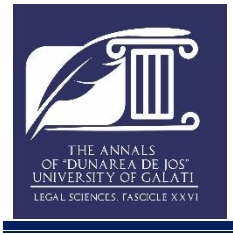

Protection of Personal Data within Platforms Developed in the context of Artificial Intelligence from the Perspective of National and European Law

Elena SÂRGHI[1]

Marian ILEANA[2]

Abstract: Artificial Intelligence (AI) is an increasingly popular technology in modern society, successfully used in a multitude of fields, from health to transportation. When using such technologies, concerns also arise regarding the protection of personal data, as AI algorithms can easily collect and process large amounts of personal data. This article will analyze the protection of personal data in platforms developed around AI from the perspective of national and European legislation. The first to be analyzed are the relevant legal provisions of Romanian and European law, focusing on the General Data Protection Regulation (GDPR). The conclusion of this paper is that the protection of personal data in the context of AI is a complex issue that requires a careful approach from personal data controllers. To ensure an adequate level of data protection, controllers must be up to date with legal regulations and apply appropriate protection measures recommended by the legislation in force.

Keywords: personal data protection; artificial intelligence; national law; European law; GDPR

1. Introducere

În zilele noastre, platformele online evoluează cu o rapiditate crescută având în vedere inteligența artificială (IA) care este tot mai accesibilă, și rapiditatea de dezvoltare a acesteia. Aplicațiile și platformele ce includ o astfel de tehnologie devin rapid omniprezente în viața cotidiană, schimbând într-un ritm accelerat și pentru

[1] "Al. Ioan Cuza" University of Iasi & National University of Science and Technology Politehnica Bucharest, University Center Pitești, Romania, Address: Str. Târgul din Vale nr. 1, Pitești 110040, Romania, Corresponding author: sarghielena7@gmail.com.

[2] "Al. Ioan Cuza" University of Iasi & National University of Science and Technology Politehnica Bucharest, University Center Pitești, Romania, Address: Str. Târgul din Vale nr. 1, Pitești 110040, Romania, E-mail: marianileana95@gmail.com.

totdeauna modul de interacţiune al utilizatorului cu tot ce înseamnă mediul online (Bostrom, 2014).

Această lucrare dorește să ofere o viziune de ansamblu asupra legislației prezente și o predicție asupra direcției privind adaptarea acesteia, pentru a face față provocărilor aduse de noile tehnologii.

Pentru a putea răspunde la întrebarea: ce este IA, trebuie să avem o privire de ansamblu asupra problemelor ce le poate rezolva aceasta. IA este utilizat în cea mai mare parte pentru a automatiza acțiuni ce depind de intervenția umană (Surden, 2019). O definiție simplă este automatizarea sarcinilor care implică utilizarea inteligenței umane pentru a fi realizate. S-a reușit automatizarea unor activități complexe printre care: jocuri de șah, prelucrarea imaginilor, traducerea din limbi străine și conducerea vehiculelor.

Odată cu utilizarea tot mai excesivă a inteligenței artificiale în diverse domenii de activitate, cantitatea de date cu caracter personal ce ajunge să fie procesată de către inteligența artificială crește vertiginos. Datele pot include informații printre altele despre: locația, identitatea, interesele și comportamentul unei persoane (Schünemann & Baumann, 2017).

Modul prin care aceste procesatoare de text inteligente își iau datele de antrenament de pe internet a ajuns să fie atent analizate de către autorități. O primă țară europeană care a arătat reticență pentru astfel de tehnologii precum ChatGPT a fost Italia (Kreitmeir & Raschky, January, 2023). Aceasta a devenit prima țară care a blocat accesul copiilor sub 13 ani, prin decizia Autorității italiene pentru protecția datelor.

Prin indexarea datelor, incluzând cele cu caracter personal este reprezentat procesul de etichetare pentru a putea fi găsite cu ușurință. Acest proces este un prim pas important pentru instruirea tehnologiilor de tip IA, deoarece pune la dispoziție modelelor IA să modeleze și să învețe asupra unor seturi de date mari și complexe.

O mare parte din tehnologiile disponibile pe internet ce sunt disponibile publicului larg sunt Large Language Model, acestea sunt antrenate pe seturi foarte mari de date și cod pentru a genera text, a realiza traduceri, și pentru a realiza conținut creativ (Russell & Norvig, 2020). Aceste LLM-uri sunt utilizate în: asistenți virtuali, traducere, scriere creativă, pot inclusiv răspunde la întrebări. Acestea sunt încă în plin proces de dezvoltare, dar impactul acestora deja modifică lumea tehnologică modernă. Utilizate într-o varietate largă de aplicații, acestea își continuă evoluția și vor devenii tot mai puternice și versatile.

Uniunea Europeană are ca obiectiv principal protecția datelor cu caracter personal, în acest sens a fost instituit Regulamentul General Privind Protecția Datelor (GDPR), acesta reprezintă principalul cadrul legal privind protecția acestor date în UE.

2. Cadru normativ

În această secţiune vom analiza reglementările europene şi naţionale referitoare la protecţia juridică a datelor cu caracter personal în operaţiunile derulate prin utilizarea diverselor platforme care apelează la inteligenţa artificială.

În privinţa cadrului normativ european, prezintă o importanţă majoră Regulamentul UE nr. 2016/679[1] privind protecţia persoanelor fizice în ceea ce priveşte prelucrarea datelor cu caracter personal şi privind libera circulaţie a acestor date (în continuare, GDPR), care trasează principalele coordonate în materia modalităţilor de protecţie a acestor informaţii personale. Regulamentul creionează ca domeniu de aplicare arii în care se efectuează prelucrarea datelor cu caracter personal, total sau parţial prin mijloace automatizate, precum şi prelucrarea prin alte mijloace decât cele automatizate a datelor cu caracter personal care fac parte dintr-un sistem de evidenţă a datelor sau care sunt destinate să facă parte dintr-un sistem de evidenţă a datelor. Din acest aspect reiese faptul că inteligenţa artificială este cea mai predispusă ca, prin acţiunile întreprinse, să intre în câmpul de acţiune al reglementării europene.

Totodată, în expunerea de motive este prezentat aspectul că persoanele fizice pot fi asociate cu identificatorii online furnizaţi de dispozitivele, aplicaţiile, instrumentele şi protocoalele lor, cum ar fi adresele IP, identificatorii cookie sau alţi identificatori, ceea ce reprezintă doar o redusă parte din consecinţele interacţiunii cu astfel de platforme. Mai multe decât atât, în definiţia oficială a termenului de „date cu caracter personal" sunt incluse şi următoarele: date de localizare, un identificator online, sau la unul sau mai multe elemente specifice, proprii identităţii sale fizice, fiziologice, genetice, psihice, economice, culturale sau sociale. Ce putem înţelege din această definiţie e că din simpla acceptare a cookies-urilor reies o serie de drepturi şi obligaţii corelative pentru operatorul de date.

Regulamentul GDPR nu reglementează într-un cadru specific această intersectare a datelor cu caracter personal cu inteligenţa artificială, ci doar oferă reguli generale cu privire la procesul de prelucrare a datelor, ceea ce este de natură a duce la apariţia unei carenţe legislative în diverse operaţiuni online, prin care s-ar aduce atingere însăşi scopului final al GDPR-ului, anume protecţia unui drept aflat în directă corelaţie cu dreptul la viaţa privată, cu consacrare distinctă în art. 8 (1) Carta Drepturilor Fundamentale a Uniunii Europene şi art. 16 (1) Tratatul privind funcţionarea Uniunii Europene.

[1] Regulamentul (UE) 2016/679 al Parlamentului European şi al Consiliului din 27 aprilie 2016 privind protecţia persoanelor fizice în ceea ce priveşte prelucrarea datelor cu caracter personal şi privind libera circulaţie a acestor date şi de abrogare a Directivei 95/46/CE, Jurnalul Oficial nr. L 119/1.

Alte două acte normative europene care privesc protecția datelor cu caracter personal, dar în domenii mult mai specifice sunt Directiva nr. 2016/680 privind protecţia persoanelor fizice referitor la prelucrarea datelor cu caracter personal de către autoritățile competente în scopul prevenirii, depistării, investigării sau urmăririi penale a infracţiunilor sau al executării pedepselor şi privind libera circulaţie a acestor date[1] şi Regulamentul nr. 2018/1725 privind protecţia persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal de către instituţiile, organele, oficiile şi agenţiile Uniunii.[2]

Directiva reia principiile GDPR-ului, făcând o distincție relevantă între conceptul de datele cu caracter personal şi verificarea calității datelor cu caracter personal, în scopul derulării procedurilor de urmărire penală sau a executării pedepselor, fără a analiza o posibilă utilizare a inteligenței artificiale pentru facilitarea acestor operaţiuni.

Regulamentul nr. 2018/1725 face referire la anumite operaţiuni care ar implica inteligența artificială, precum crearea paginilor oficiale ale instituţiilor, organelor, oficiilor şi agenţiilor UE, care ulterior vor fi accesate de către persoanele fizice, ceea ce va determina prelucrarea datelor cu caracter personal. În acest sens, sunt instituite o serie de obligaţii în sarcina acestor instituţii, obligaţii care, într-o semnificativă măsură, se aseamănă cu cele introduse de către GDPR.

Putem concluziona, până în acest punct, că la nivel european nu există un instrument juridic apt să reglementeze cadrul în care platformele create şi dezvoltate prin valorificarea inteligenței artificiale prelucrează datele cu caracter personal, în acest sens aplicându-se, într-o manieră cât se poate de generală GDPR-ul.

În privința dreptului intern, singurul act normativ care face referire la protecția datelor cu caracter personal este Legea nr. 363/2018 privind protecția persoanelor fizice referitor la prelucrarea datelor cu caracter personal de către autoritățile competente în scopul prevenirii, descoperirii, cercetării, urmăririi penale şi combaterii infracțiunilor sau al executării pedepselor, măsurilor educative şi de

[1] Directiva (UE) 2016/680 a Parlamentului European şi a Consiliului din 27 aprilie 2016 privind protecţia persoanelor fizice referitor la prelucrarea datelor cu caracter personal de către autoritățile competente în scopul prevenirii, depistării, investigării sau urmăririi penale a infracţiunilor sau al executării pedepselor şi privind libera circulaţie a acestor date şi de abrogare a Deciziei-cadru 2008/977/JAI a Consiliului, Jurnalul Oficial nr. L 119/89.

[2] Regulamentul (UE) 2018/1725 al Parlamentului European şi al Consiliului din 23 octombrie 2018 privind protecţia persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal de către instituţiile, organele, oficiile şi agenţiile Uniunii şi privind libera circulaţie a acestor date şi de abrogare a Regulamentului (CE) nr. 45/2001 şi a Deciziei nr. 1247/2002/CE, Jurnalul Oficial nr. L 295/49.

siguranță, precum şi privind libera circulație a acestor date[1], prin care este transpusă Directiva nr. 2016/680.

3. Forme de prelucrare a datelor cu caracter personal

Sistemele actuale de inteligența artificială, nu dispun de o gândire şi conştiință proprie, asta înseamnă că nu sunt maşini care gândesc singure. O înțelegere greşită asupra acestor tehnologii, o reprezintă capabilitatea acestora de a depăşii gândire umană. În realitate sistemele de inteligență artificială dezvoltate până în acest moment nu sunt în mod cert inteligente (Surden, 2019). O definiție mult mai simplă pentru acestea ar fi că sunt procesatoare de text, dar cu ajutorul euristicii (prin detectarea unor modele în date şi prin utilizarea cunoştințelor şi informațiilor) prin intermediul unor aproximări computaționale reuşesc să returneze rezultate remarcabile la sarcini complexe, care atunci când sunt realizate de către oameni necesită cunoaştere (Russell & Norvig, 2020). Pentru a oferii aceste rezultate utilizează mecanisme de calcul care nu seamănă cu mecanismele gândirii umane.

AI are un necesare de date exacte, actualizate şi complete, într-o cantitate şi de o calitate ridicată pentru a avea eficacitate şi a returna rezultate exacte. Furnizarea datelor provenit din surse cu un grad scăzut de încredere pot conduce la rezultate eronate (Russell & Norvig, 2020). Datele incomplete sau incorecte pot avea rezultate dezastruoase asupra modelului antrenat.

AI se împarte în două subdomenii principale Machine Learning (ML) şi Deep Learning (DL), cele două utilizând algoritmi complecşi pentru antrenarea datelor pentru a realiza predicții. Algoritmii ML au capabilitatea să învețe modele în date fără o programare prealabilă, pe când DL este un subdomeniu mult mai complex care implică antrenarea unor rețele neuronale profunde cu o multitudine de straturi. Principalele diferențe dintre cele două subdomenii sunt complexitatea şi scara modelelor care pot fi învățate. Algoritmii ML fiind în general cu o simplitate mai ridicată şi necesitând mai puțină putere de calcul decât algoritmii de învățare profundă, rezultatele returnate nu sunt la fel de bune în realizarea unor sarcini complexe (Russell & Norvig, 2020).

Maşinile care gândesc singure şi au abilități ce depăşesc nivelul de cunoaştere al oamenilor sunt numite Strong AI sau Artificial General Intelligence (AGI) – în prezent reprezintă o tehnologie la care încă se lucrează (Surden, 2019). Sistemele cu

[1] Legea nr. 363/2018 din 28 decembrie 2018 privind 363/2018 privind protecția persoanelor fizice referitor la prelucrarea datelor cu caracter personal de către autoritățile competente în scopul prevenirii, descoperirii, cercetării, urmăririi penale şi combaterii infracțiunilor sau al executării pedepselor, măsurilor educative şi de siguranță, precum şi privind libera circulație a acestor date, Monitorul Oficial nr. 13 din data de 7 ianuarie 2019.

inteligenţă artificială disponibile în prezent pe internet, nu dispun de abilităţi umane superioare printre care enumerăm: raţionamentul abstract, înţelegerea unor concepte complexe, înţelegerea flexibilă, abilităţi generale de rezolvare a unor probleme, precum şi alte funcţii care sunt asociate inteligenţei umane.

Două din cele mai importante moduri de indexare a datelor sunt: cuvinte cheie şi metadate. O metodă foarte des întâlnită este metoda cuvintelor cheie, se utilizează un dicţionar de cuvinte cheie pentru a se realiza organizarea datelor. În momentul în care un utilizator doreşte să caute o anumită informaţie, sistemul deja indexat poate răspunde cu uşurinţă cererii utilizatorului. Cea de-a doua metodă, mai puţin utilizată este indexarea bazată pe metadate. Metadatele sunt informaţii suplimentare ale fişierelor, care conţin data şi ora creării, date de identificare ale utilizatorului care a creat fişierul. Sistemele de indexare bazate pe metadate sunt mai eficiente, deoarece în momentul indexării au la dispoziţie mai multe date pentru a realiza o organizare mai relevantă (Russell & Norvig, 2020).

4. **Jurisprudenţă**

Trecând la modul în care se reflectă protecţia juridică a datelor cu caracter personal în practica judiciară, începem prin a prezenta o celebră hotărâre a Curţii Europene a Drepturilor Omului (în continuare, CEDO), Uzun împotriva Germaniei[1], în care reclamantul a criticat faptul că autorităţile au aflat locaţia sa prin utilizarea sistemului GPS, care a folosit alte surse de inteligenţă artificială, precum bazele de date de transport public, într-un mod care aduce o ingerinţă vieţii private. CEDO a considerat că nu a avut loc încălcarea art. 8 din Convenţie privind dreptul la viaţă privată, întrucât întreaga procedură urmărit scopurile legitime de a proteja securitatea naţională, siguranţa publică şi drepturilor victimelor, şi de a preveni săvârşirea de fapte penale. De asemenea, supravegherea prin GPS a fost dispusă numai după ce metode de anchetă mai puţin invazive s-au dovedit insuficiente, s-a desfăşurat pe o perioadă relativ scurtă (de aproximativ trei luni) şi l-a afectat pe reclamant numai atunci când acesta călătorea în autoturismul complicelui său.

Nu la aceeaşi concluzie a ajuns Curtea în cauza Ben Faiza împotriva Franţei, în care a statuat că a fost încălca art. 8, întrucât, deşi autorităţile au urmărit un interes legitim prin utilizarea datelor cu caracter personal în procesul de localizare prin GPS, dreptul francez nu conţineau la vremea respectivă prevederi suficient de clare în privinţa limitei şi modului în autorităţile puteau folosi puterea de apreciere.

În ceea ce priveşte jurisprudenţa Curţii de Justiţie a Uniunii Europene (în continuare, CJUE), identificăm o serie de interpretări obligatorii referitoare la maniera în care

[1] CEDO, Secţia a V-a, Uzun c. Germaniei, 35623/05, Hotărâre din 2 septembrie 2010. Adresă online: https://hudoc.echr.coe.int/eng?i=001-119485.

inteligenţa artificială ar trebui să interacţioneze cu viaţa privată, în special cu datele cu caracter personal, în vederea asigurării unei protecţii juridice cât mai eficiente.

În acest sens, într-o cauză[1], CJUE a statuat că accesul unor autorităţi publice la datele care vizează identificarea titularilor cartelelor SIM activate cu un telefon mobil furat, cum ar fi numele, prenumele şi, dacă este cazul, adresa acestor titulari, implică o ingerinţă în drepturile fundamentale ale acestora din urmă, consacrate la articolele menţionate din Carta drepturilor fundamentale, care nu prezintă o asemenea gravitate încât să fie necesar ca acest acces să fie limitat, în materie de prevenire, de investigare, de detectare şi de urmărire penală a infracţiunilor, la combaterea infracţionalităţii grave. Prin utilizarea inteligenţei artificiale, autorităţile care desfăşoară procedurile de urmărire penală au avut acces la date cu caracter personal păstrate de furnizorii de servicii de comunicaţii electronice. CJUE a considerat că datele vizate de cererea de acces în discuţie în litigiul principal permit doar să se pună în legătură, pe o perioadă determinată, cartela sau cartelele SIM activate cu telefonul mobil furat cu identitatea civilă a titularilor acestor cartele SIM. Fără o verificare încrucişată a datelor aferente comunicaţiilor efectuate cu respectivele cartele SIM şi a datelor de localizare, aceste date nu permit să se cunoască nici data, ora, durata şi destinatarii comunicaţiilor efectuate cu cartela sau cu cartelele SIM în cauză, nici locurile în care aceste comunicaţii au avut loc sau frecvenţa acestora cu anumite persoane într-o perioadă determinată. Prin urmare, aceste date nu permit să se tragă concluzii precise cu privire la viaţa privată a persoanelor ale căror date sunt vizate, pe cale de consecinţă nu există o ingerinţă gravă în viaţa privată a persoanei vizate.

Într-o altă cauză[2], sesizată cu o trimitere preliminară, CJUE a hotărât că dreptul UE se opune unei reglementări naţionale care guvernează protecţia şi securitatea datelor de transfer şi a datelor de localizare şi în special accesul autorităţilor naţionale competente la datele păstrate, fără a limita acest acces, în cadrul combaterii infracţionalităţii, numai la combaterea infracţionalităţii grave, fără a supune respectivul acces unui control prealabil din partea unei instanţe sau a unei autorităţi administrative independente şi fără a impune ca datele în cauză să fie păstrate pe teritoriul Uniunii. Referitor la obligaţiile autorităţilor care prelucrează astfel de date cu caracter personal, trebuie să se ofere o atenţie deosebită anumitor criterii, precum:

[6] CJUE, Marea Cameră, decizie preliminară în urma cererii declanşate de Ministerio Fiscal, C-207/16, Hotărâre din 2 octombrie 2018. Adresă online: https://curia.europa.eu/juris/document/document.jsf?text=&docid=206332&pageIndex=0&doclang=RO&mode=lst&dir=&occ=first&part=1&cid=4147014.

[2] CJUE, Marea Cameră, Tele2 Sverige AB împotriva Post- och telestyrelsen, şi Secretary of State for The Home Departament împotriva Tom Watson, cauze conexate C-203/15 şi C-698/15, Hotărâre din 21 decembrie 2016. Adresă online: https://eur-lex.europa.eu/legal-content/RO/TXT/HTML/?uri=CELEX:62015CJ0203.

cantitatea datelor păstrate, caracterul sensibil al respectivelor date, riscul de acces ilicit la acestea. De asemenea, reglementarea națională trebuie să prevadă păstrarea pe teritoriul Uniunii, precum și distrugerea iremediabilă a datelor la finalul duratei de păstrare a acestora.

5. Drept comparat

În această secțiune vom face trimiteri la legislația statelor europene și la doctrina europeană din perspectiva protecției datelor cu caracter personal la intersectarea acestora cu inteligența artificială.

În acest sens, Suedia a centralizat informațiile personale din toate cazierele judiciare de pe teritoriul statului într-un registru național, care poate fi accesat de orice persoană prin simpla inserare a numelui persoanei. Dacă acest registru a existat încă din 1901, recent a fost digitalizat, în scopul sporirii transparenței (Backman, 2011, p. 111). Însă, este interesant aspectul că nici după intrarea în vigoare a GDPR-ului, acest registru nu a suferit modificări sub aspectul accesibilității informațiilor. Acum se poate ridica întrebarea dacă o astfel de transparență este în conformitate cu rigorile regulamentului și cu principiile transmise de acesta. Considerăm că acest sistem va intra în atenția CJUE la o eventuală trimitere preliminară, întrucât modul în care funcționează intră în directă conexiune cu domeniul de aplicare al regulamentului.

Pe tărâm german, chestiunea datelor cu caracter personal este privită ca intrând în competența exclusivă a UE, în considerarea faptului că s-a recurs la forța juridică a unui regulament, și nu la flexibilitatea pe care o poate oferi o directivă sub aspectul posibilității alegerii mijloacelor pentru a ajunge la un rezultat final comun în toate statele membre. De altfel, se apreciază că autoritățile naționale nu ar trebui să se implice într-o atât de mare măsură în acest domeniu, deoarece este o îndatorire personală a individului care utilizează serviciile platformelor care apelează la inteligența artificială de a fi diligent în transmiterea acestor date, asigurându-se că datele sunt securizate (Dimmroth & Schunemann, 2017, pp. 104-105). Dar această viziune politică asupra protecției datelor cu caracter personal nu înseamnă o indiferență practică sub aspect instituțional, întrucât, în baza GDPR-ului, statele sunt obligate să înființeze o autoritate competentă în supravegherea modului în care sunt respectate dispozițiile regulamentului (Bolognini, Bistolfi, & Ziegler, 2019, p. 148)

În ceea ce privește impactul inteligenței artificiale asupra procedurilor judiciare, state precum Austria, Grecia, Finlanda și Belgia au adoptat măsura anonimizării pe platformele online care fac publice informații privind obiectul judecății, coordonatele temporare ale desfășurării procedurii (Lambert, 2018, p. 204), în timp

ce în România se pot afla astfel de informaţii doar dacă este inserat numărul dosarului[1].

În Italia a fost blocatul accesul la ChatCPT în martie 2023 (Kreitmeir & Raschky, January, 2023), un chatbot dezvoltat de compania OpenAI, pentru încălcarea legislaţiei europene privind protecţia datelor. Acesta colecta şi totodată stoca datele personale ale utilizatorilor fără consimţământul acestora. Nu avea implementat nici un sistem de verificare a vârstei utilizatorului în momentul accesări platformei. OpenAI a suferit şi un incident de securitate în care conversaţiile utilizatorilor şi informaţiile aferente plăţilor făcute de aceştia către platformă au ajuns în mâinile hackerilor. Restricţia a fost ridicată în aprilie 2023, după adaptarea acestuia la legislaţia în vigoare. Într-un articol realizat de Kreitmeier şi Raschky în 2023, aceştia au analizat comportamentul utilizatorilor de internet din Italia şi au observat o creştere în utilizarea VPN-urilor (Virtual Private Network) şi a aplicaţiei Tor (browser ce oferă o anonimitate sporită) pentru a ocoli interdicţia. O altă observaţie făcută de cei doi autori a fost că deşi restricţia de acces la platformă, a fost bine intenţionată a scăzut productivitatea de scurtă durată.

6. Concluzii

Scopul acestei lucrări a fost de a oferii o imagine de ansamblu şi totodată una realistă, o descifrare a fenomenului AI şi a legislaţiei din jurul acestuia. Tehnologia AI dezvoltată până în prezent şi disponibilă pentru publicul larg, nu este o inteligenţă în sensul de bază al cuvântului, neavând conştiinţă (Russell & Norvig, 2020). Această tehnologie este capabilă să producă răspunsuri, fără factorul principal inteligenţă, prin utilizarea corespunzătoare a unor modele matematice ce îi permit să ia decizii în anumite contexte destul de restrânse.

Cu toate acestea, tehnologia actuală are limitele sale. Nu se descurcă foarte bine la tratarea abstracţiunilor, la înţelegerea unor semnificaţii şi la transferul de cunoştinţe de la o activitate la alta. Domenii în care excelează AI (şah, detectare tumorilor, frauda cu cărţi de credit) sunt domenii cu o structură foarte clară, în care există reguli puternice, iar modele care stau la bază pot fi detectate algoritmic (Russell & Norvig, 2020).

Cunoaşterea punctelor forte şi a celor slabe în privinţa noilor tehnologi care au la bază inteligenţa artificială, ajută la o înţelegerea mai bună a aspectelor privind prelucrare datelor cu caracter personal de către astfel de platforme.

[1] Portal just https://portal.just.ro/SitePages/jurisprudenta.aspx. Accesat la data de 08.08.2023.

Protecţia datelor cu caracter personal în cadrul platformelor dezvoltate în jurul tehnologiilor ce utilizează inteligenţa artificială reprezintă un subiect de preocupare primordială. Atât pentru autorităţi (în special autorităţile de supraveghere privind gestionarea cu datele personale), cât şi pentru operatorii platformelor în încercarea de a ţine aceste platforme la zi cu modificările legislative ce au loc în acest domeniu (Surden, 2019).

Legislaţia naţională şi cea europeană oferă garanţii atunci când vine vorba de protecţia datelor cu caracter personal, acestea se aplică şi platformelor dezvoltate pe baza inteligenţei artificiale. Garanţiile includ, printre altele: principiul transparenţei, principiul limitării scopului, principiul integrităţii şi confidenţialităţii, precum şi dreptul de acces la date, dreptul la rectificarea a acestora şi dreptul de ştergere a acestora.

Mai mult, legislaţia europeană conţine o serie de măsuri specifice privind datele cu caracter personal în utilizarea acestora în cadrul inteligenţei artificiale, precum obligaţia de a realiza o analiză de impact asupra prelucrării a datelor cu caracter personal, obligaţia de a asigura măsurii tehnice şi organizatorice adecvate pentru a proteja aceste date şi obligaţia de a respecta principiul responsabilităţii (Dimmroth & Schunemann, 2017).

Autorităţile de supraveghere au un rol important de jucat în asigurarea respectării drepturilor persoanelor vizate, atunci când datele cu caracter personal sunt prelucrate prin intermediul platformelor dezvoltate pe baza inteligenţei artificiale. Aceste autorităţi au competenţa de a investiga şi posibilitatea de a sancţiona companiile care încalcă legislaţia în vigoare.

În concluzie, protejarea datelor cu caracter personal în cadrul platformelor dezvoltate în jurul inteligenţei artificiale reprezintă o sarcină complexă care necesită o abordare multidisciplinară. Autorităţile de supraveghere, operatorii şi persoanele vizate joacă un rol important în asigurarea respectării drepturilor şi libertăţilor persoanelor vizate de prelucrarea datelor ce se realizează prin intermediul acestor platforme.

7. References

Backman, C. (2011). Regulating Privacy: Vocabularies of Motive in Legislating Right of Access to Criminal Records in Sweden. In S. Gutwirth, Y. Poullet, P. De Hert, & R. Leenes, *Computers, Privacy and Data Protection: an Element of Choice* (p. 111). London: Springer.

Bolognini, L., Bistolfi, C., & Ziegler, S. (2019). Voluntary Compliance Commitment Tool for European General Data Protection Regulation. *Internet of Things Security and Data Protection*, 148.

Bostrom, N. (2014). *Superintelligence: Paths, Dangers, Strategies.* Mureş: University Press.

Dimmroth, K., & Schunemann, W. (2017). The Ambiguous Relation Between Privacy and Security in German Cyber Politics. A Discourse Analysis of Governmental and Parliamentary Debates. *Privacy, Data Protection and Cybersecurity in Europe*, 104-105.

Kreitmeir, D., & Raschky, P. A. (January, 2023). The Unintended Consequences of Censoring Digital Technology - Evidence from Italy's ChatGPT Ban. *Social Science Research Network*. doi:https://doi.org/10.2139/ssrn.4422548

Lambert, P. (2018). *Understanding the New European Data Protection Rules*. Boca Raton: CRC Press.

Russell, S., & Norvig, P. (2020). *Artificial Intelligence: A Modern Approach (4th ed.)*. London: Pearson.

Schünemann, W. J., & Baumann, M.-O. (2017). *Privacy, Data Protection and Cybersecurity in Europe*. London: Springer EBooks. From https://doi.org/10.1007/978-3-319-53634-7

Surden, H. (2019). *Artificial Intelligence and Law: An Overview*. Georgia: Georgia State University Law. From https://readingroom.law.gsu.edu/cgi/viewcontent.cgi?article=2981&context=gsulr.

CEDO, Secţia a V-a, Uzun c. Germaniei, 35623/05, Hotărâre din 2 septembrie 2010/ ECHR, Fifth Section, Uzun v. Germany, 35623/05, Judgment of 2 September 2010. https://hudoc.echr.coe.int/eng?i=001-119485.

CJUE, Marea Cameră, decizie preliminară în urma cererii declanşate de Ministerio Fiscal, C-207/16, Hotărâre din 2 octombrie 2018/ CJEU, Grand Chamber, preliminary ruling following the request brought by the Ministerio Fiscal, C-207/16, Judgment of 2 October 2018. https://curia.europa.eu/juris/document/document.jsf?text=&docid=206332&pageIndex=0&doclang=RO&mode=lst&dir=&occ=first&part=1&cid=4147014

CJEU, Grand Chamber, Tele2 Sverige AB v Post- och telestyrelsen, and Secretary of State for The Home Department v Tom Watson, Joined Cases C-203/15 and C-698/15, Judgment of 21 December 2016. https://eur-lex.europa.eu/legal-content/RO/TXT/HTML/?uri=CELEX:62015CJ0203.

Directiva (UE) 2016/680 a Parlamentului European şi a Consiliului din 27 aprilie 2016 privind protecţia persoanelor fizice referitor la prelucrarea datelor cu caracter personal de către autorităţile competente în scopul prevenirii, depistării, investigării sau urmăririi penale a infracţiunilor sau al executării pedepselor şi privind libera circulaţie a acestor date şi de abrogare a Deciziei-cadru 2008/977/JAI a Consiliului, Jurnalul Oficial nr. L 119/89/ Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, detection, investigation or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA, Official Journal No. L 119/89.

Regulamentul (UE) 2018/1725 al Parlamentului European şi al Consiliului din 23 octombrie 2018 privind protecţia persoanelor fizice în ceea ce priveşte prelucrarea datelor cu caracter personal de către instituţiile, organele, oficiile şi agenţiile Uniunii şi privind libera circulaţie

a acestor date şi de abrogare a Regulamentului (CE) nr. 45/2001 şi a Deciziei nr. 1247/2002/CE, Jurnalul Oficial nr. L 295/49/ Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC, Official Journal No L 295/49.

Regulamentul (UE) 2016/679 al Parlamentului European şi al Consiliului din 27 aprilie 2016 privind protecţia persoanelor fizice în ceea ce priveşte prelucrarea datelor cu caracter personal şi privind libera circulaţie a acestor date şi de abrogare a Directivei 95/46/CE, Jurnalul Oficial nr. L 119/1/ Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC, Official Journal No. L 119/1/..

Legea nr. 363/2018 din 28 decembrie 2018 privind 363/2018 privind protecţia persoanelor fizice referitor la prelucrarea datelor cu caracter personal de către autorităţile competente în scopul prevenirii, descoperirii, cercetării, urmăririi penale şi combaterii infracţiunilor sau al executării pedepselor, măsurilor educative şi de siguranţă, precum şi privind libera circulaţie a acestor date, Monitorul Oficial nr. 13 din data de 7 ianuarie 2019/ Law No. 363/2018 of 28 December 2018 on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of preventing, detecting, investigating, prosecuting and combating criminal offences or the execution of penalties, educational and security measures, and on the free movement of such data, Official Monitor No. 13 of 7 January 2019.

Portal just https://portal.just.ro/SitePages/jurisprudenta.aspx. Accessed on 08.08.2023.