UNIVERSITATEA ECOLOGICĂ DIN BUCUREŞTI

FACULTATEA DE DREPT

Program de studii universitare de master

Dreptul inteligenței artificiale (DIA)

Forma de învăţământ: ***cu frecvenţă***

-suport de curs-

Inteligenţa artificială (IA) şi Dreptul protecţiei datelor cu caracter personal

Conf.univ.dr. Aurelian Gherghe

Inteligenţa artificială (IA) şi Dreptul protecţiei datelor cu caracter personal

Capitolul 1

Considerații introductive privind protecția datelor cu caracter personal și inteligența artificială

Capitolul 2

Conceptul de date cu caracter personal și libera circulație a acestor date

Capitolul 3

Principiile protecției datelor cu caracter personal

Capitolul 4

Drepturile persoanelor vizate privind protecția datelor cu caracter personal și inteligența artificială

Capitolul 5

Provocări specifice inteligenței artificiale în aplicarea principiilor RGPD

Capitolul 6

Considerații generale privind riscurile utilizării sistemelor de inteligența artificială(IA)

Capitolul 1

Considerații introductive privind protecția datelor cu caracter personal și inteligența artificială

Cadrul legal al protecției datelor cu caracter personal și a liberei circulații a acestor date în Uniunea Europeană a cunoscut o dezvoltare semnificativă în decursul ultimilor ani, odată cu intrarea în vigoare a *Regulamentului general privind protecția datelor* (RGPD). Din punct de vedere al evoluției tehnologice moderne, a fost necesară impunerea unui *Regulament* care să creeze un context unitar de aplicare a normelor privind protecția datelor, la nivel european. În contextul digitalizării afacerilor și al schimbului de informații în Uniunea Europeană, protecția datelor personale a devenit un aspect crucial al reglementărilor și legislației în dreptul Uniunii Europene.

Inteligența artificială (IA) a revoluționat într-o manieră extrem de rapidă modul în care sunt colectate, procesate și analizate datele cu caracter personal, oferind beneficii semnificative în diverse domenii, de la sănătate și educație, la comerț și securitate.

Inteligența artificială (IA) reprezintă un concept care descrie un sistem informatic care are capacitatea de a prelucra o cantitate de informații, a crea modele, tipare, categorii, etc., în baza cărora poate genera *concluzii* ori poate dobândi *capacitatea de a lua decizii*. Cu alte cuvinte, sistemele informatice bazate pe tehnologiile de *inteligență artificială* (IA) au ca *scop* simularea gândirii umane.

Cu toate acestea, utilizarea *inteligenței artificiale* (IA) implică *o serie de riscuri* privind protecția datelor cu caracter personal, precum *discriminarea,*

crearea de profiluri, lipsa de transparență și *lipsa de responsabilitate* a operatorului de date.

Regulamentul General privind Protecția Datelor (RGPD), cunoscut și ca GDPR (*General Data Protection Regulation*), reprezintă unul dintre cele mai importante acte legislative în domeniul protecției datelor cu caracter personal în Uniunea Europeană.

Regulamentul General privind Protecția Datelor (RGPD) reglementează în principal, obligațiile operatorilor de date cu caracter personal și persoanelor împuternicite de operator în raport cu drepturile persoanelor vizate, atunci când datele acestora sunt prelucrate de cei dintâi.

Intrat în vigoare la data de *25 mai 2018*, RGPD stabilește un set de *principii fundamentale* care ghidează prelucrarea datelor personale, având ca scop protejarea drepturilor și libertăților fundamentale ale persoanelor fizice, precum și asigurarea unei abordări uniforme la nivel european. Cu alte cuvinte, *Regulamentul General privind Protecția Datelor* (RGPD) oferă un cadru legal care asigură prelucrarea datelor într-un mod *echitabil* și *responsabil*.

Principiile de bază ale *Regulamentului General privind Protecția Datelor* (UE) nr.679/2016 le regăsim în *art.5*:

-principiul *legalității*, *echității* și *transparenței*;

- principiul *limitării prelucrării* datelor cu caracter personal;

- principiul *reducerii la minim a datelor*;

- principiul *exactității* datelor cu caracter personal;

- principiul *limitării legate de perioada de stocare*;

- principiul *integrității si confidentialității*;

- principiul *responsabilității operatorului de date*;

Acest *suport de curs* abordează principiile *Regulamentului General privind Protecția Datelor* (RGPD) din perspectiva utilizării *inteligenței artificiale* (IA), analizând atât provocările, cât și soluțiile practice pentru conformitate și totodată își propune să analizeze principalele principii prevăzute de RGPD dintr-o perspectivă teoretică, cu referire la articolele specifice din regulament, și să discute aplicabilitatea lor practică, ilustrând cu exemple relevante din jurisprudență sau din activitatea instituțiilor publice și private în raport cu reglementările făcute odată cu apariția *inteligenței artificiale* (AI).

Capitolul 2

Conceptul de date cu caracter personal și libera circulație a acestor date

Conceptul de *confidențialitate*, ca drept al persoanelor fizice, s-a maturizat în secolul al XIX-lea, când au început să apară legi legate de confidențialitate, în Franța și Germania, legând necesitatea protejării acesteia de noțiunea de autonomia individuală, adică demnitatea umană și onoarea în sens mai larg, percepute ca valori fundamentale. Crearea unor protecții juridice explicite a fost determinată de evoluția mijloacelor de comunicații, prin liberalizarea și creșterea presei. Directiva 95/46/CE, adoptată în UE în anii 1990, a devenit un stabilizator global de standarde în protecția vieții private, încorporând o abordare bazată pe drepturile persoanelor vizate. Acest instrument pentru promovarea dreptului la confidențialitate a luat naștere ca un instrument de creare a pieței. Regulamentul general privind protecția datelor reprezintă o actualizare a Directivei 95/46/CE, pe o piață unică deja stabilizată. Abordarea istorică neo-instituţionalistă, care urmărește parcursul reglemetărilor de confidențialitate și protecție a datelor, se concentrează pe contextul temporal în care este vizibil impactul deciziilor politice anterioare asupra celor ulterioare. Geneza drepturilor fundamentale în UE și modul în care acestea au fost modelate reprezintă interesele strategice ale diferiților actori cu intere în domeniu. Se dezvăluie, astfel, modul în care evoluția drepturilor la viața privată și protecția datelor a fost prinsă între dezvoltarea instituțională a UE,

interesele celor implicați și procesul unic de constituționalizare a drepturilor omului în UE[1].

Conceptul de *date cu caracter personal* reprezintă informațiile care se referă la o persoană identificată, sau care pot duce la identificarea unei persoane vizate. Astfel, toate aceste date sunt vizate de Regulamentul general privind protecția datelor, dacă acestea sunt prelucrate în mod automat, indiferent de tehnologia folosită, sau manual, daca prelucrarea se face în baza unor criterii predefinite[2].

Datele cu caracter personal pot fi atât numele unei persoane fizice, adresa de e-mail, numărul unic de identificare, dar și adresa de protocol de Internet (IP), identificatori de modul cookie sau de publicitate. De asemenea, rămân sub auspiciile RGPD datele care au fost anonimizate, criptate sau pseudonimizate, dacă acestea pot fi folosite pentru reidentificarea personei vizate.

Prelucrarea *datelor cu caracter personal* se referă la orice activitate efectuată asupra acestor date, precum colectarea, înregistrarea, organizarea, structurarea, stocarea, modificarea sau ștergerea datelor. Prelucrarea datelor este efectată de către un operator de date sau de către persoana împuternicită de către operatorul de date, conform RGPD.

Mai mult, datele sensibile au parte, conform RGPD, de protecție suplimentară, deoarece acestea vizează date sensibile cu privire la aspecte private ale vieții unei persoane, precum informațiile medicale, genetice, orientarea sexuală, opiniile politice sau religioase, apartenența etnică sau rasială, condamnări penale

---

[1] Ronald Leens, Rosamunde van Brakel, Serge Gutwirth&Paul de Hert, *"Data Protection and Privacy – The Age of Intelligent Machines"*, Hart Publishing, 2017, p. 1 și urm.

[2] Termenul *"criterii predefinite"*, în contextual prelucrării datelor cu caracter personal, se referă la seturile de reguli, instrucțiuni sau parametri stabiliți anterior în cadrul unui algoritm sau sistem informatic pentru a lua decizii automate în legătură cu persoanele vizate

sau datele genetice. Artiolul 9 al RGPD stabilește condițiile de prelucrare ale datelor cu caracter sensibil, care este interzisă fără a obține consimțământul explicit al persoanei, în cazul în care necesitatea prelucrării nu implică măsuri de securitate națională sau protejarea intereselor vitale ale persoanei. Mai mult, pe lângă consimțământul explicit al persoanei vizate, se implementează și alte măsuri de ordin tehnic și organizatoric pentru securitatea sporită a datelor, precum criptarea datelor, restricționarea accesului la seturile de date sau autentificarea în doi factori.

Criptarea datelor presupune convertirea informațiilor, prin folosirea unui algoritm matematic și a unei chei, într-un text cifrat. Descifrarea textului se poate face folosind cheia criptografică. Aceasta poate fi o secvență sau o combinație de caractere și numere. Prin folosirea criptării datelor, confidențialitatea acestora este protejată împotriva accesului neautorizat. De asemenea, se poate verifica integritatea setului de date.

Libera circulație a datelor cu caracter personal este un principiu care se referă la garantarea faptului că datele pot fi transferate liber în interiorul Uniunii Europene și în afara ei, fără a fi impuse restricții nejustificate. Principiul este de a se permite realizarea unui mediu de afaceri competitiv care respectă în același timp protecția datelor cu caracter personal.

Capitolul 3
Principiile protecției datelor cu caracter personal

Regulamentul general privind protecția datelor stabilește principiile generale, care stau la baza unei prelucrări adecvate a prelucrării datelor cu caracter personal. Acestea reprezintă bazele abordării privind protecția datelor, și punctul de plecare al dispozițiilor Regulamentului. În ceea ce privește nerespectarea acestor principii, art. 83 din RGPD prevede că o astfel de încălcare a normelor impune cel mai ridicat nivel de amendă administrativă. În cazul protecției datelor, aceasta se ridică la suma de 20 milioane Euro, respectiv 4% din cifra de afaceri totală anuală[3].

Principiul prelucrării datelor în mod legal, echitabil și transparent se respectă în practicile RGPD prin informarea persoanelor vizate cu privire la scopul și modul de prelucrare a datelor cu caracter personal. Pentru ca prelucrarea să fie efectuată în mod echitabil, operatorii trebuie să se asigure că datele obținute provin dintr-o sursă autorizată să le colecteze și că datele sunt gestionate în mod rezonabil, evitând potențialele efecte negative asupra persoanelor vizate. Transparența este esențială în informarea persoanelor vizate despre orice prelucrare a datelor cu caracter personal ale acestora. În continuare, legalitatea datelor prelucrate reprezintă un domeniu complex. Majoritatea companiilor apelează la

[3] Daniel-Mihail Șandru, Principiile protecţiei datelor – de la teorie la practică, Curierul Judiciar, nr. 6/ 2018, pp. 364-366

consiliere juridică în privința acestui aspect, deoarece o bază legală a prelucrării este necesară, conform RGPD[4].

Colectarea în scop limitat a datelor cu caracter personal are ca scop prelucrarea într-un mod legitim a datelor și interzicerea prelucrării ulterioare, într-un alt scop decât cel menționat inițial, cu excepția arhivării în interes public, în scopul cercetării științifice sau statistice. Notificările de confidențialitate, termenii și condițiile și formularele de consimțământ trebuie să ofere persoanei vizate informații clare despre prelucrarea implicată, astfel încât scopul prelucrării să fie înțeles. De exemplu, multe supermarketuri colectează date personale, astfel încât să poată oferi clienților oferte care se potrivesc cel mai bine cu obiceiurile lor în materie de cumpărături uzuale. În cazul în care acele supermarketuri transmit aceste date unei alte companii, scopul ar fi diferit față de scopul pentru care datele au fost colectate inițial, iar principiul colectării în scop limitat ar fi încălcat[5].

Principiul reducerii la minimum a datelor privește limitarea cantității datelor în raport direct cu necesitatea prelucrării acestora, prin eliminarea oricăror seturi de date irelevante, prin raportare la scopul prelucrării. Datele cu caracter personal trebuie să fie adecvate, relevante și limitate în raport cu scopurile pentru care sunt prelucrate. De asemenea, criteriul necesității se referă și la perioada pentru care datele cu caracter personal sunt stocate[6].

Respectarea ***principiului exactității datelor*** presupune actualizarea acestora și rectificarea sau ștergerea eventualelor date inexacte. Responsabilitatea datelor

---

[4] *"Eu General Data Protection Regulation (GDPR) – An implementation and Compliance Guide",* Ediția a 4-a, IT Governance Publishing, 2020, pp. 43-50

[5] *"Eu General Data Protection Regulation (GDPR) – An implementation and Compliance Guide", op.cit., pp. 50-51*

[6] Christopher Kuner, Lee A. Bygrave, Christopher Docksey, *"The Eu General Data Protection Regulation (GDPR) – A commentary",* Oxford University Press, Oxford, 2020, p. 317

corecte este a organizațiilor care prelucrează date cu caracter personal. De asemenea, persoanele vizate pot să își exercite dreptul la rectificare sau la ștergere ("dreptul de a fi uitat"). Toate datele inexacte trebuie rectificate sau șterse. Operatorul de date trebuie să ia toate măsurile rezonabile pentru a asigura respectarea acestui principiu. GDPR clarifică faptul că această intervenție trebuie făcută fără nicio întârziere nejustificată.

Principiul limitării legate de stocare se referă la păstrarea datelor pe perioada strict necesară îndeplinirii scopului sau scopurilor în care acestea au fost prelucrate, cu excepția arhivării în interes public, în scopul cercetării științifice sau statistice. Minimizarea datelor ar trebui, de asemenea, luată în considerare în ceea ce privește acordurile cu furnizorii de date, incluzând eliminarea anumitor date înainte de a transmite informații pentru procesare externă. Asigurarea minimizării datelor ar trebui inclusă în regulile corporatiste obligatorii, în procedurile de achiziții și aprovizionare[7].

Principiul integrității și confidențialității presupune ca organizațiile care prelucrează date cu caracter personal să ia măsuri tehnice și organizatorice adecvate pentru a asigura protecția datelor împotriva prelucrărilor neautorizate, a pierderii sau a distrugerii. Securitatea datelor include obligația de a notifica încălcările datelor cu caracter personal către autoritatea de supraveghere națională și, în anumite cazuri, persoanelor vizate[8].

[7] *"Eu General Data Protection Regulation (GDPR) – An implementation and Compliance Guide", op.cit., pp. 51-53*

[8] Christopher Kuner, Lee A. Bygrave, Christopher Docksey, op.cit., p. 318

Capitolul 4

Drepturile persoanelor vizate privind protecția datelor cu caracter personal și inteligența artificială

Un aspect important al noilor reglementări privind protecția sunt *drepturile persoanelor vizate*. Capitolul III al RGPD stabilește *drepturile persoanelor vizate privind protecția datelor*. Aceștia au posibilitatea să le ceară organizațiilor să își exercite oricare dintre drepturi, printr-o cerere scrisă, sau comunicare verbală. Deși drepturile privind protecția datelor cu caracter personal nu sunt absolute, organizațiile trebuie să aibă motive întemeiate pentru a refuza exercitarea acestora.

Primul drept prevăzut de RGPD este *dreptul la informare al persoanelor vizate*, în cadrul art. 13 și 14 din Capitolul III RGPD, Secțiunea 2: Informare și acces la date cu caracter personal. Persoanele vizate ale căror date cu caracter personal au fost prelucrate de o organizație au dreptul de a li se transmite identitatea și datele de contact ale operatorului și ale responsabilului cu protecția datelor, precum și scopul prelucrării, categoriile de date, destinatarii sau categoriile de destinatari.

În continuare, art. 15 din Capitolul III RGPD prevedere *dreptul de acces al persoanei vizate.* Accesul se referă la confirmarea sau infirmarea prelucrării datelor de către un operator. În cazul în care prelucrarea se confirmă, persoana vizată are dreptul de a accesa aceste date și de a obține orice informații suplimentare, precum scopul în care aceste date au fost prelucrate, categoriile de date care au fost

prelucrate, destinatarii, dar și perioada de stocare și criteriile care au fost folosite pentru a determina perioada respectivă, cât și alte informații relevante. În ceea ce privește procedurile de informare ale persoanei vizate, organizațiile folosesc un limbaj cât mai simplu, transparent și concis, pentru a evita riscul unor eventuale confuzii.

Mai mult, există operatori care prelucrează date din *motive de interes public*. Autoritățile competente în scopul prevenirii, cercetării, urmăririi penale și combaterii infracțiunilor prelucrează date personale pentru a asigura ordinea și siguranța publică. În acest sens, operatorii pot amâna furnizarea de informații, la cerere, către persoanele vizate, pentru evitarea obstrucționării procesului penal sau a urmăririi penale, precum și în cazul în care informațiile sunt necesare pentru protejarea ordinii și siguranței publice, a securității naționale sau a drepturilor și libertăților celorlalți[9].

Secțiunea 3 a Capitolului III RGPD stabilește *normele de rectificare și ștergere a datelor cu caracter personal*. În acest sens, art. 16 RGPD prevede faptul că persoana vizată poate obține rectificarea datelor inexacte sau completarea datelor incomplete. În cel de-al doilea caz, completarea datelor de către operator se poate face inclusiv prin transmiterea, de către persoana vizată, a unor informații suplimentare.

În continuare, dreptul la ștergerea datelor, sau "dreptul de a fi uitat", oferă persoanelor vizate posibilitatea de a cere ștergerea datelor cu caracter personal care îi privesc. Acest drept se aplică, fără întârzieri nejustificate, dacă datele respective

[9] Art. 15 din *Legea nr. 363 din 28 decembrie 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*

nu mai sunt necesare pentru îndeplinirea scopurilor pentru care au fost prelucrate, sau dacă prelucrarea a fost făcută în mod ilegal. De asemenea, persoana vizată își poate retrage consimțământul pentru prelucrarea datelor cu caracter personal, sau se poate opune prelucrării. Există anumite situații în care ștergerea datelor nu este posibilă, și anume din motive de interes public sau, în scopuri de arhivare, statistice, sau pentru cercetare științifică.

Restricționarea prelucrării datelor cu caracter personal reprezintă o alternativă a ștergerii datelor și se poate aplica în cazul în care ștergerea definitivă nu este posibilă sau, sub auspiciile obligației de arhivare a datelor sau în scopuri statistice, aceasta se va face ulterior cererii. În acest sens, operatorul ia măsurile necesare pentru a restricționa datele, iar acestea vor putea fi folosite, cu excepția stocării, doar cu consimțământul persoanei vizate, sau în vederea exercitării unui drept în instanță[10].

Secțiunea 4 a Capitolului III RGPD stabilește *normele privind dreptul la opoziție și procesul decizional individual automatizat* al persoanelor vizate. *Dreptul la opoziție*, prevăzut de art. 21, prevede faptul că persoanele vizate au dreptul de a se opune prelucrării, spre exemplu, în cazul în care datele sunt folosite pentru marketingul direct[11].

[10] Dacă datele cu caracter personal sunt restricționate, acestea sunt păstrate într-o stare inactivă, fără a fi șterse complet sau eliminate din sistemul de stocare. Aceasta poate fi o măsură temporară sau permanentă, în funcție de circumstanțele specifice și de cerințele legale aplicabile

[11] Colectarea și utilizarea informațiilor personale ale clienților și potențialilor clienți este o practică comună în campaniile de marketing. Companiile trebuie să obțină consimțământul explicit al clienților înainte de a le colecta și utiliza datele personale în scopuri de marketing direct. Utilizatorii trebuie să fie informați în mod clar și transparent cu privire la modul în care datele lor vor fi utilizate și să aibă opțiunea de a refuza

Dreptul de a nu face obiectul unei decizii bazate exclusiv pe prelucrarea automată, inclusiv crearea de profiluri, este aplicabil dacă o astfel de prelucrare poate produce efecte juridice care privesc persoanele vizate.

În final, persoanele vizate au dreptul de a depune o *plângere* la Autoritatea Națională de Supraveghere a Prelucrării Datelor cu Caracter Personal (ANSPDCP), prevăzut de art. 77 RGPD, prin completarea formularului pus la dispoziție pe Website-ul instituției. În Uniunea Europeană, fiecare țară are propria sa autoritate de supraveghere a datelor cu caracter personal, responsabilă cu aplicarea legislației privind protecția datelor. EDPB este organul de coordonare și cooperare între autoritățile de supraveghere din UE. Acesta oferă orientări și asistență în interpretarea și aplicarea Regulamentului General privind Protecția Datelor în întreaga Uniune Europeană[12].

Prin implementarea prevederilor RGPD privind drepturile persoanelor vizate, UE a dorit crearea unei noi culturi a protecției datelor cu caracter personal în statele membre, dar și în cadrul companiilor care prelucrează datele cetățenilor UE. În acest sens, în centru se află dorința de a oferi un control sporit persoanelor vizate asupra datelor lor și a modului în care acestea sunt folosite, prin promovarea transparenței activităților de prelucrare și consolidarea încrederii între persoane și instituțiile Uniunii.

[12] Laima Jančiūtė, "European Data Protection Board: a nascent EU agency or an 'intergovernmental club'?", în *"International Data Privacy Law",* Vol. 10, Issue 1,2020, pp. 57–75

Capitolul 5

Provocări specifice inteligenței artificiale în aplicarea principiilor RGPD

Implementarea *principiilor* RGPD în contextul inteligenței artificiale (IA) este adesea marcată de provocări specifice, determinate de natura complexă și dinamică a tehnologiei. Deși IA oferă soluții inovatoare pentru prelucrarea datelor, aceasta ridică probleme unice care necesită soluții adaptate.

O provocare majoră este legată de *deciziile automate și profilare*, aspect reglementat de articolul 22 din RGPD. Acesta garantează dreptul persoanelor vizate de a nu fi supuse unor decizii automate care produc efecte juridice semnificative asupra lor. În cazul IA, utilizarea algoritmilor pentru selecția automată a candidaților pentru un loc de muncă sau pentru acordarea unui credit bancar poate avea un impact profund asupra drepturilor persoanelor. De exemplu, un algoritm poate exclude un candidat pe baza unui model de date care reflectă prejudecăți istorice sau statistice. Soluția propusă de legislație și de bunele practici este introducerea unei intervenții umane în procesul decizional, astfel încât să se garanteze o analiză echitabilă și contextualizată.

Un alt obstacol semnificativ este *riscul reidentificării datelor anonimizate*. Deși RGPD încurajează utilizarea datelor anonimizate pentru reducerea riscurilor de confidențialitate, metodele avansate de procesare utilizate de IA pot permite reidentificarea datelor prin corelarea informațiilor din surse multiple. De exemplu, în cazul unui algoritm utilizat pentru cercetări medicale, datele despre pacienți pot fi reidentificate prin combinarea cu alte baze de date publice. Pentru a contracara acest risc, operatorii pot recurge la tehnici avansate de pseudonimizare sau anonimizare dinamică, care îngreunează semnificativ reidentificarea.

Interoperabilitatea normativă reprezintă o altă provocare de amploare, mai ales pentru organizațiile internaționale care operează în diverse jurisdicții. De exemplu, companiile trebuie să asigure conformitatea simultană cu RGPD în Uniunea Europeană și cu reglementări precum California Consumer Privacy Act (CCPA) în Statele Unite. Acest lucru creează dificultăți, deoarece cerințele diferitelor regimuri legale pot fi contradictorii sau greu de armonizat. În acest context, o soluție viabilă este crearea unor echipe multidisciplinare care să includă experți juridici și tehnici, capabili să dezvolte politici compatibile cu cerințele internaționale.
Concentrat asupra managementului și controlului datelor, Regulamentul general privind protecția datelor accentuează importanța securității cibernetice, neimpunând, totuși, modalități exacte – din punct de vedere tehnic – cu privire la modul în care organizațiile ar trebui să își protejeze datele. În schimb, în temeiul art. 32, Regulamentul prevede că operatorii și persoanele împuternicite de operator au obligația de a "implementa măsuri tehnice și organizatorice adecvate", ținând seama de "starea actuală și costurile de implementare" și de "natura, domeniul de aplicare, contextul și scopurile prelucrarea, precum și riscul de probabilitate și severitate variabile pentru drepturile și libertățile persoanelor fizice.

În schimb, oferă câteva sugestii cu privire la tipul de apărare care ar trebui folosit, inclusiv *pseudonimizarea* și *criptarea datelor*, asigurarea confidențialității și integrității datelor, restabilirea disponibilității datelor în cazul unui accident tehnic și existența unui proces de evaluare periodică a eficienței măsurilor tehnice și organizatorice pentru asigurarea securității prelucrării.

În conformitate cu art. 31 din RGPD, operatorul, persoana împuternicită de operator și reprezentanții acestora cooperează cu autoritățile de supraveghere naționale. În conformitate cu art. 30, este necesar să se păstreze evidențele ale

activităților de prelucrare de date personale și să le pună la dispoziția autorităților de supraveghere, la cerere[13].

În cazul unei încălcări a securității datelor, organizațiile sunt obligate să notifice Autoritatea de Supraveghere națională în termen de 72 de ore de la descoperirea acesteia. Notificarea inițială poate fi urmată de furnizarea, în etape, a tuturor informațiilor necesare, precum natura încălcării datelor cu caracter personal, informațiile de contact ale responsabilului cu protecția datelor, consecințele posibile ale încălcării datelor și eforturile de atenuare ale consecințelor încălcării securității datelor.

Un nou rol organizațional introdus de RGPD este cel de *Responsabil cu protecția datelor* (DPO), în cadrul oricărei organizații care manipulează date cu caracter personal de orice fel, inclusiv pentru procesatorii de date. Aceştia din urmă sunt de obicei terți care manipulează datele aparținând altor afaceri. Responsabilitățile DPO sunt descrise în art. 39 din RGPD.

În ceea ce privește consimțământul persoanelor vizate, se înlătură capacitatea întreprinderilor de a se baza pe consimțământul implicit. În schimb, necesită "o declarație sau o acțiune afirmativă clară". Aceasta înseamnă că procedurile de documentare pentru orice activitate de culegere de date – de la marketing la recrutare – vor trebui revizuite și actualizate în mod riguros. De asemenea, se limitează capacitatea copiilor de a-și da consimțământul pentru prelucrarea datelor fără autorizația părintească și necesită consimțământul explicit pentru prelucrarea anumitor "categorii speciale" de date cu caracter personal, care includ originea rasială sau etnică, opiniile politice, convingerile religioase sau filozofice și apartenența la sindicate.

---

[13] Christopher Kuner, Lee A. Bygrave, Christopher Docksey, *op.cit.*, p. 863

Transferurile transfrontaliere de date sunt supuse, de asemenea, noilor reglementări în domeniul protecției datelor, dacă vizează date care aparțin cetățenilor UE. Se permit transferurile de date cu caracter personal către alte țări sau organizații internaționale, cu obligația ca regimul lor juridic să fie considerat de către Comisia Europeană ca să asigure un nivel "adecvat" de protecție a datelor cu caracter personal. În absența unei decizii de adecvare, totuși, transferurile sunt permise și în afara statelor din afara UE în anumite circumstanțe, cum ar fi prin utilizarea clauzelor contractuale standard sau a regulilor corporative obligatorii. Derogările sunt, de asemenea, permise în circumstanțe suplimentare limitate[14].

Progresele tehnologice au permis organizațiilor să adune o gamă largă de date cu caracter personal și să le analizeze. Unul dintre principalele motive îl reprezintă cercetarea de piață, în care afacerea va aduna și analiza date, va trage concluzii și apoi va lua măsuri, cum ar fi campanii de marketing direcționate și strategii de diferențiere a prețurilor. Conform GDPR, acest lucru este clasificat drept "profilare", prelucrarea automată a datelor cu caracter personal și utilizarea acestor date personale pentru a evalua anumite aspecte personale referitoare la o persoană fizică. Cu toate acestea, GDPR impune multe restricții diferite asupra procesării automate a datelor și asupra deciziilor luate folosind acele date.

În cazul în care o organizație are activități care includ profilarea, este necesar să se asigure că drepturile persoanelor vizate de a fi informate cu privire la consecințele deciziilor luate au fost îndeplinite, mai exact cu privire la formularele de consimțământ ale persoanelor vizate.

[14] Mirela Carmen Dobrilă, *"Dreptul European al afacerilor. Principii, politici, piața unică, libertăți, drept european al constractelor"*, Editura Universul Juridic, 2019

Capitolul 6

Considerații generale privind riscurile utilizării sistemelor de inteligență artificială(IA)

Utilizarea inteligenței artificiale în procesarea datelor personale vine cu o serie de *riscuri și probleme de protecție a datelor* .[15]În ceea ce privește riscurile asociate cu utilizarea inteligenței artificiale în contextul protecției datelor cu caracter personal, există o serie de aspecte de care trebuie să ținem cont.

Primul dintre acestea este *discriminarea,* care poate avea loc atunci când algoritmii de inteligență artificială sunt instruiți să ia decizii bazate pe date istorice care au fost generate de sisteme de tipărire discriminatorii. Acest lucru 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 cel al *profilării,* care poate avea loc atunci când datele personale sunt colectate și utilizate pentru a crea profiluri detaliate ale utilizatorilor. Aceste profiluri pot fi folosite pentru a lua decizii automatizate în ceea ce privește serviciile și produsele oferite, dar și în alte scopuri, cum ar fi analiza riscului sau detectarea fraudelor. O altă problemă este legată de *lipsa de responsabilitate și transparență a sistemelor de inteligență artificială*, care pot fi greu de controlat și monitorizat. Acest lucru poate duce la o lipsă de încredere în sistemul în cauză și poate face ca utilizatorii să fie reticenți în a furniza datele personale necesare.

În plus, există riscuri asociate cu *securitatea datelor și confidențialitatea,* în special în ceea ce privește *stocarea și transferul* acestora. De asemenea, există riscul ca datele personale să fie folosite în mod incorect 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 procesarea datelor personale și ar trebui luate măsuri adecvate pentru a minimiza aceste riscuri.

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* (art. 5), 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.

Domeniul IA cunoaște mai multe ramuri de dezvoltare, în funcție de rezultatele care se urmăresc a fi atinse, de exemplu *machine larning, supervised learning, deep learning, sisteme de decizie, robotică inteligentă ș.a.m.d.*

Datele medicale se referă la toate datele personale privind starea de sănătate a unei persoane, incluzând date genetice şi date care au o legătură clară şi strânsă cu starea de sănătate (Art. 1, CoE Rec. no R 97 5 privind *Protecţia datelor medicale*), actualizată de Recomandarea privind protecţia datelor referitoare la starea de sănătate. Datele medicale depăşesc cadrul relaţiei discrete dintre medic şi pacient, incluzând orice persoană care poate păstra date privind starea de sănătate. Conform art.3 din Recomandarea privind datele referitoare la starea de sănătate, datele referitoare la starea de sănătate, înseamnă toate datele personale care privesc starea de sănătate fizică sau mentală ale unei persoane, incluzând asigurarea de servicii medicale, care dezvăluie informaţii privind starea de sănătate trecută, prezentă şi cea viitoare a unei persoane.

Prin natura lor*, datele medicale* se aplică la starea de sănătate trecută, prezentă şi viitoare a persoanei vizate, atât fizică, cât şi psihică. *Datele privind starea de sănătate a unei persoane* sunt clasificate, ca şi categorii de date speciale, atât de legislaţia UE, cât şi în cea a Co E (Art. 9.1, GDPR, Art. 6, Convenţia 108+). Art. 9 din GDPR şi art. 6 din Convenţia 108+ tratează, în mod specific, datele genetice şi biometrice, prin care este identificată o persoană, ca fiind o categorie specială de date . Statele membre au dreptul, conform art. 9(4) din GDPR să menţină sau să

impună condiţii suplimentare (incluzând limitări), pentru datele genetice, biometrice sau medicale . Conform interpretării 29 WP, toate datele cuprinse în documente medicale, în dosarele medicale electronice şi în sistemele DMI, trebuie considerate *date sensibile*. În cauza *Z contra Finlandei,* s-a statuat, că datele medicale fac obiectul unui regim mai strict de prelucrare a datelor decât datele ne-sensibile.

Orice activitate de prelucrare de date medicale trebuie să fie conformă cu regulile generale de protecţie a datelor personale. Drept urmare, orice operator de date care colectează informaţii medicale identificabile individual, trebuie să respecte principiile generale de prelucrare a datelor. În plus, pentru datele medicale, GDPR oferă garanţii suplimentare în ceea ce priveşte prelucrarea datelor cu caracter medical . Art. 6 din Convenţia 108+ permite prelucrarea datelor genetice, a datelor biometrice care identifică, în mod unic o persoană, precum şi a datelor referitoare la starea de sănătate, numai dacă, în lege sunt prevăzute garanţii adecvate.

Datele referitoare la starea de sănătate sunt supuse unui regim mai strict de prelucrare a datelor decât *datele nesensibile*. GDPR interzice prelucrarea datelor legate de sănătate, precum şi a datelor genetice şi biometrice, cu excepţia cazului, când este autorizată, conform art. 9.2 .

În conformitate cu *principiul reducerii la minim a datelor*, datele trebuie păstrate într-o formă care să permită identificarea persoanelor vizate pentru o perioadă care nu poate depăşi perioada necesară pentru scopurile pentru care au fost colectate datele sau pentru care sunt prelucrate ulterior.

Anonimizarea şi pseudonimizarea se numără printre tehnicile de securitate IT, care permit atenuarea intruziunii în intimitate, propusă de prelucrarea datelor, în timpul activităţilor legale de prelucrare datelor.

Anonimizarea este procesul de eliminare a identificatorilor personali, atât direcţi, cât şi indirecţi, care pot conduce la identificarea unei persoane. Datele sunt anonime dacă toate elementele de identificare au fost eliminate dintr-un set de date cu caracter personal. În cazul în care datele au fost eliminate cu succes, acestea nu mai sunt date cu caracter personal şi sunt în afara domeniului de aplicare al regimului juridic privind protecţia datelor. *Pseudominizarea* constă, în înlocuirea unui atribut de către altul, într-o înregistrare. Prin urmare, este posibilă identificarea persoanei fizice, în mod indirect . În consecinţă, utilizată singură, pseudonimizarea nu va conduce la un set de date anonime. Datele pseudonimizate nu pot fi asimilate informaţiilor anonime, deoarece acestea permit identificarea unei persoane vizate şi legarea acesteia în diferite sete de date. Pseudonimizarea este de natură să permită identificabilitatea şi, prin urmare, face obiectul regimului juridic de protecţie a datelor.

Grupul de Lucru, înfiinţat prin articolul 29, identifică *trei scenarii principale* în care datele cu caracter personal prelucrate prin intermediul aplicaţiilor de stil de viaţă şi bunăstare, sunt considerate a fi date medicale:

1. Datele prelucrate prin aplicaţie sau dispozitiv sunt în mod inerent date medicale,
2. Datele brute ale senzorilor prelucrate prin aplicaţie sau dispozitiv pot fi utilizate, independent sau în combinaţie cu alte date, pentru atrage concluzii cu privire la starea reală de sănătate a unui individ sau la riscurile pentru sănătate şi,
3. Pe baza datelor colectate prin aplicaţie sau dispozitiv, se trag concluzii cu privire la starea de sănătate a unui individ sau la riscurile pentru sănătate (indiferent dacă aceste concluzii sunt exacte sau inexacte, legitime sau nelegitime, adecvate sau inadecvate).

Grupul de lucru, înfiinţat de art. 29 a clarificat faptul că, informaţiile obţinute prin testarea sau examinarea unei părţi de corp sau a unei substanţe corporală (de exemplu, informaţii generate de dispozitive care analizează urina sau sângele persoanei sau aplicaţii care monitorizează tensiunea arterială sau frecvenţa cardiacă a unei persoane), informaţiile despre riscurile de îmbolnăvire (informaţii referitoare la un risc ştiinţific sau perceput în mod obişnuit de boală viitoare, cum ar fi, consumul de droguri, consumul excesiv de alcool şi informaţiile despre starea reală fiziologică sau biomedicală a unei persoane, independent de sursa acestora, se încadrează, de asemenea, în categoria datelor medicale. În plus, faţă de informaţiile considerate ca date medicale prin natura acestora, anumite activităţi de prelucrare a datelor pot fi luate în considerare de autorităţile de protecţie a datelor ca fiind prelucrări ale datelor medicale datorită modului în care sunt efectuate. În acest sens, prelucrarea informaţiilor apărute inofensiv, ar putea fi considerată prelucrare a datelor medicale, în cazul în care presupune urmărirea informaţiilor în timp, combinarea acestora cu alte date sau dezvăluirea acestora altor părţi care au acces la informaţii suplimentare referitoare la persoana respectivă, în particular, dacă această prelucrare se face în scopul creării profilului sau de marketing direct.

Comisia a elaborat un Document de lucru al personalului Comisiei privind cadrul juridic existent al UE aplicabil aplicaţiilor privind stilul de viaţă şi bunăstarea. Acest act intenţionează să furnizeze o descriere neexhaustivă a legislaţiei UE, care se aplică aplicaţiilor de stil de viaţă şi bunăstare.

GDPR nu se aplică atunci când datele prelucrate de aplicaţii de stil de viaţă şi bunăstare nu sunt transmise în afara dispozitivului utilizatorului. Dacă datele sunt transmise în afara dispozitivului, atunci acestea sunt calificate drept date medicale şi prelucrarea lor este permisă numai în cazuri limitate. Pentru prelucrarea legală, va fi necesar consimţământul explicit. De fapt, în orice caz, va fi necesar consimţământul în cazul în care aplicaţia sau dispozitivul de bunăstare sau stil de

viaţă procesează date despre locaţie sau alte date colectate prin intermediul senzorilor pe dispozitivul mobil al unui individ. Dezvoltatorii de aplicaţii şi dispozitive trebuie să respecte regulile de confidenţialitate a datelor, în special, furnizând informaţii clare şi uşor accesibile utilizatorilor înainte de a instala o aplicaţie sau de a cumpăra un dispozitiv.

Comunicaţiile electronice generează o cantitate importantă de date personale sensibile din utilizarea serviciilor (meta date). Accesul la anumite meta date, cum ar fi adresele IP şi combinaţiile acestora, poate fi mai intruziv decât interceptarea comunicaţiilor vocale, permiţând astfel, stabilirea unor modele de comportament, cercuri de contact personal şi preferinţe în activitatea noastră online, pe care le ştim doar noi înşine.

Apariţia telefoanelor inteligente şi a tabletelor conectate permanent la internet, adesea utilizând reţele WIFI, a mărit volumul de date sensibile pe care le producem zilnic şi nivelul de expunere la riscurile de securitate cibernetică. Printre provocările recente, se pot identifica: internetul obiectelor, articolele purtabile, casele inteligente, oraşele inteligente sau reţelele inteligente, toate bazate pe comunicaţiile electronice.

Potrivit art. 8 alin. (1) CEDO, orice persoană are dreptul la respectarea vieţii sale private şi de familie, a domiciliului său şi a corespondenţei sale. Totodată, art. 7 din Carta UE prevede că, orice persoană are dreptul la respectarea vieţii private şi de familie, a domiciliului şi a secretului comunicaţiilor.

Directiva 2002/58/CE asupra confidenţialităţii şi comunicaţiilor electronice, modificată prin Directiva 2006/24 este parte din cadrul de reglementare al comunicaţiilor electronice UE, reprezentând un element cheie pentru liberalizarea sectorului comunicaţiilor electronice, creşterea concurenţei, inovarea şi consolidarea drepturilor utilizatorilor. Directiva asupra confidenţialităţii şi comunicaţiilor electronice se aplică în cauze privind prelucrarea datelor cu caracter

personal în legătură cu furnizarea de servicii de comunicaţii electronice destinate publicului în reţelele de comunicaţii publice, inclusiv, reţelele publice de comunicaţii care susţin dispozitivele de colectare şi identificare a datelor.

Cookie este un text alfanumeric scurt care este stocat (şi ulterior recuperat) pe echipamentul terminal al persoanei vizate. În principiu, organizaţiile trebuie să obţină consimţământul abonatului sau utilizatorului înainte de a introduce cookie-uri pe dispozitivele acestora.

Un *cookie* poate fi clasificat, după durata acestuia, *cookie de sesiune*, şters după ce utilizatorul închide browserul, sau un *cookie persistent*, care rămâne în dispozitivul utilizatorului pentru o perioadă de timp după închiderea broserului. *Cookie-urile* pot fi, de asemenea, de primă parte (setate de serverul web al paginii vizitate şi cu acelaşi domeniu) şi ale unor terţe părţi stocate de un domeniu diferit de domeniul paginii vizitate (de exemplu, pagina web se referă la un fişier, cum ar fi Java script, aflat în afara domeniului său).

Acest lucru reprezintă provocări pentru *confidenţialitate,* deoarece companiile de publicitate folosesc cookie-uri de terţă parte pentru a construi profiluri despre obiceiurile de navigare, chiar dacă profilul este anonim.

Conform considerentului 24 din *expunerea de motive*, aşa numitele *spyware, web bugs, hidden identifiers* şi alte procedee similare pot să acceseze terminalul utilizatorului, fără ştirea acestuia şi să acceadă la informaţii, să copieze informaţii ascunse sau să urmărească activitatea utilizatorului şi pot încălca flagrant confidenţialitatea datelor acestor utilizatori. Folosirea de astfel de procedee trebuie permisă doar în scopuri legitime, cu informarea utilizatorilor în cauză.

Consimţământul trebuie să fie acordat, pe baza unor informaţii specifice, clare şi complete, înainte de setarea sau citirea cookie-urilor, printr-o acţiune pozitivă, ca urmare a unei acţiuni libere.

Folosirea sistemelor de apelare şi comunicare automată, fără intervenţia umană, a faxului sau a poştei electronice, în scopuri de marketing directă este permisă numai în legătură cu acei abonaţi sau utilizatori care şi-au acordat, în prealabil consimţământul. Obţinerea consimţământului nu este necesară în cazul în care detaliile de contact ale unui client sunt utilizate pentru comercializarea directă a unor produse similare cu cele achiziţionate anterior de acesta. Clienţilor trebuie să li se ofere clar şi distinct posibilitatea de a-şi retrage acordul, în mod gratuit şi uşor, fie la colectarea iniţială a datelor, fie cu ocazia fiecărui mesaj.

Statele membre pot decide ca exprimarea acordului pentru comercializare directă sau retragerea acestuia să se aplice şi la alte tipuri de comercializare directă, cum este comercializarea directă, utilizând telefonul, cu condiţia ca ambele opţiuni să fie disponibile gratuit.

Fie că vorbim despre computer, laptop sau telefon, echipamentele respective reţin și prelucrează multe date personale. Toate aceste informații se pot dovedi vulnerabile în fața criminalității cibernetice. Datele personale au valoare monetară, adică sunt "vânate" pentru că se pot transforma în bani reali.

Cele mai căutate *date personale* sunt:

- *Parolele* salvate în browser sau stocate în fișiere de sistem;
- Detaliile *cardurilor de* credit/debit cu care se fac plăți online și care sunt salvate în echipament sau în browser;
- Detalii despre *conturile bancare*;
- *Numere naționale unice de identificare* (cum ar fi *CNP-ul*), salvate în documente sau fotografii;
- *Mesajele text* conținând oricare din datele enumerate mai sus și/sau preferințele unei persoane, în orice domeniu (această ultimă categorie de date personale este extrem de căutată ca să se trimită reclame personalizate);

- *Numerele apelate* sau de la care se primesc apeluri telefonice;
- *Nume, adrese* și numere de telefon salvate în lista de contacte, în browser, în listele de contacte din diverse aplicații, etc.;
- *Site-urile* vizitate recent. Deținătorii acestor site-uri, precum și partenerii lor, sunt foarte interesați de istoricul căutărilor/achizițiilor unei persoane și, prin intermediul cookie-urilor obțin o multitudine de informații pe care le folosesc pentru a obține un câștig direct sau, indirect, vânzându-le altora etc.16;
- *Locațiile* în care s-a aflat o persoană, care sunt extrase din aplicațiile de navigare folosite;
- *Locația actuală*, mai ales dacă este folosită funcția *"share location"* a telefonului sau din aplicații precum WhatsApp, sau alte aplicații care oferă această funcție (ex.*: "Find My Friends",* care este o aplicație disponibilă în "Apple Store"17 utilizatorilor de iPhone sau celorcare folosesc dispozitive cu sistem de operare IOS);
- *Fișiere accesate recent*, care conțin informații despre utilizatori;
- *Fișiere șterse.* Toate fișierele șterse, chiar și cele care nu mai sunt în coșul de gunoi *(Recycle Bin),* pot fi recuperate până în moment rescrierii fizice a echipamentului - momentul în care se formatează dispozitivul, adică se șterge tot și se pregătește dispozitivul pentru utilizare, sau ștergerea se face prin scrierea, în sens IT, a unor informații peste cele deja existente, în așa fel încât acestea din urmă să devină imposibil de recunoscut și utilizat.

Cyberbullying-ul se manifestă atunci când cineva folosește tehnologiile digitale, cum ar fi telefoanele mobile sau rețelele de socializare, pentru a face rău sau a intimida pe altcineva în mod repetat.

Cu titlu de exemplu de *cyberbullying*, se pot enumera următoarele situaţii:

- Hărțuirea unei persoane prin trimiterea de SMS sau mesaje instant, în număr mare, pentru a amenința sau a intimida destinatarul, sau chiar fără un scop precis,
- Jignirea, amenințarea, intimidarea, șantajarea cuiva, indiferent de motiv, în mediul online;
- Divulgarea în mediul online a datelor personale despre o persoană,
- Postarea de texte și/sau imagini/clipuri video despre o anumită persoană, fără consimţământul acesteia, pentru a umili,
- Răspândirea în mediul online a datelor personale ale unei persoane (număr de telefon, adresa de e-mail, adresa),
- Răspândirea în mediul online de mesaje jignitoare, care fac rău, folosind identități false;
- Crearea de pagini web, bloguri, vloguri etc. pentru a evalua exagerat pe cineva .

Furtul de identitate are loc atunci când cineva pretinde a fi altcineva pentru a obține bani sau alte lucruri. Este important ca informațiile personale să fie păstrate în siguranță și să nu fie împărtășite cu persoane necunoscute, fie *online* sau *offline*. Furtul de identitate este o infracțiune, este ilegal și este pedepsit în orice țară, inclusiv în România.

Unele dintre cele mai comune metode de furt utilizare de către atacatori sunt frauda prin e-mail *(Phishing),* apel telefonic *(Vishing)* și SMS *(Smishing).* Cu toate acestea, se poate fura identitatea utilizând doar informațiile disponibile public pe internet sau pe rețelele de Wi-Fi nesigure.

Atacurile de phishing au ca scop furtul sau deteriorarea datelor confidențiale, înșelându-i pe utilizatori să dezvăluie date şi informații personale, cum ar fi parolele și numerele cardurilor de credit. „Pescarul” pretinde că este o persoană de

încredere și, înșelând victima, primește acces la date cu caracter personal (de exemplu, parole, detalii card bancar). Atacurile de phishing pot facilita accesul la toate tipurile de date confidențiale. Pe măsură ce tehnologiile evoluează, la fel fac și atacurile cibernetice

Cea mai comună formă de *atac de phishing* utilizează tactici cum ar fi *hyper-linkurile false* pentru a convinge destinatarii mesajelor de e-mail să-și partajeze informațiile personale. Atacatorii se prefac adesea a fi furnizori importanți de conturi, cum ar fi Microsoft sau Google, sau chiar coleg

Altă abordare prevalentă a atacurilor de *phishing* implică plantarea de mal-ware deghizat ca atașare de încredere (cum ar fi un CV sau un extras de cont bancar) într-un e-mail. În unele cazuri, deschiderea unei atașări malware poate paraliza întregi sisteme de IT.

În vreme ce majoritatea atacurilor de phishing aruncă o plasă largă, phishingul țintit vizează anumite persoane, exploatând informațiile colectate prin cercetarea activității și a vieții lor sociale. Aceste atacuri sunt foarte particularizate, ceea ce le face deosebit de eficiente la ocolirea securității cibernetice de bază.

Când utilizatorii rău intenționați vizează un *„pește mare”* cum ar fi un direc-tor de firmă sau o celebritate, tehnica se numește *whaling*. Acești escroci efec-tuează adesea cercetări considerabile asupra țintelor lor, pentru a găsi un moment oportun de a le fura acreditările de conectare sau alte informații confidențiale.

O combinație a cuvintelor *„SMS”* și *„phishing”, smishing* implică trimiterea de mesaje text deghizate în comunicări de încredere de la firme precum *Amazon* sau *FedEx*. Utilizatorii sunt deosebit de vulnerabili la înșelătoriile prin SMS, de-oarece mesajele text sunt livrate ca text simplu și par mai personale.

În campaniile de *vishing*, atacatorii din centre de apelare frauduloase încearcă să păcălească oamenii să furnizeze informații confidențiale prin telefon. În multe

cazuri, aceste înșelătorii utilizează tehnici de inginerie socială pentru a păcăli victimele să instaleze malware pe dispozitivele lor, sub forma unei aplicații.

Un atac de *phishing* reușit poate avea consecințe grave, cum ar fi: pierderea de date personale generale și date sensibile; pierderea accesului la conturile de socializare (e.g. e-mail, rețele de socializare etc.); pierderea datelor financiare, instalarea de malware şi alte ameninţări informatice, etc.

Wi-Fi este o familie de protocoale de rețea fără fir bazate pe familia de standarde IEEE 802.11, care sunt utilizate în mod obișnuit pentru rețelele locale ale dispozitivelor și accesul la Internet, permițând dispozitivelor digitale din apropiere să facă schimb de date prin unde Radio.

Wi-Fi este, în esență, un radio digital foarte avansat, care utilizează frecvențe între 2 gigaherți și 5 gigaherți în spectrul electromagnetic. Principala problemă cu securitatea rețelei wireless este accesul simplificat la rețea, în comparație cu rețelele tradiționale cu fir, cum ar fi Ethernet.

Cu o rețea prin cablu, trebuie să fie obţinut acces la o clădire sau utilizat un firewall extern. Pentru a accesa Wi-Fi, trebuie doar să te afli în raza de acțiune a rețelei Wi-Fi. Majoritatea rețelelor de afaceri protejează datele și sistemele sensibile încercând să interzică accesul extern. Activarea conectivității wireless reduce securitatea, dacă rețeaua folosește o criptare inadecvată sau nu o folosește deloc.

Bibliografie

1. Mirela Carmen Dobrilă, *"Dreptul European al afacerilor. Principii, politici, piața unică, libertăți, drept european al constractelor"*, Editura *Universul Juridic*, 2019;

2. Ronald Leens, Rosamunde van Brakel, Serge Gutwirth&Paul de Hert, *"Data Protection and Privacy – The Age of Intelligent Machines"*, *Hart Publishing*, 2017;

3. Christopher Kuner, Lee A. Bygrave, Christopher Docksey, *"The Eu General Data Protection Regulation (GDPR) – A commentary", Oxford University Press*, Oxford, 2020;

4. Daniel-Mihail Șandru, *Principiile protecţiei datelor – de la teorie la practică*, *Curierul Judiciar*, nr. 6/ 2018;

5. Stanciu D . Cărpenaru , *Drept comercial român*, Editura *Juridică*, Bucureşti, 2008;

6. Ana-Maria Lupulescu, *Reorganizarea societăţilor comerciale în contextul*

integrării Europene, Editura *Wolters Kluwer*, România, 2008;

7. Răducan OPREA, *Dreptul european al afacerilor*, Galaţi, *University Press*, 2010;

8. Aurelian Gherghe, *Drept internaţional privat*, Editura *Universul Juridic*, Bucureşti, 2010;

9. Aurelian Gherghe, *Efectele neexecutării contractelor sinalagmatice*, Editura *Universul Juridic*, Bucureşti, 2010;

10. Aurelian Gherghe, *Teoria conflictelor de legi în noul Cod Civil*, editia a III-a revizuită şi adăugită, Editura *Contrast*, Bucureşti, 2019;

11. *"Eu General Data Protection Regulation (GDPR) – An implementation and Compliance Guide",* Ediția a 4-a, IT *Governance Publishing*, 2020.

.