2025

Impactul utilizării AI asupra protecției datelor cu caracter personal

Formator: OPRITA FLORIN ALEXANDRU

ASOCIATIA ELOAH CRAIOVA

Introducere

Mulți oameni consideră Inteligența Artificială (**AI**) un concept complex și dificil de înțeles.

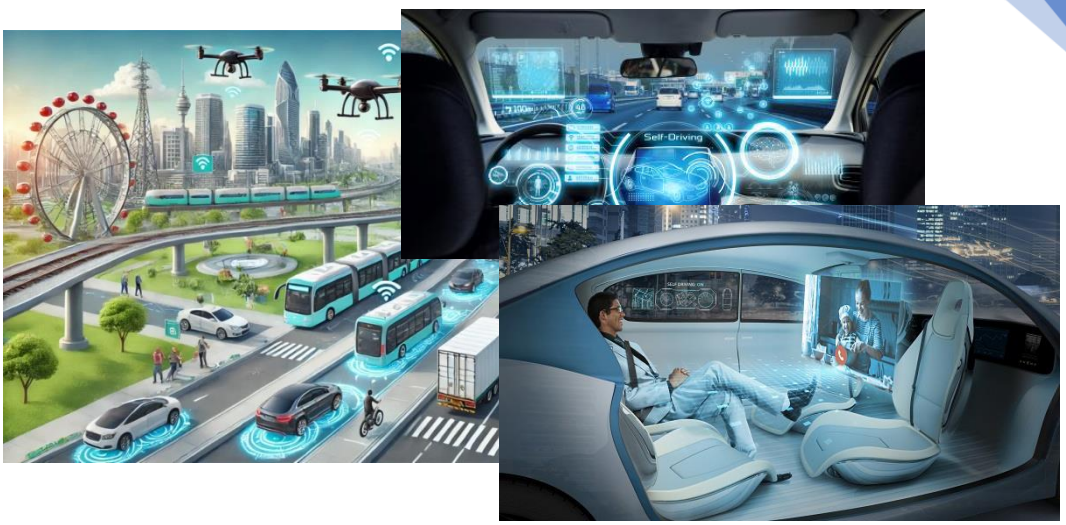
Inteligența artificială a devenit una dintre cele mai discutate tehnologii în ultimii ani, iar utilizarea sa în procesarea datelor personale a devenit tot mai frecventă.

Inteligența artificială este o ramură a informaticii axată pe dezvoltarea de sisteme care reproduc funcțiile cognitive umane - cum ar fi învățarea, rezolvarea problemelor și luarea deciziilor - permițând mașinilor să analizeze date, să recunoască modele și să ia decizii autonome, stimulând inovarea în diverse industrii.

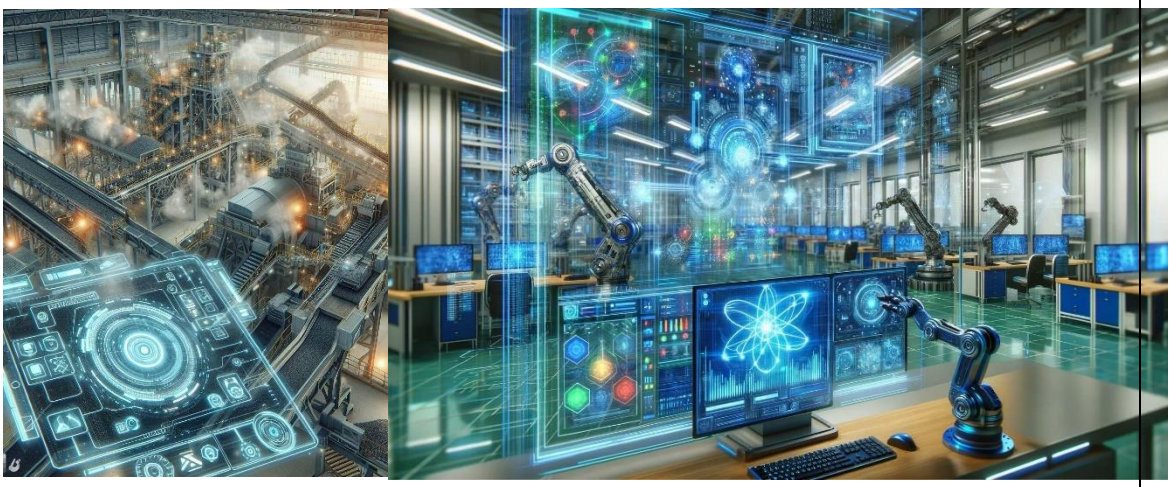
Inteligența artificială a evoluat rapid în ultimii ani, aducând numeroase beneficii în diverse domenii precum:

-sănătate;

-transport;



-industrie.



Principalele domenii de aplicare ale inteligenței artificiale sunt:

- **Învățarea automată (Machine Learning)** – capacitatea mașinilor de a învăța din date și de a lua decizii fără intervenția umană;
- **Rețele neurale artificiale (Artificial Neural Networks)** – sisteme informatice inspirate din funcționarea creierului uman, folosite pentru recunoașterea modelor și a pattern-urilor în date;
- **Prelucrarea limbajului natural (Natural Language Processing)** – capacitatea mașinilor de a interpreta și genera limbaj uman;
- **Viziunea artificială (Computer Vision)** – capacitatea mașinilor de a înțelege și interpreta informațiile vizuale, precum obiecte sau scene.

Pentru a profita de beneficiile **AI**, nu este nevoie să fii expert în domeniu. Există numeroase resurse online, cursuri și platforme care te pot ajuta să îți însușești cunoștințele de bază în acest domeniu fascinant. De asemenea, poți experimenta cu diverse aplicații și tool-uri de **AI** disponibile pe internet, pentru a-ți dezvolta abilitățile practice.

Este important să fim conștienți de impactul pe care **AI** îl are în societate și să ne asigurăm că aceasta este folosită în mod responsabil și etic. Dezbaterile cu privire la reglementările și standardele în domeniu sunt tot mai intense, iar conștientizarea asupra importanței unei dezvoltări sustenabile a **AI** este din ce în ce mai mare.

Pe măsură ce inteligența artificială devine tot mai sofisticată, având capacitatea de a analiza seturi mari de date cu eficiență și precizie, se naște și întrebarea:"Cum ține regulamentul GDPR pasul cu evoluția rapidă a acestei tehnologii?"

La începutul lunii iunie 2023, a avut loc, la Lyon, ENISA Annual Privacy Forum, unde Supervizorul European al Protecției Datelor, Wojciech Wiewiórowski, a adus în discuție dezvoltarea fulminantă a inteligenței artificiale și efectele acestei tehnologii pe termen scurt și mediu asupra confidențialității datelor. Potrivit acestuia, *„ar fi aproape imposibil să discutăm despre confidențialitate în 2023 fără a lua în considerare efectele pe care Inteligența Artificială le are și le va avea în protecția datelor și confidențialitate."*

Acces limitat la inteligența artificială?

Accesul neîngrădit la tehnologia de ultimă oră dă naștere unor întrebări la care ar trebui să găsim răspunsul rapid:*„Ar trebui limitat accesul la AI? În ce condiții?"*

Comisia Europeană consideră că ar trebui inclusă o secțiune referitoare la cazurile în care ar trebui interzisă folosirea AI. Printre aceste interdicții se numără utilizarea inteligenței artificiale pentru exploatarea vulnerabilităților unor anumite grupuri de persoane precum cele cu dizabilități fizice sau mentale.

Wojciech Wiewiórowski afirmă că *„pentru a prospera, inteligența artificială trebuie să depășească mai multe provocări legate de aspecte legale, etice și sociale. Este evident că*

sistemele AI trebuie să respecte legislația existentă. Cu toate acestea, având în vedere implementarea lor largă și impactul lor profund, acestea trebuie să se comporte și în conformitate cu standardele etice convenite de societate. Sistemele AI trebuie, de asemenea, să fie percepute de societate ca fiind de încredere și benefice, altfel vor întâmpina o rezistență puternică."

Schimbările au fost mereu percepute cu reticență pentru că aceasta este natura noastră umană, dar fără a ne adapta la schimbare, nu putem evolua. Nu există tehnologie nouă a cărei efecte să fie doar pozitive, dar le putem anticipa pe cele negative prin crearea unor cadre standardizate pentru efectuarea evaluărilor de risc ale sistemelor de AI. Până în prezent crearea acestor standarde și aplicarea lor la scară largă a fost dificil de corelat. Liderii G7 au solicitat dezvoltarea și adoptarea unor standarde tehnice internaționale pentru o AI *„de încredere"* și este o solicitare pertinentă, având în vedere că până acum, obiectivul principal al AI a fost înțelegerea și generarea unui limbaj similar celui uman, corectitudinea din punct de vedere sintetic și semantic, mai degrabă decât acuratețea informațiilor.

În acest context, provocarea va fi găsirea informațiilor de calitate, a informațiilor reale și discernerea între informațiile adevărate și cele false.

Transparența & dreptul la proprietate intelectuală

Transparența pare să nu fie punctul forte pentru Chat GPT sau BARD, cele două companii, OpenAI și Google punând mare accent pe drepturile de proprietate intelectuală, însă cele două drepturi nu ar trebui să se excludă, ci să se completeze.

Supervizorul European al Protecției Datelor scoate în evidență următorul aspect: *„Sistemele de genul modelelor lingvistice mari care pot să se dea drept ființe umane trebuie să fie transparente în ceea ce privește natura lor ca sisteme de inteligență artificială. Aceasta este una dintre cerințele stabilite în propunerea de Reglementare a Inteligenței Artificiale și cred că are mult sens."*

Wojciech Wiewiórowski crede că dezvoltarea sistemelor de inteligență artificială explicative (Explainable AI) ar fi următorul pas logic în dezvoltarea inteligenței artificiale:*„Cred că în curând multe dintre eforturile în acest domeniu al inteligenței artificiale se vor dedica capacității de a explica de ce un sistem de inteligență artificială generativ a creat sau a ales un anumit răspuns din multele posibile"*.

INTELIGENȚA ARTIFICIALĂ NU ARE CONȘTIINȚĂ PROPRIE

Este de reținut însă un aspect foarte important, care încă nu este înțeles de mulți oameni: Inteligența Artificială **NU ARE CONȘTIINȚĂ PROPRIE (cel puțin deocamdată).**

Termenul „conștiință" implică capacitatea de a avea senzații, percepții subiective și conștientizarea sinelui, ceea ce este distinct de procesarea informațiilor și luarea deciziilor pe care o poate realiza o AI.

AI funcționează pe baza algoritmilor, modelelor matematice și datelor de intrare, procesând informații și generând rezultate în funcție de setările și parametrii programării. Deși AI poate realiza sarcini complexe și poate învăța din experiență, nu posedă în mod intrinsec conștiință sau înțelegere subiectivă a lumii înconjurătoare.

Există o diferență semnificativă între inteligența artificială, care poate simula inteligența și procesele cognitive umane și conștiința umană, care implică aspecte subiective, emoționale și experiența personală. Conceptul de conștiință este încă un subiect intens dezbătut în domeniul științelor cognitive și filozofiei, iar crearea unei conștiințe artificiale ar ridica numeroase probleme etice și filozofice.

Până în prezent, AI nu are conștiință în sensul în care oamenii o înțeleg și dezvoltarea unei asemenea conștiințe artificiale este o provocare considerabilă și o direcție de cercetare controversată.

În concluzie, **AI** reprezintă o provocare și o oportunitate în același timp. Cu o înțelegere clară a conceptelor de bază și cu o abordare responsabilă, oricine poate să exploreze lumea fascinantă a inteligenței artificiale și să contribuie la evoluția acesteia în mod pozitiv.

Riscuri asociate cu folosirea inteligenței artificiale

Utilizarea inteligenței artificiale în procesarea datelor personale vine cu o serie de **riscuri și probleme de protecție a datelor**.

Scopul acestui curs este să ofere o mai bună înțelegere a modului în care inteligența artificială poate afecta datele personale, precum și să evidențieze riscurile implicate de utilizarea acesteia și măsurile care pot fi luate pentru a minimiza aceste riscuri.

În privința riscurilor asociate cu utilizarea inteligenței artificiale în contextul protecției datelor cu caracter personal, trebuie avute în vedere mai multe aspecte.

Unul dintre acestea este **discriminarea**, care poate să apară atunci când algoritmii de inteligență artificială sunt instruiți să ia decizii pe baza datelor istorice generate de sisteme discriminatorii. Aceasta poate duce la **discriminarea unor grupuri vulnerabile**, cum ar fi persoanele în vârstă sau cele aparținând unor grupuri etnice sau rasiale.

Un alt risc important este **profilarea**, care apare atunci când datele personale sunt colectate și utilizate pentru a crea profiluri detaliate ale utilizatorilor. Aceste profiluri pot fi folosite pentru a lua decizii automate în privința serviciilor și produselor oferite, dar și în alte scopuri, cum ar fi analiza riscului sau detectarea fraudelor.

O altă problemă este reprezentată de **lipsa de responsabilitate și transparență a sistemelor de inteligență artificială**, care pot fi greu de controlat și monitorizat. Aceasta poate conduce la o lipsă de încredere în sistem și poate face ca utilizatorii să fie reticenți în a furniza datele personale necesare.

Pe lângă acestea, există **riscuri asociate securității datelor și confidențialității**, în special în ceea ce privește stocarea și transferul acestora. De asemenea, există riscul ca datele personale să fie utilizate în mod necorespunzător sau să fie dezvăluite către terțe părți fără acordul utilizatorilor.

Toate aceste riscuri ar trebui luate în considerare atunci când se utilizează inteligența artificială pentru prelucrarea datelor personale și ar trebui să fie implementate măsuri adecvate pentru a le minimiza.

Protecția datelor personale în conformitate cu GDPR

Regulamentul general privind protecția datelor (GDPR) a fost creat pentru a proteja drepturile persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal. Acesta impune un set de principii care trebuie respectate de oricine prelucrează astfel de date, inclusiv în contextul utilizării inteligenței artificiale.

Aceste principii includ:

- **Legalitate, echitate și transparență**: datele cu caracter personal trebuie prelucrate în mod legal, echitabil și transparent în raport cu persoana vizată. Persoana vizată trebuie să fie informată cu privire la prelucrarea datelor și să i se ofere acces la informațiile referitoare la prelucrare.
- **Scopul limitat**: datele cu caracter personal trebuie colectate și prelucrate numai în scopul specific, explicit și legitim pentru care au fost colectate.
- **Minimizarea datelor**: datele cu caracter personal trebuie să fie adecvate, relevante și limitate la ceea ce este necesar în raport cu scopul pentru care sunt prelucrate.
- **Exactitate**: datele cu caracter personal trebuie să fie exacte și, dacă este necesar, actualizate.

- **Stocarea limitată:** datele cu caracter personal trebuie păstrate doar pentru perioada necesară în raport cu scopul pentru care au fost colectate și prelucrate.
- **Integritatea și confidențialitatea**: datele cu caracter personal trebuie protejate împotriva prelucrării neautorizate sau ilegale și împotriva pierderii, distrugerii sau deteriorării accidentale.
- **Responsabilitatea**: cel care prelucrează datele trebuie să fie responsabil pentru respectarea acestor principii și să poată demonstra conformitatea cu ele.

Este important să se ia în considerare aceste principii în timpul **dezvoltării și utilizării sistemelor de inteligență artificială** pentru a se asigura că se respectă drepturile persoanelor fizice în ceea ce privește protecția datelor cu caracter personal.

Inteligența artificială și măsurile tehnice și organizatorice pentru protecția datelor personale

Măsurile tehnice și organizatorice sunt esențiale pentru a proteja datele personale în utilizarea inteligenței artificiale.

În primul rând, politica de confidențialitate trebuie să fie clară și accesibilă, pentru a informa utilizatorii cu privire la modul în care datele lor sunt colectate, stocate, prelucrate și utilizate de către AI.

Un alt aspect important este aplicarea principiului de "**privacy by design**", care implică proiectarea și dezvoltarea sistemelor de inteligență artificială cu confidențialitatea în minte, **încă din faza de planificare**. Acest lucru poate include utilizarea de date anonime sau pseudonimizate, reducerea cantității de date personale colectate, precum și utilizarea de tehnologii de criptare și de securitate.

Este important să se dezvolte proceduri și protocoale adecvate pentru evaluarea riscurilor și implementarea măsurilor de securitate și confidențialitate, cum ar fi evaluarea impactului asupra protecției datelor (DPIA). De asemenea, se poate lua în considerare angajarea unui responsabil cu protecția datelor (DPO), care poate monitoriza utilizarea inteligenței artificiale și poate oferi sfaturi și asistență cu privire la protecția datelor personale.

Inteligența artificială și evaluarea impactului asupra protecției datelor (DPIA)

Evaluarea impactului asupra protecției datelor (DPIA) este un **proces obligatoriu** în cadrul GDPR și este deosebit de important în contextul utilizării inteligenței artificiale. DPIA

este necesară pentru a evalua și identifica riscurile și amenințările asupra datelor cu caracter personal.

Atunci când se utilizează inteligența artificială, este important să se efectueze o DPIA, care poate fi realizată în etapele de planificare și dezvoltare a soluției.

În timpul evaluării, ar trebui să se **analizeze toate riscurile potențiale legate de procesarea datelor cu caracter personal**, cum ar fi incertitudinea asupra rezultatelor AI sau incertitudinea privind exactitatea datelor de intrare.

DPIA (Evaluarea impactului asupra protecției datelor) **ar trebui să includă** o evaluare a impactului potențial asupra confidențialității și securității datelor, precum și o evaluare a riscurilor de discriminare sau de efecte negative asupra drepturilor și libertăților individuale. În plus, DPIA ar trebui să includă măsuri de mitigare a riscurilor identificate, precum și o evaluare a eficacității acestor măsuri.

În general, DPIA ar trebui să includă o descriere detaliată a procesului de prelucrare a datelor cu caracter personal, inclusiv tipurile de date utilizate, scopurile și metodele de prelucrare, precum și o analiză a riscurilor asociate. Aceasta ar trebui să includă, de asemenea, o evaluare a impactului asupra indivizilor, precum și o analiză a măsurilor tehnice și organizatorice luate pentru a proteja datele.

În concluzie, DPIA este un instrument important pentru a evalua și identifica riscurile asociate cu procesarea datelor cu caracter personal utilizând inteligența artificială și pentru a dezvolta măsuri de protecție adecvate.

Rolul DPO și utilizarea inteligenței artificiale

Rolul DPO (Responsabil cu Protecția Datelor) este esențial în protejarea datelor cu caracter personal și în evaluarea riscurilor asociate cu utilizarea inteligenței artificiale.

DPO-ul are **responsabilitatea de a se asigura că organizația respectă regulile de protecție a datelor** și că riscurile asociate cu utilizarea inteligenței artificiale sunt evaluate și gestionate corespunzător.

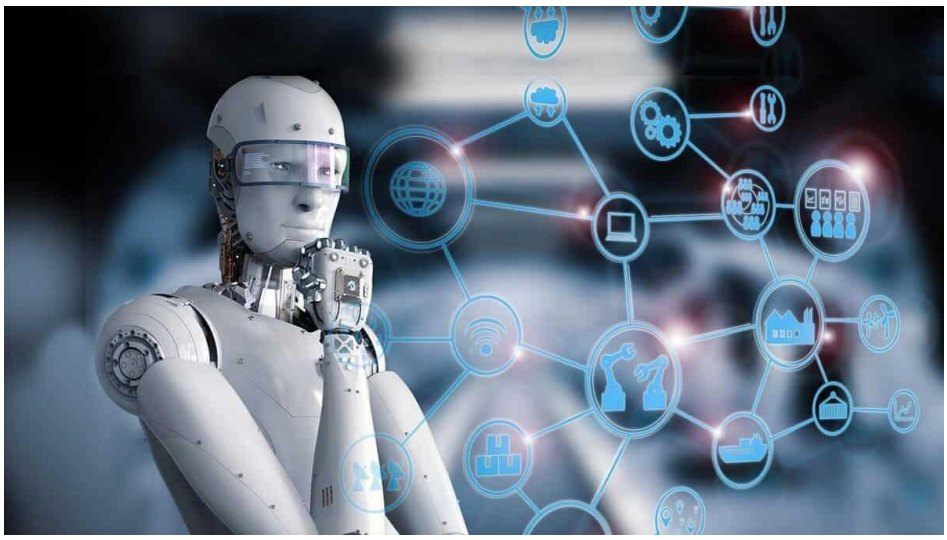
DPO-ul ar trebui să aibă **cunoștințe solide despre GDPR**, **precum și despre inteligența artificială și utilizarea acesteia în organizație**. DPO-ul ar trebui să se asigure că organizația ia în considerare toate riscurile asociate cu utilizarea inteligenței artificiale și că se iau măsuri corespunzătoare pentru a le aborda.

DPO-ul trebuie să se asigure că **organizația are politici și proceduri clare** pentru protecția datelor personale și că acestea sunt actualizate în mod regulat. În plus, DPO-ul ar trebui să colaboreze cu alte departamente din organizație, inclusiv cu departamentul IT, pentru

a se asigura că toate măsurile tehnice și organizatorice necesare sunt luate pentru a proteja datele cu caracter personal și pentru a evita riscurile asociate cu utilizarea inteligenței artificiale.

În concluzie, DPO-ul are un rol esențial în protejarea datelor cu caracter personal în utilizarea inteligenței artificiale și trebuie să fie implicat în toate aspectele legate de protecția datelor în organizație.

1. ***Cum să identificăm dacă un sistem de inteligență artificială generativă implică prelucrarea datelor cu caracter personal?***



Normele puse în aplicare în temeiul GDPR pot fi aplicate indiferent de tehnologia utilizată de operator și trebuie respectate, împreună cu toate celelalte acte legislative relevante ale UE (cum ar fi Legea privind AI în acest caz).

Dar aceste norme pot fi aplicate numai dacă sunt prelucrate datele cu caracter personal. În această măsură, în cazul unui sistem de inteligență artificială, în special al unui sistem de inteligență artificială generativă care este antrenat folosind cantități mari de date, atât personale, cât și nepersonale, identificarea posibilității de aplicare a GDPR poate fi complicată, mai ales dacă se ia în considerare faptul că dezvoltatorii sau furnizorii sistemului ar putea să nu fie întotdeauna suficient de specifici în analiza sistemului.

În această măsură, ar trebui să fie de datoria (cel puțin din punctul de vedere al Autorității Europeane pentru Protecția Datelor) UE să se asigure că legea este pusă în aplicare și că aceste sisteme sunt monitorizate în mod corespunzător pentru conformitate.

Prin urmare, este esențial să existe cooperare cu toate părțile implicate și să fie stabilit:

a. Dacă datele prelucrate de sistem sunt anonimizate sau dacă, în timpul proiectării, dezvoltării și testării sistemului, sunt utilizate seturi de date sintetice;

b. Controalele specifice care au fost instituite pentru a garanta astfel de rezultate (datele pierzându-și trasabilitatea către o persoană și eliminând astfel riscurile la adresa drepturilor acesteia);
c. Modalități de evitare a utilizării unor tehnici periculoase (din punctul de vedere al drepturilor fundamentale), cum ar fi web scraping-ul, care implică faptul că persoana vizată nu este în măsură să își dea consimțământul sau chiar să știe că datele sale personale sunt prelucrate;
d. Cel mai bun mod de a pune în aplicare un sistem de monitorizare constantă a sistemului în toate etapele dezvoltării și punerii sale în aplicare, care să asigure cel mai înalt grad de atenție pentru normele de protecție a datelor și drepturile fundamentale ale oricărei persoane vizate care ar putea fi implicată în prelucrare.

2. *Care este rolul RPD (Responsabilului cu protecția datelor), în procesul de dezvoltare a sistemelor de inteligență artificială generativă?*

În conformitate cu sarcinile stabilite la articolul 45 din RGPD (Regulamentul general privind protecția datelor), RPD este responsabil pentru informarea și consilierea în legătură cu obligațiile relevante în materie de protecție a datelor, pentru a asista operatorii în monitorizarea conformității interne și pentru a oferi (la cerere) consiliere cu privire la evaluarea impactului asupra protecției datelor (DPIA).

În plus, RPD trebuie să acționeze ca punct de contact între persoanele vizate și operatori.

Așadar, care este relevanța acestui aspect în contextul punerii în aplicare a AI generativă? AEPD (Autoritatea Europeană pentru Protecția Datelor) a reafirmat importanța menținerii acestor sarcini prevăzute la articolul 45, dar a susținut, de asemenea, că rolul RPD (Responsabilului cu protecția datelor) va trebui, de asemenea, să evolueze. În această măsură, acesta va trebui să se instruiască în mod proactiv, astfel încât să aibă o înțelegere adecvată a ciclului de viață al sistemului de AI. RPD va trebui să învețe cum și când acest sistem colectează date, cum funcționează mecanismele de intrare și ieșire, precum și cum funcționează procesul "decizional" implementat în sistem în raport cu toate aceste aspecte menționate anterior.

Cu toate acestea, este clar că această sarcină nu va fi ușoară sau simplă, motiv pentru care AEPD recomandă, de asemenea, ca, în ceea ce privește conformitatea sistemului de inteligență artificială generativă cu normele de protecție a datelor, comunicarea semnificativă și eficientă să joace un rol esențial în activitatea RPD (Responsabilul cu protecția datelor). În acest sens, AEPD (Autoritatea Europeană pentru Protecția Datelor) recomandă inițierea unei relații de

dialog continuu între respectivul RPD și toate celelalte părți interesate relevante din cadrul organizației (fie că este vorba de reprezentanți ai serviciilor juridice sau IT, responsabili locali cu securitatea informatică etc.) pe parcursul ciclului de viață al sistemului AI.

În ceea ce privește necesitatea efectuării unei DPIA, AEPD (Autoritatea Europeană pentru Protecția Datelor) recunoaște că o astfel de analiză trebuie efectuată înainte de orice operațiune de prelucrare care este susceptibilă să prezinte un risc ridicat pentru drepturile și libertățile fundamentale ale persoanelor vizate. În acest caz, operatorul este obligat să recurgă la ajutorul și să asculte sfaturile unui RPD (Responsabilul cu protecția datelor).

În plus, din cauza modului în care funcționează modelul, AEPD consideră că, pe parcursul ciclului de viață al sistemului AI, sunt predispuse să apară noi riscuri. În această măsură, AEPD recomandă ca, în cazul unei analize DPIA, riscurile să fie identificate și abordate ca un proces continuu de-a lungul întregului ciclu de viață al sistemului.

3. *Principiile generale ale protecției datelor pot fi aplicate în continuare în contextul implementării sistemelor de inteligență artificială generativă?*

Principalele puncte de interes adresate de AEPD (Autoritatea Europeană pentru Protecția Datelor) au fost:

- *Prelucrarea legală a datelor cu caracter personal în timpul dezvoltării și implementării unui sistem de inteligență artificială generativă;*

În această măsură, AEPD a decis că prelucrarea datelor cu caracter personal de către aceste tipuri de sisteme necesită un temei juridic care este în conformitate cu principiile RGPD. În plus, în cazul în care consimțământul urmează să fie utilizat ca temei juridic, există un grad mai mare de atenție care trebuie să fie utilizat de către colector pentru a se asigura că respectivul consimțământ este valabil (îndeplinind cerințele RGPD).

- *Modul în care principiul minimizării datelor poate fi aplicat prelucrării datelor cu caracter personal atunci când se utilizează sisteme de inteligență artificială generativă;*

În ciuda faptului că sistemele de inteligență artificială generativă depind de analiza unei cantități relativ mari de date pentru a produce rezultate eficiente, AEPD a susținut că acest lucru nu înseamnă că principiul minimizării datelor nu poate fi aplicat. Modul în care aceste sisteme sunt concepute și puse în aplicare va trebui să ia în considerare obligațiile operatorilor de date de a colecta și prelucra numai acele date care sunt necesare în scopul prelucrării.

- *Respectarea principiului acurateței datelor;*

În documentul său de orientare, AEPD recunoaște o problemă care rezultă din utilizarea inteligenței artificiale generative. Și anume, faptul că aceste sisteme sunt încă predispuse la rezultate inexacte care afectează drepturile și libertățile subiecților. Din acest motiv, AEPD pledează pentru mai multe eforturi atât din partea dezvoltatorilor de sisteme, cât și din partea celor care adoptă aceste sisteme.

AEPD consideră că ar trebui implementate și aplicate instrumente de supraveghere mai puternice pe parcursul întregului ciclu de viață al sistemului. În cazul în care inexactitățile se dovedesc a cauza un risc prea mare, AEPD recomandă, de asemenea, să nu se implementeze complet sistemul inexact.

4. Cum mai putem aplica drepturile persoanelor vizate în contextul sistemelor de inteligență artificială generativă?

Parcurgând răspunsul AEPD (Autoritatea Europeană pentru Protecția Datelor) la întrebarea privind modul în care dreptul la informare al persoanei vizate va evolua odată cu adoptarea sistemelor AI generative, AEPD subliniază faptul că această obligație va rămâne neschimbată.

Conform aplicării articolelor 12 și 22 din RGPD, persoana vizată trebuie să fie informată în mod semnificativ nu numai cu privire la prelucrare (și actualizată atunci când este necesar, dacă se schimbă ceva în cursul ciclului de viață al sistemului de inteligență artificială), ci și cu privire la logica sistemului și la modul în care acesta ajunge la decizii, oferind informații persoanei vizate cu privire la modul în care drepturile sale ar putea fi afectate. AEPD continuă să pledeze în favoarea păstrării de către persoana vizată a controlului asupra propriilor date.
În ceea ce privește sistemele AI generative și responsabilitatea operatorilor (în ceea ce privește drepturile persoanelor vizate), AEPD rămâne fermă în orientările sale. AEPD pledează pentru o abordare care rămâne foarte protectoare a drepturilor persoanelor vizate, afirmând că ar trebui să se acorde o atenție deosebită riscurilor la adresa acestor drepturi. În plus, AEPD susține că este necesară o supraveghere suplimentară a sistemului pe parcursul întregului ciclu de viață al acestuia, asigurând ca prioritate minimizarea și atenuarea prejudecăților.

În ceea ce privește exercitarea drepturilor persoanelor vizate, AEPD reafirmă obligația operatorilor de date cu caracter personal și oferă o soluție la dificultățile percepute asociate cu aplicarea drepturilor persoanelor vizate în contextul sistemelor AI. În această măsură, pentru a contracara dificultăți precum identificarea datelor cu caracter personal ale persoanei vizate sau obținerea accesului la acestea, ar trebui instituite astfel de mecanisme chiar înainte de adoptarea

sistemului sau încă din primele etape ale punerii sale în aplicare, care ar permite înregistrarea detaliată și trasabilitatea activităților de prelucrare.

Corectitudinea (Fairness) în inteligența artificială

Fairness este un aspect important în utilizarea inteligenței artificiale, deoarece **sistemele AI pot avea o serie de influențe și efecte nedorite** asupra diferitelor grupuri de utilizatori sau asupra unor caracteristici ale acestora.

În consecință, este important să se evalueze corectitudinea acestor sisteme în raport cu grupurile de utilizatori și să se ia măsuri pentru a asigura o utilizare echitabilă a acestora.

Metricile care pot fi utilizate pentru a evalua **corectitudinea unui sistem AI** includ:

- **Error rate** – Aceasta măsoară proporția de clasificări greșite pentru fiecare grup de utilizatori în ceea ce privește un anumit atribut, cum ar fi rasă sau gen. Dacă există diferențe semnificative în ratele de eroare între grupuri, sistemul poate fi considerat nedrept.
- **Confusion matrix** – Acesta este un tabel care arată numărul de adevărate pozitive, false pozitive, adevărate negative și false negative pentru fiecare grup de utilizatori. Această metrică poate fi utilizată pentru a evalua dacă există o discriminare în ceea ce privește clasificările făcute de sistem pentru fiecare grup.
- **Disparate impact** – Aceasta măsoară dacă un sistem AI are un impact diferit asupra grupurilor de utilizatori în ceea ce privește un anumit atribut. De exemplu, dacă un sistem de împrumuturi refuză mai mulți utilizatori dintr-un anumit grup decât din altul, sistemul poate fi considerat nedrept.
- **Accesul la date** – Este important să se ia în considerare accesul la date în evaluarea corectitudinii unui sistem AI. Dacă datele utilizate în antrenarea sistemului sunt în mod incorect părtinitoare sau incomplete, acest lucru poate duce la un sistem nedrept.

Inteligența Artificială și GDPR – un parteneriat complicat

La prima vedere, AI și GDPR par să aibă obiective contradictorii: AI vrea date, multe date, pentru a putea funcționa optim; GDPR impune limite stricte asupra modului în care sunt prelucrate datele personale. Această „tensiune” ridică întrebări de etică și responsabilitate.
Să luăm câteva exemple concrete:

- **Recomandări personalizate în comerțul online**: Mulți retaileri folosesc AI pentru a recomanda produse pe baza istoricului de cumpărături și a preferințelor noastre online. Însă,

pentru a respecta GDPR, aceste recomandări trebuie să fie transparente. Clientul are dreptul să știe că datele sale sunt folosite pentru profilare și, în plus, are dreptul de a se opune.

- **Aplicațiile de recunoaștere facială în centrele comerciale**: Unele magazine testează camere inteligente care recunosc emoțiile clienților pentru a le oferi o experiență personalizată. Cu toate acestea, GDPR impune reguli stricte pentru prelucrarea datelor biometrice, iar acest tip de monitorizare poate fi considerat o încălcare a confidențialității dacă nu există consimțământ explicit.
- **Sisteme de monitorizare în sănătate**: În spitale, AI poate analiza datele medicale pentru a face predicții despre starea de sănătate a pacienților. Deși acest lucru are un impact pozitiv major, confidențialitatea pacientului trebuie respectată. GDPR cere ca astfel de prelucrări să fie realizate doar cu pseudonimizare și anonimizare, pentru a proteja identitatea pacienților.

Confidențialitatea datelor pentru comercianții mici și mijlocii

Pentru a asigura o utilizare corectă și echitabilă a inteligenței artificiale, este important să se evalueze corectitudinea sistemelor AI și să se ia măsuri adecvate pentru a îmbunătăți această corectitudine, dacă este cazul.

În era digitală, confidențialitatea datelor și considerentele etice în inteligența artificială (AI) sunt probleme critice pentru companiile de toate dimensiunile. Pentru comercianții mici și mijlocii, înțelegerea și implementarea celor mai bune practici în aceste domenii este esențială pentru a construi încrederea clienților, pentru a respecta reglementările și pentru a menține o reputație pozitivă.

De ce este importantă confidențialitatea datelor pentru comercianții mici și mijlocii?

- **Încrederea clienților:** menținerea confidențialității datelor este crucială pentru construirea și păstrarea încrederii clienților. Când clienții știu că datele lor sunt în siguranță, este mai probabil să interacționeze cu afacerea ta.
- **Conformitatea cu reglementările:** aderarea la legile privind protecția datelor, cum ar fi Regulamentul general privind protecția datelor (GDPR) nu este opțională. Nerespectarea poate duce la sancțiuni severe.
- **Gestionarea reputației:** încălcările de date pot dăuna semnificativ reputației afacerii tale. Asigurarea confidențialității datelor ajută la prevenirea unor astfel de incidente și protejează imaginea mărcii.

Înțelegerea colectării și utilizării datelor

Este esențial pentru comercianții mici și mijlocii să înțeleagă cum colectează și utilizează datele clienților. Trebuie să fii clar cu ce tipuri de date colectezi, cum ar fi informații personale, istoricul achizițiilor și comportamentul de navigare.

La fel de important este să înțelegi de ce colectezi aceste date și cum le vei folosi pentru a îmbunătăți experiențele clienților și operațiunile de afaceri. A fi transparent cu privire la practicile tale de date creează încredere cu clienții tăi și asigură conformitatea cu reglementările privind protecția datelor.

Considerații etice în AI

Pe măsură ce tehnologiile AI continuă să avanseze, întrebările legate de etică și implementarea responsabilă a AI au ajuns în prim-plan. În timp ce AI oferă numeroase beneficii, inclusiv eficiență îmbunătățită și experiențe personalizate pentru clienți, ea ridică și provocări etice care trebuie abordate.

La 13 martie 2024, Parlamentul European a adoptat oficial Legea privind inteligența artificială a UE („Legea AI”) cu o mare majoritate de 523-46 de voturi în favoarea legislației. Actul AI este prima lege orizontală și de sine stătătoare din lume care guvernează AI, marcând o etapă legislativă semnificativă pentru UE.

Regulile propuse sunt:

- Abordarea riscurilor create special de aplicațiile AI.
- Interzicerea practicilor AI care prezintă riscuri inacceptabile.
- Stabilirea unei liste de aplicații cu risc ridicat.
- Stabilirea cerințelor clare pentru sistemele AI utilizate în aplicații cu risc ridicat.

-Definirea obligațiilor specifice pentru implementatorii și furnizorii de aplicații AI cu risc ridicat.

- Solicitarea unei evaluări a conformității înainte ca un anumit sistem AI să fie pus în funcțiune sau introdus pe piață.

- Implementarea măsurilor de aplicare după ce un anumit sistem AI este introdus pe piață.

- Stabilirea unei structuri de guvernanță atât la nivel european, cât și național.

Sistemele AI considerate o amenințare clară pentru siguranța, mijloacele de trai și drepturile oamenilor vor fi interzise, de la punctaj social de către guverne până la jucării care folosesc asistență vocală care încurajează comportamentul periculos.

Una dintre considerentele etice cheie în AI este părtinirea. Algoritmii AI sunt la fel de imparțiali ca datele pe care sunt antrenați. Fără o atenție deosebită, acești algoritmi pot perpetua sau chiar exacerba părtinirile existente, ducând la rezultate discriminatorii. Companiile trebuie să se asigure că sistemele lor de inteligență artificială sunt instruite pe seturi de date diverse și reprezentative pentru a atenua părtinirea și a promova corectitudinea.

În plus, transparența și responsabilitatea sunt principii esențiale în etica AI. Companiile ar trebui să fie transparente cu privire la utilizarea AI în operațiunile lor și să răspundă pentru deciziile luate de sistemele AI. Aceasta include oferirea de căi de recurs în cazul erorilor algoritmice sau a consecințelor neintenționate.

Implementarea AI conform eticii

- **Cadre etice de AI:** adoptă cadre și linii directoare care promovează practicile etice de AI. Aceste cadre oferă o abordare structurată a integrării eticii în dezvoltarea AI.
- **Selectarea furnizorilor:** alegeți furnizori și parteneri AI care acordă prioritate confidențialității datelor și practicilor etice AI.
- **Monitorizare continuă:** auditează și monitorizează în mod regulat sistemele AI pentru a asigura conformitatea continuă cu standardele etice. Acest lucru ajută la identificarea și remedierea promptă a oricăror probleme etice.

Impactul legilor privind confidențialitatea datelor asupra comercianților

Pe lângă considerentele etice, comercianții trebuie, de asemenea, să navigheze într-un peisaj de reglementare complex în jurul confidențialității datelor și AI. În funcție de locația lor geografică și de natura afacerii lor, comercianții pot fi supuși diferitelor reglementări, cum ar fi Regulamentul general privind protecția datelor (GDPR) în Europa sau Legea privind confidențialitatea consumatorilor din California (CCPA) în Statele Unite.

Respectarea acestor reglementări nu numai că evită potențialele repercusiuni legale, dar demonstrează și angajamentul de a respecta confidențialitatea clienților și de a susține standardele etice. Comercianții ar trebui să se familiarizeze cu reglementările relevante și să caute consiliere juridică, dacă este necesar, pentru a asigura conformitatea.

Comunicarea cu clientul și consimțământul

- **Politici transparente:** crează politici de confidențialitate clare și concise care informează clienții despre datele pe care le colectezi și despre modul în care acestea sunt utilizate.
- **Obținerea consimțământului:** obține consimțământul explicit de la clienți înainte de a colecta și utiliza datele acestora. Asigură-te că consimțământul este informat și dat în mod liber.
- **Gestionarea solicitărilor de date:** fii pregătit să gestionezi solicitările clienților cu privire la datele lor, cum ar fi accesul, corectarea și ștergerea. Stabilește un proces simplu pentru gestionarea acestor solicitări.

Generarea de date sintetice în domeniul inteligenței artificiale (AI)

Generarea de date sintetice în domeniul inteligenței artificiale (AI) reprezintă o tehnică crucială ce joacă un rol central în diverse domenii și aplicații. Această practică implică crearea de date artificiale care să semene cât mai mult cu datele reale din lumea reală, chiar dacă nu provin din observații sau măsurători efective.

Datele sintetice sunt generate folosind o gamă variată de algoritmi sofisticați, modele statistice sau tehnici computaționale, permițându-le să imite proprietățile statistice și modelele găsite în datele reale.

Această abordare oferă mai multe avantaje și aplicații în diferite domenii:

1. **Augmentarea Datelor:** Unul dintre principalele scopuri ale generării de date sintetice este augmentarea datelor. Atunci când se lucrează cu seturi de date limitate, ceea ce este frecvent în multe sarcini de învățare automată, generarea de date sintetice poate ajuta la extinderea dimensiunii și diversității setului de date. Aceasta este deosebit de utilă pentru instruirea modelelor de învățare automată mai robuste, care necesită o cantitate semnificativă de date.
2. **Păstrarea Intimității:** În situațiile în care informații sensibile sau private sunt implicate, organizațiile nu pot să împărtășească sau să utilizeze în mod liber datele reale pentru dezvoltarea și testarea modelelor, din cauza reglementărilor privind intimitatea și a preocupărilor etice. Datele sintetice oferă o modalitate de a genera date reprezentative care păstrează proprietățile statistice esențiale ale datelor originale, în timp ce asigură protecția intimității.

3. **Abordarea Dezechilibrului Datelor:** Seturile de date dezechilibrate, în care o clasă sau categorie este semnificativ subreprezentată în comparație cu celelalte, pot duce la performanța viciată a modelului. Generarea de date sintetice poate ajuta la echilibrarea acestor seturi de date, creând exemple suplimentare ale clasei minoritare, permițând modelului să învețe mai bine și să reprezinte cu precizie toate clasele.
4. **Testarea și Dezvoltarea Algoritmilor:** În cazurile în care accesul la datele din lumea reală este limitat, în special în domenii emergente sau aplicații de nișă, datele sintetice pot fi folosite pentru testarea și dezvoltarea algoritmilor. Acest lucru asigură că algoritmii și modelele performează eficient înainte de a fi implementați în scenarii din lumea reală.
5. **Simularea:** Datele sintetice sunt adesea folosite în simulări și modele pentru a replica scenarii din lumea reală. De exemplu, în dezvoltarea vehiculelor autonome, datele sintetice sunt folosite pentru a simula diverse condiții și scenarii de conducere pentru testarea percepției și sistemelor de luare a deciziilor ale vehiculului.
6. **Îmbunătățirea Diversității Datelor:** Generarea de date sintetice facilitează crearea de seturi de date diverse, acoperind o gamă largă de scenarii și variații posibile. Această diversitate poate îmbunătăți semnificativ generalizarea și robustețea modelelor de învățare automată, făcându-le mai adaptabile la complexitatea din lumea reală.

   Tehnicile folosite pentru generarea de date sintetice sunt diverse și se adaptează la aplicații specifice.

   Câteva abordări comune includ:

- **Generarea Aleatorie a Datelor:** Generarea simplă de numere aleatoare poate fi folosită pentru a crea date sintetice pentru anumite tipuri de variabile, cum ar fi date, nume sau valori numerice în anumite intervale specificate.
- **Modele Generative:** Modele generative avansate, cum ar fi Rețelele Generative Adversariale (GANs) și Autoencoder-urile Variational (VAEs), sunt instrumente puternice pentru generarea de date sintetice. GAN-urile, în special, excelențează în generarea de exemple care arată realist, prin antrenarea unui generator pentru a produce date care sunt de nerecunoscut ca fiind sintetice de către un discriminator.
- **Modele Parametrice:** Modele statistice, cum ar fi distribuțiile Gaussian sau alte distribuții de probabilitate, pot fi utilizate pentru a genera date sintetice cu proprietăți statistice specifice, asigurându-se că acestea respectă distribuția dorită.
- **Transformarea Datelor:** Tehnici precum inversarea, rotația sau scalarea pot fi folosite pentru a crea variații sintetice ale datelor existente, în special în cazul augmentării datelor de imagini.

- **Generarea Bazată pe Reguli:** În unele cazuri, datele sintetice pot fi generate pe baza unor reguli sau modele predefinite. De exemplu, simularea unui set de date de trafic bazat pe reguli și modele de trafic stabilite.

  Este important de subliniat că eficacitatea generării de date sintetice depinde de precizia modelelor subiacente și de gradul de asemănare dintre datele sintetice și datele reale pe care sunt menite să le reprezinte. Procese riguroase de validare și evaluare sunt esențiale pentru a asigura că datele sintetice îndeplinesc eficient scopul lor în aplicațiile de inteligență artificială. Generarea de date sintetice găsește aplicații în diverse domenii, demonstrând versatilitatea și importanța sa:
- **Sănătate:** În imagistica medicală, datele sintetice pot fi generate pentru a crea exemple suplimentare pentru instruirea modelelor de învățare profundă folosite în sarcini precum segmentarea imaginilor RMN, detectarea leziunilor sau clasificarea bolilor.
- **Finanțe:** Datele sintetice pot simula profiluri de credit și tranzacții financiare pentru a instrui modele de evaluare a creditului fără a utiliza date reale ale clienților, asigurându-se astfel confidențialitatea și conformitatea cu reglementările.
- **Retail și Comerț Electronic:** Datele sintetice pot simula comportamentele clienților, modelele de navigare și deciziile de cumpărare pentru a optimiza designul site-urilor web și pentru a îmbunătăți sistemele de recomandare, fără a utiliza datele reale ale clienților.
- **Vehicule Autonome:** Datele sintetice sunt esențiale în crearea de scenarii realiste de conducere pentru testarea algoritmilor de conducere autonomă. Datele simulate de senzori ajută la instruirea și validarea sistemelor de vehicule autonome.
- **Procesarea Limbajului Natural (NLP):** În NLP, datele sintetice de text pot fi generate pentru diverse sarcini, inclusiv rezumatul textelor, traducerea limbilor și analiza sentimentelor. Aceste date de text sintetic ajută la augmentarea datelor și la instruirea modelelor.
- **Producție:** Datele sintetice pot simula produse defecte și non-defecte pe linii de producție, facilitând instruirea sistemelor de viziune artificială pentru controlul calității fără a implica datele reale ale produselor.
- **Securitate Cibernetică:** Datele sintetice de trafic de rețea pot fi generate pentru a instrui sistemele de detectare a intruziunilor, asigurându-se că acestea pot recunoaște și răspunde eficient la diverse tipuri de amenințări cibernetice.
- **Științele Mediului:** Datele climatice sintetice pot completa datele limitate despre climatul real, utilizate pentru instruirea modelelor de prognoză a climei, meteorologie și cercetări de mediu.

- **Științe Sociale:** Datele sintetice pot simula răspunsuri la sondaje și chestionare pentru cercetarea socială, fără a compromite confidențialitatea indivizilor, asigurându-se astfel colectarea etică și conformă cu privire la date.
- **Detectarea Anomaliei:** În domeniul detecției fraudei, datele sintetice pot fi utilizate pentru a crea exemple de tranzacții frauduloase și non-frauduloase, permițând instruirea modelelor de învățare automată pentru a detecta eficient frauda financiară.
- **Procesarea Imaginilor:** În domeniul producției și controlului calității, se pot genera imagini sintetice ale produselor cu defecte pentru a instrui algoritmii de detectare a defectelor folosiți pe linii de producție.
- **Agricultură:** Datele sintetice, inclusiv imagini ale culturilor sănătoase și ale celor afectate de boli, pot fi generate pentru a instrui modele de viziune artificială pentru detectarea automată a bolilor culturilor, contribuind la agricultura de precizie.

Concluzii

- Utilizarea inteligenței artificiale implică o serie de riscuri privind protecția datelor cu caracter personal, precum discriminarea, profilarea, lipsa de transparență și responsabilitate. Pentru a proteja datele cu caracter personal în contextul inteligenței artificiale, este important să se aplice principiile GDPR și să se dezvolte politici de confidențialitate și securitate adecvate, precum și să se aplice principiul de "privacy by design".
- De asemenea, evaluarea impactului asupra protecției datelor (DPIA) și rolul DPO sunt esențiale pentru evaluarea riscurilor asociate cu utilizarea inteligenței artificiale. În plus, se recomandă dezvoltarea și utilizarea de metrici pentru a evalua corectitudinea unui sistem AI.
- În final, implementarea măsurilor tehnice și organizatorice adecvate poate ajuta la protejarea datelor cu caracter personal și asigurarea conformității cu GDPR în utilizarea inteligenței artificiale.
- WIRED analizează utilizarea algoritmilor de învățare automată în detectarea fraudelor și alte forme de automatizare a suspiciunii.
- Pe măsură ce învățarea automată devine tot mai sofisticată, aceasta poate fi **folosită acum pentru a detecta comportamente suspecte**, precum și **pentru a analiza seturi mari de date cu eficiență și precizie**. În plus, datorită capacității sale de a procesa datele mai rapid decât oamenii, poate fi implementată în diferite domenii, cum ar fi sistemele de asistență socială și platformele de socializare. Deși există beneficii asociate

cu utilizarea algoritmilor de învățare automată pentru detectarea suspiciunilor, **există și riscuri potențiale**. De exemplu, aceasta poate duce la **acuzații false sau la identificări eronate,** ceea ce ar putea cauza prejudicii imense persoanelor sau grupurilor de persoane.

BIBLIOGRAFIE

- https://orasuldeva.ro/2024/04/24/demystifying-artificial-intelligence-a-beginners-guide/
- https://gdprcomplet.ro/inteligenta-artificiala-si-gdpr/
- https://decalex.ro/blog/ghid-privind-inteligenta-artificiala-generativa-gai-si-protectia-datelor
- https://www.globalpayments.ro/ro-ro/blog/2024/06/12/confidentialitate-date-ai
  https://issuemonitoring.eu/inteligenta-artificiala-in-contextul-confidentialitatii-datelor/
- https://corpquants.ro/generarea-de-date-sintetice-in-domeniul-inteligentei-artificiale-ai/
- https://www.dpoconsulting.ro/inteligenta-artificiala/