропоморфних інтерфейсів, таких як людські голоси, що використовуються в таких помічниках, як Alexa та Siri, може викликати нові проблеми конфіденційності. Соціологічні дослідження вказують на те, що люди схильні взаємодіяти з технологіями так, ніби це люди. Це означає, що люди, швидше за все, розвиватимуть довірливі стосунки з ШІ, створеним для повторення людських характеристик, і, отже, будуть більш схильні ділитися все більш особистою інформацією порівняно з інші форми технології, які збирають інформацію традиційним способом.

Сучасна доктрина загалом розглядає будь-які дані як товар, яким можна торгувати, що не повністю визнає що у фізичних осіб існують труднощі із прийняттям рішень відносно їхніх даних, в справах з системами штучного інтелекту, якого вони не розуміють. Але водночас ШІ їх добре розуміє та навчилася, за допомогою прийому їхніх даних, як маніпулювати їхніми уподобаннями. Крім того, багато адаптивних алгоритмів, які використовуються в штучному інтелекті, постійно змінюються до такої міри, що часто ті, хто їх створює, не можуть повністю пояснити результати, які вони генерують – машинне навчання.

Загальноприйняті уявлення про конфіденційність інформації базуються на ідеї, що люди є основними обробниками інформації і не створені для боротьби з обчислювальними можливостями ШІ, які не відповідають традиційним уявленням про збір і обробку даних. Те, як ми зараз думаємо про такі поняття, як інформована згода, повідомлення, а також те, що означає доступ до особистої інформації або контроль за нею, ніколи раніше не піддавалися такому фундаментальному виклику, як тепер в часи ШІ [1].

Варто розпочати із визначення конфіденційної інформації. В Законі України «Про доступ до публічної інформації» зазначено, що конфіденційною є інформація, доступ до якої обмежено фізичною або юридичною особою, крім суб'єктів владних повноважень, та яка може поширюватися у визначеному ними порядку за їхнім бажанням відповідно до передбачених ними умов. Закон «Про інформацію» має своє визначення, а саме: «конфіденційною є інформація про фізичну особу, а також інформація, доступ до якої обмежено фізичною або юридичною особою, крім суб'єктів владних повноважень. Конфіденційна інформація може поширюватися за бажанням (згодою) відповідної особи у визначеному нею порядку відповідно до передбачених нею умов, а також в інших випадках, визначених законом».

Отже, порівнюючи ці дві дефініції, можемо казати, що лише фізична особа може визначати відносно себе, які її дані є конфіденційними, а які ні. Водночас, в українському законодавстві прописані види даних які є конфіденційними за замовчуванням – дані про здоров'я, національність, освіту, сімейний стан, релігійні переконання, адреса, дата та місце її народження [6]; первинні дані, отримані органами державної статистики від респондентів під час проведення статистичних спостережень, а також адміністративні дані щодо респондентів, отримані органами державної статистики від органів, що займаються діяльністю, пов'язаною із збиранням та використанням адміністративних даних [4].

Важливо також згадати і про термін персональні дані, який часто ототожнюють з конфіденційною інформацією про особу. Персональні дані – це відомості чи сукупність відомостей про фізичну особу, яка ідентифікована або може бути конкретно ідентифікована [5]. Проте у цьому Законі прямо не сказано, що вся інформація про особу – це її персональні дані. Але не всі дані про особу захищаються законом. Зокрема у Регламенті Європейського Парламенту і Ради (ЄС) 2016/679 зазначається, що принцип захисту даних не застосовується до даних про фізичну особу, за допомогою яких її неможливо ідентифікувати, або якщо такі дані були депресоналізовані(анонімні), то вони не підлягають захисту.

Конфіденційна інформація про особу, її персональні дані можуть поширюватись лише якщо ця особа надала свою згоду на поширення або самостійно поширила її серед необмеженого кола осіб, наприклад, розповіла про певні факти свого життя в прямому ефірі, опублікувала щось у соціальних мережах у відкритому доступі. Але є виключення, за частиною 2 статті 14 Закону України «Про захист персональних даних», поширення персональних даних без згоди суб'єкта персональних даних або уповноваженої ним особи дозволяється у випадках, визначених законом, і лише (якщо це необхідно) в інтересах національної безпеки, економічного добробуту та прав людини. До прикладу, поширення інформації про особу в межах кримінального провадження з метою розшуку цієї особи.

Отже, концепція персональних даних спирається на ідею ідентифікації – чи можна обґрунтовано встановити особу особи за цією інформацією. Однак розрізнення між тим, що вважається «особистим», і тим, що не вважається «особистим», заперечується здатністю пов'язувати та зіставляти дані з окремими особами, навіть якщо вони раніше вважалися «деперсоналізованими» або не ідентифікаційним. У цьому сенсі комбінація, здавалося б, неособистої інформації може стати особистою під час аналізу або співвідношення. Зі збільшенням обсягу доступних даних і вдосконаленням технологій їх обробки та об'єднання стає все важче оцінити, чи є дана частина даних «ідентифікованою»; розгляд частини даних окремо не сумісний із технологією штучного інтелекту та більше не є справжнім відображенням того, чи можна вважати її «особистою інформацією».

Велика частина цінності штучного інтелекту полягає в його здатності ідентифікувати моделі, невидимі людському оку, навчатися та робити прогнози щодо окремих людей і груп. У цьому сенсі ШІ може створювати інформацію, яку інакше важко зібрати або яка ще не існує. Це означає, що зібрана та використана інформація може виходити за межі того, що спочатку було свідомо розкрито особою. Частина перспектив передбачуваних технологій полягає в тому, що висновки можна робити з інших (здавалося б, непов'язаних і нешкідливих) фрагментів даних. Наприклад, система штучного інтелекту, розроблена для підвищення ефективності процесу найму, може мати можливість зробити висновок про політичні переконання кандидата з іншої наданої ним інформації, а потім включити її в процес прийняття рішень.

Виведення інформації таким чином не тільки ставить під сумнів те, що вважається особистою інформацією, але також викликає питання про те, чи прийнятно виводити особисту інформацію про особу, яка вирішила не розголошувати її. Також піднімаються інші питання, наприклад, кому належить ця інформація та чи підпадає вона під принципи конфіденційності інформації, включаючи вимогу інформувати цю особу про те, що інформацію про неї було зібрано шляхом висновку.

У цій ситуації визначення того, що захищено законом про конфіденційність, а що ні, відповідно до визначення особистої інформації, навряд чи буде технічно чи юридично практичним, або хоча б корисним як ефективний спосіб захисту конфіденційності (або анонімності) осіб.

Деякі науковці стверджують, що необхідно відійти від подвійного розуміння особистої інформації, щоб Закон «Про захист персональних даних» [4] продовжував захищати конфіденційність інформації осіб у середовищі ШІ.

Але чи завжди ми дійсно надаємо згоду на всі маніпуляції, які штучний інтелект за допомогою алгоритмів та аналізу може застосовувати до наших персональних даних, а в деяких випадках і до конфіденційних? За вимогою законодавства про захист персональних даних, фізична особа майже у всіх установах, в соціальних мережах, у додатках, сайтах де вона залишає хоч якісь відомості про себе підписує згоду на обробку персональних даних. Але чи уважно ви читаєте цей текст? Деякі вчені називають це явище, принципом «повідомлення та згоди». Споживачі послуг стикаються з таким підходом у безлічі повідомлень і банерів на сайті чи додатку, пов'язаних із довгою та неінформативною політикою конфіденційності та умовами, з якими ми нібито погоджуємося, але рідко читаємо. Цей принцип зводить нанівець весь сенс цієї згоди. Адже саме там прописується що компанія може робити та як використовувати ваші персональні дані, які ви заповнили для, наприклад, реєстрації на сайті.

Аналізуючи нормативно-правові акти українського законодавства, можна дійти висновку, 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.188-39Кодексупроадміністративніправопорушення)[3].

Також, у зв'язку з використанням штучного інтелекту при доступі до персональних даних, виникає і проблема з порушенням приватності життя. Згідно з Європейською конвенцією з прав людини, вказано що держава не може втручатись до приватного життя людини. Загальна декларація з прав людини закріплює, що «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» [2]. В контексті порушення права на приватність, зазвичай говорять про порушення ще двох прав людини – право на свободу висловлення та право мирних зборів [8]. До прикладу, право на свободу висловлення може порушуватись через тимчасове або постійне припинення дії акаунтів у соцмережах за допомогою фільтрів систем штучного інтелекту, які відслідковують дописи, які визначаються як такі, що порушують права інших людей: несуть загрозу, булінг, дискримінацію за національністю, релігією тощо. Доволі поширений приклад сьогодні, в умовах війни, це застосування ботоферм, які пишуть алгоритмнічний тексти на фальшивих акаунтах чи в коментарях звичайних людей, задля розпалу ворожнечі, дезінформації та закликів до терористичних дій. Саме за допомогою фільтрів із штучним інтелектом вдається заблокувати такі акаунти та запобігти розповсюдженню неправдивої інформації. Варто зазначити, що і без автоматизованих алгоритмів штучного інтелекту можна було б аналізувати такі дані і виявляти злочинні наміри порушників, але це б зайняло набагато більше часу та завдяки похибці на людський фактор не давало б такого високого результату.

У **висновках** ми можемо зазначити проблеми щодо штучного інтелекту та приватності життя особи:

1. Визначення того, кому належать дані, чи є вони персоніфіковані і чи підлягають законодавству про захист персональних даних та хто несе за них відповідальність, є складним завданням.
2. Ефективне управління має базуватися на розумінні технології. Оскільки штучний інтелект продовжує швидко розвиватися, розрив між законодавством і технологіями штучного інтелекту збільшується, а складність правового регулювання ШІ продовжує зростати. Застосування сучасних технологій ШІ не повинно суперечити правам та свободам людини та принципу верховенства права.
3. Регулювання конфіденційності та захисту приватності в контексті використання штучного інтелекту не відбувається в межах однієї держави чи юрисдикції. Адже Інтернет речей не має кордонів, як і соціальні мережі чи сайти в інтернеті, ними користуються, з них беруть і обробляють дані люди з усього світу, тож і законодавство має бути загальним щодо регулювання цього питання.

Держава відіграє важливу роль у створенні середовища, в якому зобов'язання щодо розробки безпечного та справедливого штучного інтелекту мають бути збалансовані з технологічним прогресом та правом. Правильний баланс вимагає консультативного, міждисциплінарного підходу, оскільки надмірне, неналежне чи неправильне регулювання може сповільнити впровадження штучного інтелекту або не в змозі вирішити його справжні виклики. Використання існуючих структур конфіденційності інформації, а також переосмислення традиційних концепцій стане ключовим компонентом у створенні, використанні та регулюванні ШІ.

ЛІТЕРАТУРА

1. Artificial Intelligence and Privacy – Issues and Challenges. URL: https://ovic.vic.gov.au/privacy/resources-for-organisations/artificial-intelligence-and-privacy-issues-and-challenges/#conclusion (дата звернення 20.12.2022р.).
2. Загальна декларація прав людини. URL: https://zakon.rada.gov.ua/laws/show/995_015? lang=uk#Text (дата звернення 27.12.2022р.).
3. Кодекс України про адміністративні правопорушення : Закон України від 07.12.84 р. № 8073-X. URL: https://zakon.rada.gov.ua/laws/show/80731-10#Text (дата звернення: 27.12.2022).
4. Про державну статистику : Закон України від 17.09.1992 № 2614-XII / Верховна рада України. URL: https://zakon.rada.gov.ua/laws/show/2614-12#Text (дата звернення 21.12.2022 р.).
5. Про захист персональних даних : Закон України від 01.06.2010 № 2297-VI / Верховна рада України. URL: https://zakon.rada.gov.ua/laws/show/2297-17#Text (дата звернення 21.12.2022 р.).
6. Про інформацію : Закон України від 02.10.1992 № 2657-XII / Верховна рада України. URL: https://zakon.rada.gov.ua/laws/show/2657-12#Text (дата звернення 21.12.2022 р.).
7. Долян І.В., Тимошенко Є.А. Правове регулювання використання систем штучного інтелекту в смарт сіті. *Юридичний науковий електронний журнал*. 2021.№ 11. С. 525–528.
8. Косілова О.І. Солодовнікова Х.К. Права і свободи людини і громадянина V.S. штічний інтелект : проблемні аспекти. *Інформація і право*. № 4(35)/2020. С. 56–66.