Avizul 28/2024 privind anumite aspecte ale protecției datelor legate de prelucrarea datelor cu caracter personal în contextul modelelor de IA

Adoptat la 17 decembrie 2024

Rezumat

Tehnologiile IA creează multe oportunități și beneficii într-o gamă largă de sectoare și activități sociale.

Prin protejarea dreptului fundamental la protecția datelor, RGPD sprijină aceste oportunități și promovează alte drepturi fundamentale ale UE, și anume dreptul la libertatea de gândire, de exprimare și de informare, dreptul la educație sau libertatea de a desfășura o activitate comercială. În acest fel, RGPD este un cadru legal care încurajează inovarea responsabilă.

În acest context, având în vedere chestiunile legate de protecția datelor ridicate de aceste tehnologii, autoritatea de supraveghere irlandeză a solicitat CEPD să emită un aviz cu privire la chestiuni de aplicare generală în virtutea articolului 64 alineatul (2) din RGPD. Cererea se referă la prelucrarea datelor cu caracter personal în contextul fazelor de dezvoltare și implementare a modelelor de inteligență artificială („**IA**"). Mai precis, întrebările din cerere sunt: (1) când și cum poate fi considerat „anonim" un model de IA; (2) cum pot demonstra operatorii caracterul adecvat al interesului legitim ca temei juridic în fazele de dezvoltare și (3) implementare; și (4) care sunt consecințele prelucrării ilegale a datelor cu caracter personal în faza de dezvoltare a unui model de IA asupra prelucrării sau funcționării ulterioare a modelului de IA.

În ceea ce privește prima întrebare, avizul menționează că afirmațiile privind anonimatul unui model de IA trebuie evaluate de autoritățile competente de supraveghere de la caz la caz, deoarece CEPD consideră că modelele de IA antrenate cu date cu caracter personal nu pot fi considerate, în toate cazurile, anonime. Pentru ca un model de IA să fie considerat anonim, atât (1) probabilitatea de extragere directă (inclusiv probabilistică) a datelor cu caracter personal privind persoanele ale căror date cu caracter personal au fost utilizate pentru elaborarea modelului, cât și (2) probabilitatea de a obține, intenționat sau nu, asemenea date cu caracter personal din interogări, trebuie să fie nesemnificative, având în vedere „*toate mijloacele [...] pe care este probabil în mod rezonabil să le utilizeze*" operatorul sau altă persoană.

Pentru a-și efectua evaluarea, autoritățile de supraveghere trebuie să analizeze documentația furnizată de operator pentru a demonstra anonimatul modelului. În acest sens, avizul oferă o listă neprescriptivă și neexhaustivă de metode pe care operatorii le pot folosi în demonstrarea anonimatului și care pot fi deci luate în considerare de autoritățile de supraveghere când evaluează declarația de anonimat a unui operator. Aceasta cuprinde, de exemplu, abordările adoptate de operatori, în faza de dezvoltare, pentru a preveni sau a limita culegerea datelor cu caracter personal utilizate la antrenare, pentru a reduce posibilitatea de a le identifica, pentru a preveni extragerea lor sau a oferi asigurări cu privire la rezistența la atacuri, conform stadiului actual al tehnologiei.

Cu privire la a doua și a treia întrebare, avizul furnizează considerații generale pe care autoritățile de supraveghere trebuie să le ia în considerare când evaluează dacă operatorii pot recurge la interesul legitim ca temei juridic adecvat pentru prelucrarea efectuată în contextul dezvoltării și implementării modelelor de IA.

Avizul reamintește că între temeiurile juridice prevăzute de RGPD nu există o ierarhie și că este de competența operatorilor să identifice temeiul juridic adecvat pentru activitățile lor de prelucrare. Avizul reamintește apoi testul în trei etape care trebuie efectuat la evaluarea utilizării interesului legitim ca temei juridic, și anume (1) identificarea interesului legitim urmărit de operator sau de un terț; (2) analiza necesității prelucrării în scopul interesului (intereselor) legitim(e) urmărit(e) (numită și

„testul necesității"); și (3) evaluarea prevalenței intereselor sau drepturilor și libertăților fundamentale ale persoanelor vizate asupra interesului (intereselor) legitim(e) (numită și „testul comparativ").

Cât privește prima etapă, avizul reamintește că un interes poate fi considerat legitim dacă sunt îndeplinite cumulativ următoarele trei criterii cumulativ: interesul (1) este legitim; (2) este formulat în mod clar și precis; și (3) este real și prezent (adică nu speculativ). Acest interes poate acoperi, de exemplu, dezvoltarea unui model de IA - dezvoltarea serviciului unui agent conversațional care să asiste utilizatorii, sau implementarea lui - îmbunătățirea detectării amenințărilor într-un sistem informatic.

Cât privește a doua etapă, avizul reamintește că evaluarea necesității presupune luarea în considerare a următoarelor aspecte: (1) dacă activitatea de prelucrare va permite urmărirea interesului legitim; și (2) dacă nu există o metodă mai puțin intruzivă de a urmări acest interes. Când evaluează dacă este îndeplinită condiția necesității, autoritățile de supraveghere trebuie să acorde atenție deosebită volumului de date cu caracter personal prelucrate și proporționalității în urmărirea interesului legitim în cauză, având în vedere, de asemenea, principiul reducerii la minimum a datelor.

În ce privește a treia etapă, avizul reamintește că testul comparativ trebuie efectuat în funcție de circumstanțele specifice fiecărui caz. Oferă apoi o prezentare generală a elementelor pe care autoritățile de supraveghere le pot lua în considerare când evaluează dacă interesele, drepturile și libertățile fundamentale ale persoanelor vizate prevalează asupra interesului unui operator sau al unui terț.

Ca parte a celei de a treia etape, avizul evidențiază riscurile specifice pentru drepturile fundamentale care pot apărea fie în fazele de dezvoltare, fie în fazele de implementare a modelelor de IA. De asemenea, precizează că prelucrarea datelor cu caracter personal care are loc în fazele de dezvoltare și implementare a modelelor de IA poate avea un impact asupra persoanelor vizate în diferite moduri, care pot fi pozitive sau negative. Pentru a evalua acest impact, autoritățile de supraveghere pot lua în considerare natura datelor prelucrate de modele, contextul prelucrării și posibilele consecințe ulterioare ale prelucrării.

Avizul subliniază și rolul așteptărilor rezonabile ale persoanelor vizate în testul comparativ. Acest lucru poate fi important din cauza complexității tehnologiilor folosite în modelele de IA și a faptului că, pentru persoanele vizate, varietatea utilizărilor lor potențiale, precum și diferitele activități de prelucrare implicate pot fi greu de înțeles. În această privință, atât informațiile furnizate persoanelor vizate, cât și contextul prelucrării pot fi printre elementele care trebuie luate în considerare pentru a evalua dacă persoanele vizate se pot aștepta în mod rezonabil la prelucrarea datelor lor cu caracter personal. Cât privește contextul, acesta poate include: dacă datele cu caracter personal au fost sau nu disponibile public, natura relației dintre persoana vizată și operator (și dacă există sau nu o legătură între cei doi), natura serviciului, contextul în care au fost culese datele cu caracter personal, sursa din care au fost culese datele (și anume, site-ul sau serviciul în care au fost culese datele cu caracter personal și setările de confidențialitate pe care le oferă), posibilele utilizări ulterioare ale modelului și dacă persoanele vizate știu, de fapt, că datele lor cu caracter personal sunt disponibile online.

Avizul reamintește, de asemenea, că, atunci când interesele, drepturile și libertățile persoanelor vizate par să prevaleze asupra interesului sau intereselor legitime urmărite de operator sau de un terț, operatorul poate avea în vedere introducerea unor măsuri de atenuare pentru a limita impactul prelucrării asupra acestor persoane vizate. Măsurile de atenuare nu trebuie confundate cu măsurile pe care operatorul este obligat prin lege să le adopte oricum pentru a asigura conformitatea cu RGPD. În plus, măsurile trebuie adaptate la circumstanțele cazului și la caracteristicile modelului de IA, inclusiv la utilizarea preconizată a acestuia. În acest sens, avizul oferă o listă neexhaustivă de exemple de

măsuri de atenuare în legătură cu faza de dezvoltare (inclusiv cu privire la extragerea de date de pe web) și faza de implementare. Măsurile de atenuare pot face obiectul unei evoluții rapide și trebuie adaptate la circumstanțele cazului. Prin urmare, rămâne la latitudinea autorităților de supraveghere să evalueze caracterul adecvat al măsurilor de atenuare aplicate de la caz la caz.

În ceea ce privește a patra întrebare, avizul reamintește, în general, că autoritățile de supraveghere dispun de competențe discreționare pentru a evalua posibila (posibilele) încălcare (încălcări) și a alege măsuri adecvate, necesare și proporționale, în funcție de circumstanțele fiecărui caz. În continuare, avizul are în vedere trei scenarii.

În scenariul 1, datele cu caracter personal sunt păstrate în modelul de IA (ceea ce înseamnă că modelul nu poate fi considerat anonim, după cum se menționează în prima întrebare) și sunt prelucrate ulterior de același operator (de exemplu, în contextul implementării modelului). Avizul precizează că trebuie evaluat de la caz la caz, în funcție de contextul cazului, dacă fazele de dezvoltare și de implementare implică scopuri separate (constituind deci activități de prelucrare separate) și în ce măsură lipsa temeiului juridic pentru activitatea de prelucrare inițială afectează legalitatea prelucrării ulterioare.

În scenariul 2, datele cu caracter personal sunt păstrate în model și sunt prelucrate de alt operator în contextul implementării modelului. În acest sens, avizul precizează că autoritățile de supraveghere ar trebui să ia în considerare dacă operatorul care implementează modelul a efectuat o evaluare adecvată, ca parte a obligațiilor sale de răspundere pentru a demonstra conformitatea cu articolul 5 alineatul (1) litera (a) și cu articolul 6 din RGPD, pentru a se asigura că modelul de IA nu a fost dezvoltat prin prelucrarea ilegală de date cu caracter personal. Această evaluare trebuie să ia în considerare, de exemplu, sursa datelor cu caracter personal și dacă prelucrarea în faza de dezvoltare a făcut obiectul constatării unei încălcări, în special dacă a fost stabilită de o autoritate de supraveghere sau de o instanță, și ar trebui să fie mai mult sau mai puțin detaliată în funcție de riscurile pe care le prezintă prelucrarea în faza de implementare.

În scenariul 3, un operator prelucrează ilegal date cu caracter personal pentru a dezvolta modelul de IA, apoi se asigură că acestea sunt anonimizate, după care același operator sau alt operator inițiază altă prelucrare a datelor cu caracter personal în contextul implementării. În acest sens, avizul precizează că, dacă se poate demonstra că operarea ulterioară a modelului de IA nu implică prelucrarea de date cu caracter personal, CEPD consideră că RGPD nu se aplică. Prin urmare, ilegalitatea prelucrării inițiale nu ar trebui să afecteze operarea ulterioară a modelului. În plus, CEPD consideră că, atunci când operatorii prelucrează ulterior datele cu caracter personal culese în faza de implementare, după ce modelul a fost anonimizat, RGPD s-ar aplica în legătură cu aceste operațiuni de prelucrare. În aceste cazuri, avizul consideră că, în ceea ce privește RGPD, legalitatea prelucrării efectuate în faza de implementare nu ar trebui să fie afectată de nelegalitatea prelucrării inițiale.

Cuprins

1 Introducere 6

1.1 Expunerea sumară a faptelor 6

1.2 .....Admisibilitatea cererii de emitere a unui aviz în temeiul articolului 64 alineatul (2) din RGPD 8

2 Obiectul și noțiunile principale 9

2.1 Obiectul avizului 9

2.2 Noțiuni de bază 11

2.3 Modelele de IA în contextul avizului 12

3 Cu privire la temeinicia cererii 13

3.1 Cu privire la natura modelelor de IA în raport cu definiția datelor cu caracter personal 13

3.2 Cu privire la situațiile în care modelele de IA ar putea fi considerate anonime și demonstrația aferentă 15

3.2.1 Considerații generale privind anonimizarea în contextul de față 15

3.2.2 Elemente de evaluare a probabilității reziduale de identificare 17

3.3 Cu privire la oportunitatea interesului legitim ca temei juridic pentru prelucrarea datelor cu caracter personal în contextul dezvoltării și implementării modelelor de IA 20

3.3.1 Observații generale 20

3.3.2 Considerații cu privire la cele trei etape ale evaluării interesului legitim în contextul dezvoltării și implementării modelelor de IA 22

3.4 Cu privire la impactul posibil al unei prelucrări ilegale în dezvoltarea unui model de IA asupra legalității prelucrării sau funcționării ulterioare a modelului de IA 32

3.4.1 Scenariul 1. Un operator prelucrează în mod ilegal date cu caracter personal pentru a dezvolta modelul, datele cu caracter personal sunt păstrate în model și sunt prelucrate ulterior de același operator (de exemplu, în contextul implementării modelului) 34

3.4.2 Scenariul 2. Un operator prelucrează ilegal date cu caracter personal pentru a dezvolta modelul, datele cu caracter personal sunt păstrate în model și sunt prelucrate de alt operator în contextul implementării modelului. 35

3.4.3 Scenariul 3 Un operator prelucrează ilegal date cu caracter personal pentru a dezvolta modelul, apoi se asigură că modelul este anonimizat, înainte ca același operator sau alt operator să inițieze altă prelucrare a datelor cu caracter personal în contextul implementării 36

4 Observații finale 37

Comitetul european pentru protecția datelor

Având în vedere articolul 63 și articolul 64 alineatul (2) din Regulamentul 2016/679/UE al Parlamentului European și al Consiliului din 27 aprilie 2016 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și privind libera circulație a acestor date și de abrogare a Directivei 95/46/CE (denumit în continuare „RGPD”),

având în vedere Acordul privind SEE, în special anexa XI și Protocolul 37 la acesta, astfel cum au fost modificate prin Decizia nr. 154/2018 a Comitetului mixt al SEE din 6 iulie 2018[1],

având în vedere articolele 10 și 22 din Regulamentul său de procedură,

întrucât:

(1) Principalul rol al Comitetului European pentru Protecția Datelor (denumit în continuare **„Comitetul”** sau **„CEPD”**) este de a asigura aplicarea coerentă a RGPD în întregul Spațiu Economic European (**„SEE”**). Articolul 64 alineatul (2) din RGPD prevede că orice autoritate de supraveghere (**„AS”**), președintele Comitetului sau Comisia poate solicita ca orice chestiune de aplicare generală sau care produce efecte în mai mult de un stat membru SEE să fie examinată de Comitet în vederea obținerii unui aviz. Scopul acestui aviz este de a analiza o chestiune de aplicare generală sau care produce efecte în mai mult de un stat membru SEE.

(2) Avizul Comitetului se adoptă în temeiul articolului 64 alineatul (3) din RGPD, coroborat cu articolul 10 alineatul (2) din Regulamentul de procedură al Comitetului European pentru Protecția Datelor, în termen de opt săptămâni după ce președintele și autoritatea de supraveghere competentă decid că dosarul este complet. Prin decizia președintelui, această perioadă poate fi prelungită cu șase săptămâni, în funcție de complexitatea chestiunii.

ADOPTĂ URMĂTORUL AVIZ:

1 Introducere

1.1 Expunerea sumară a faptelor

1. La 4 septembrie 2024, autoritatea de supraveghere irlandeză („**AS IE**” sau „**AS solicitantă**”) a solicitat CEPD să emită un aviz în temeiul articolului 64 alineatul (2) din RGPD în legătură cu modelele de IA și prelucrarea datelor cu caracter personal („**cererea**”).

2. Președintele Comitetului și AS IE au considerat dosarul încheiat la 13 septembrie 2024. În următoarea zi lucrătoare, pe 16 septembrie 2024, dosarul a fost transmis de Secretariatul CEPD. Având în vedere complexitatea problemei, președintele Comitetului a decis să prelungească termenul legal în conformitate cu articolul 64 alineatul (3) din RGPD și cu articolul 10 alineatul (4) din Regulamentul de procedură al CEPD.

3. Cererea se referă la anumite elemente ale antrenării, actualizării, dezvoltării și operării modelelor de IA în care există date cu caracter personal care fac parte din setul de date relevant. AS IE subliniază că

[1] Trimiterile la „statele membre” din prezentul aviz trebuie înțelese ca trimiteri la „statele membre ale SEE”. Trimiterile la „Uniune” din prezentul aviz trebuie înțelese ca trimiteri la „SEE”.

cererea privește aspecte-cheie, care au un impact mare asupra persoanelor vizate și operatorilor din SEE și că în această etapă nu există o poziție armonizată în rândul autorităților naționale de supraveghere[2]. Terminologia care va fi folosită în scopul prezentului aviz este prezentată în secțiunile 2.2 și 2.3 de mai jos.

4. AS IE a pus următoarele întrebări:

Întrebarea 1: Se consideră că, în toate cazurile, modelul final de IA, care a fost antrenat utilizând date cu caracter personal, nu corespunde definiției datelor cu caracter personal [așa cum prevede articolul 4 alineatul (1) din RGPD]?

În cazul unui răspuns afirmativ la întrebarea 1:

i. În ce etapă a operațiunilor de prelucrare care duc la un model de IA nu se mai prelucrează date cu caracter personal?
   a) Cum se poate demonstra că modelul de IA nu prelucrează date cu caracter personal?

ii. Există factori care ar putea face ca operarea modelului final de IA să nu mai fie considerată anonimă?
   a) Dacă da, cum se pot demonstra măsurile luate pentru a atenua, preveni sau proteja împotriva acestor factori (încât să se asigure că modelul de IA nu prelucrează date cu caracter personal)?

În cazul unui răspuns negativ la întrebarea 1:

i. În ce situații poate apărea acest lucru?
   a) În caz afirmativ, cum se pot demonstra măsurile care s-au luat pentru a se asigura că modelul de IA nu prelucrează date cu caracter personal?

Întrebarea 2: În cazul în care un operator de date se bazează pe interese legitime ca temei juridic pentru prelucrarea datelor cu caracter personal în vederea creării, actualizării și/sau dezvoltării unui model de IA, cum ar trebui operatorul respectiv să demonstreze caracterul adecvat al intereselor legitime ca temei juridic, atât în ceea ce privește prelucrarea datelor de la terți, cât și a datelor de la prima parte?

i. Ce considerente ar trebui să ia în considerare operatorul pentru a se asigura că interesele persoanelor vizate, ale căror date cu caracter personal sunt prelucrate, sunt echilibrate în mod corespunzător față de interesele operatorului în contextul:
   a) Datelor furnizate de terți

   b) Datelor de la prima parte

Întrebarea 3: După antrenare, dacă un operator de date se bazează pe interese legitime ca temei juridic pentru prelucrarea datelor cu caracter personal care are loc în cadrul unui model de IA sau al unui sistem de IA din care face parte un model de IA, cum ar trebui un operator să demonstreze caracterul adecvat al intereselor legitime ca temei juridic?

Întrebarea 4: Dacă s-a constatat că un model de IA a fost creat, actualizat sau dezvoltat utilizând date cu caracter personal prelucrate ilegal, care este impactul lui, dacă este cazul, asupra legalității

[2] Cerere, p. 1.

prelucrării sau operării continue sau ulterioare a modelului de IA, fie pe cont propriu, fie ca parte a unui sistem de IA, când:

i. modelul de IA, fie singur, fie ca parte a unui sistem de IA, prelucrează date cu caracter personal?
ii. nici modelul de IA, nici modelul de IA ca parte a unui sistem de IA nu prelucrează date cu caracter personal?

1.2 Admisibilitatea cererii de emitere a unui aviz în temeiul articolului 64 alineatul (2) din RGPD

5. Articolul 64 alineatul (2) din RGPD prevede, în special, că orice autoritate de supraveghere poate solicita ca orice chestiune de aplicare generală sau care produce efecte în mai mult de un stat membru să fie examinată de Comitet în vederea obținerii unui aviz.

6. Autoritatea de supraveghere solicitantă a adresat CEPD întrebări cu privire la aspectele legate de protecția datelor în contextul modelelor de IA. Aceasta a precizat în cerere că, deși multe organizații folosesc în prezent modele de IA, inclusiv modele lingvistice mari („**LLM**"), operațiunile, antrenarea și utilizarea lor ridică *„o serie de preocupări de amploare privind protecția datelor"*[3], care *„au impact asupra persoanelor vizate din întreaga UE/SEE"*[4].

7. Cererea ridică, în esență, întrebări cu privire la (i) aplicarea conceptului de date cu caracter personal; (ii) principiul legalității, în special în ceea ce privește temeiul juridic al interesului legitim, în contextul modelelor de IA, precum și cu privire la (iii) consecințele prelucrării ilegale a datelor cu caracter personal în faza de dezvoltare a modelelor de IA, asupra prelucrării sau operării ulterioare a modelului.

8. Prin urmare, Comitetul consideră că această cerere privește o *„chestiune de aplicare generală"* în sensul articolului 64 alineatul (2) din RGPD. În special, chestiunea se referă la interpretarea și aplicarea articolului 4 alineatul (1), a articolului 5 alineatul (1) litera (a) și a articolului 6 din RGPD în ceea ce privește prelucrarea datelor cu caracter personal în dezvoltarea și implementarea modelelor de IA. După cum a subliniat autoritatea de supraveghere solicitantă, aplicarea acestor dispoziții la modele de IA ridică probleme sistemice, abstracte și noi[5]. Dezvoltarea și implementarea rapidă a modelelor de IA de către tot mai multe organizații ridică probleme specifice și, după cum se subliniază în cerere, *„CEPD va beneficia foarte mult de pe urma ajungerii la o poziție comună cu privire la chestiunile ridicate de prezenta cerere, aceste chestiuni fiind esențiale pentru activitatea planificată a CEPD pe termen scurt și mediu"*[6]. În plus, tehnologiile de IA creează multe oportunități și beneficii într-o gamă largă de sectoare și activități sociale. În plus, RGPD este un cadru legal care încurajează inovarea responsabilă. Rezultă că există un interes general în efectuarea acestei evaluări sub forma unui aviz al CEPD, pentru a asigura aplicarea consecventă a anumitor dispoziții ale RGPD în contextul modelelor de IA.

9. Condiția alternativă menționată la articolul 64 alineatul (2) din RGPD se referă la chestiuni *„care produc efecte în mai mult de un stat membru"*. CEPD reamintește că termenul „efecte" trebuie interpretat

[3] Cerere, p. 1.
[4] Ibid.
[5] Cerere, p. 2.
[6] Cerere, p. 1. După cum se menționează în Programul de activitate al CEPD pentru 2024-2025, adoptat la 8 octombrie 2024, disponibil la adresa https://www.edpb.europa.eu/system/files/2024-10/edpb_work_programme_2024-2025_en.pdf, CEPD intenționează să emită, printre altele, orientări privind anonimizarea, pseudonimizarea și extragerea de date de pe web în contextul inteligenței artificiale generative.

lato sensu și nu se limitează deci doar la efecte juridice[7]. Întrucât din ce în ce mai multe modele de IA sunt antrenate și folosite de un număr tot mai mare de organizații din SEE, ele au un impact asupra unui număr mare de persoane vizate din întregul SEE, unele exprimând deja preocupări în fața autorității lor de supraveghere competente[8]. Prin urmare, CEPD consideră că problema ridicată de autoritatea de supraveghere solicitantă îndeplinește și această condiție.

10. Cererea conține o motivare scrisă privind contextul și motivațiile pentru transmiterea întrebărilor către Comitet, inclusiv cu privire la cadrul legal relevant. Prin urmare, Comitetul consideră că cererea este motivată conform articolului 10 alineatul (3) din Regulamentul de procedură al CEPD.

11. Conform articolului 64 alineatul (3) din RGPD[9], CEPD nu emite un aviz dacă a emis deja un aviz pe această temă. CEPD nu a emis un aviz pe această temă și nu a furnizat încă răspunsuri la întrebările care decurg din cerere.

12. Din aceste motive, Comitetul consideră că cererea este admisibilă, iar întrebările care decurg din ea trebuie analizate în acest aviz („**avizul**”) adoptat conform articolului 64 alineatul (2) din RGPD.

2 Obiectul și noțiunile principale

2.1 Obiectul avizului

13. Comitetul este de acord cu autoritatea de supraveghere solicitantă că, din perspectiva protecției datelor, dezvoltarea și implementarea modelelor de IA ridică probleme fundamentale privind protecția datelor. Întrebările se referă în special la: (i) când și cum poate fi considerat „anonim” un model de IA (întrebarea 1 din cerere); (ii) cum pot operatorii să demonstreze caracterul adecvat al interesului legitim ca temei juridic în fazele de dezvoltare (întrebarea 2 din cerere) și de implementare (întrebarea 3 din cerere); și (iii) dacă prelucrarea ilegală a datelor cu caracter personal în faza de dezvoltare are consecințe asupra legalității prelucrării sau operării ulterioare a modelului de IA (întrebarea 4 din cerere).

14. CEPD reamintește că autoritățile de supraveghere sunt responsabile pentru monitorizarea aplicării RGPD și trebuie să contribuie la aplicarea lui coerentă în întreaga Uniune[10]. Prin urmare, este de competența autorităților de supraveghere să investigheze modelele specifice de IA și, în acest sens, să efectueze evaluări de la caz la caz.

15. Prezentul aviz oferă un cadru pentru ca autoritățile de supraveghere competente să evalueze cazurile specifice în care ar apărea (unele dintre) problemele ridicate în cerere. Prezentul aviz nu urmărește să fie exhaustiv, ci să ofere considerații generale cu privire la interpretarea dispozițiilor relevante, de care autoritățile de supraveghere competente trebuie să țină seama în cea mai mare măsură când își exercită competențele de investigare. Deși se adresează autorităților de supraveghere competente și se referă la activitățile și competențele lor, avizul nu aduce atingere obligațiilor care le revin operatorilor și persoanelor împuternicite de operatori în temeiul RGPD. În special, conform principiului responsabilității consacrat la articolul 5 alineatul (2) din RGPD, operatorii sunt responsabili de toate

[7] CEPD, Documentul intern nr. 3/2019 privind orientările interne referitoare la articolul 64 alineatul (2) din RGPD, adoptat la 8 octombrie 2019, punctul 15, disponibil la adresa https://www.edpb.europa.eu/system/files/2022-07/internaledpb_document_201903_art64.2_en.pdf.
[8] Cerere, p. 1-2.
[9] Articolul 64 alineatul (3) din RGPD și articolul 10 alineatul (4) din Regulamentul de procedură al CEPD.
[10] Articolul 51 alineatul (1) din RGPD și articolul 51 alineatul (2) din RGPD.

principiile referitoare la prelucrarea datelor cu caracter personal și sunt în măsură să demonstreze respectarea lor.

16. În unele cazuri, în aviz pot fi furnizate câteva exemple, dar, având în vedere obiectul vast al întrebărilor cuprinse în cerere, precum și diferitele tipuri de modele de IA pe care le vizează, în aviz nu vor fi luate în considerare toate scenariile posibile. Tehnologiile asociate cu modelele de IA sunt supuse unei evoluții rapide; în consecință, considerațiile CEPD din prezentul aviz trebuie interpretate în lumina acestui fapt.

17. **Avizul nu analizează dispozițiile de mai jos, care pot juca însă un rol important în evaluarea cerințelor de protecție a datelor aplicabile modelelor de IA:**

- **Prelucrarea categoriilor speciale de date:** CEPD reamintește interdicția prevăzută la articolul 9 alineatul (1) din RGPD în ceea ce privește prelucrarea categoriilor speciale de date și excepțiile limitate de la articolul 9 alineatul (2) din RGPD[11]. În această privință, Curtea de Justiție a Uniunii Europene (denumită în continuare **„CJUE"**) a clarificat în continuare că *„în cazul în care un ansamblu de date care conține atât date sensibile, cât și date care nu sunt sensibile este [...] colectat în bloc, fără ca datele să poată fi disociate unele de celelalte la momentul acestei colectări, prelucrarea ansamblului respectiv de date trebuie considerată interzisă, în sensul articolului 9 alineatul (1) din RGPD, atunci când cuprinde cel puțin o dată sensibilă și nu este aplicabilă niciuna dintre derogările prevăzute la articolul 9 alineatul (2) din acest regulament*"[12]. În plus, CJUE a subliniat, de asemenea, că *„în scopul aplicării excepției prevăzute la articolul 9 alineatul (2) litera (e) din RGPD, trebuie să se verifice dacă persoana vizată a înțeles, în mod explicit și printr-o acțiune fără echivoc, să facă accesibile publicului larg datele cu caracter personal în discuție"*[13]. Aceste considerații trebuie luate în considerare atunci când prelucrarea datelor cu caracter personal în contextul modelelor de IA implică categorii speciale de date.

- **Luarea de decizii automatizate, inclusiv crearea de profiluri**: Operațiunile de prelucrare efectuate în contextul modelelor de IA pot intra în domeniul de aplicare al articolului 22 din RGPD, care impune operatorilor obligații suplimentare și oferă persoanelor vizate garanții suplimentare. CEPD reamintește, în acest sens, orientările sale privind luarea automată a deciziilor individuale și crearea de profiluri în sensul Regulamentului 2016/679[14].

- **Compatibilitatea scopurilor**: Articolul 6 alineatul (4) din RGPD prevede, pentru anumite temeiuri juridice, criterii pe care un operator trebuie să le ia în considerare pentru a stabili dacă prelucrarea în alt scop este compatibilă cu scopul pentru care sunt colectate inițial datele cu caracter personal. Această dispoziție poate fi relevantă în contextul dezvoltării și implementării modelelor de IA, iar aplicabilitatea ei trebuie evaluată de autoritățile de supraveghere.

[11] Vezi și Raportul CEPD privind activitatea desfășurată de Grupul operativ al ChatGPT, adoptat la 23 mai 2024, punctul 18: „În ceea ce privește prelucrarea unor categorii speciale de date cu caracter personal, pentru ca prelucrarea să fie legală trebuie să se aplice, în plus, una dintre excepțiile prevăzute la articolul 9 alineatul (2). *În principiu, una dintre aceste excepții poate fi articolul 9 alineatul (2) litera (e) din RGPD. Cu toate acestea, simplul fapt că datele cu caracter personal sunt accesibile publicului nu înseamnă că „persoana vizată a făcut publice în mod manifest astfel de date" [...]*".

[12] Hotărârea CJUE din 4 iulie 2023, cauza C-252/21, *Meta v. Bundeskartellamt* (ECLI:EU:C:2023:537), punctul 89.

[13] Hotărârea CJUE din 4 iulie 2023, cauza C-252/21, *Meta v. Bundeskartellamt* (ECLI:EU:C:2023:537), punctul 77.

[14] Orientările Grupului de lucru „Articolul 29" privind procesul decizional automatizat și crearea de profiluri în sensul Regulamentului 2016/679 (WP251 rev. 01), astfel cum au fost revizuite și adoptate ultima dată la 6 februarie 2018, aprobate de CEPD la 25 mai 2018. Vezi și Hotărârea CJUE din 7 decembrie 2023, cauza C-634/21, *SCHUFA Holding și alții* (ECLI:EU:C:2023:957).

- **Evaluări ale impactului asupra protecției datelor** („**EIPD**”) (articolul 35 din RGPD): EIPD reprezintă un element important al responsabilității, atunci când prelucrarea în contextul modelelor de IA este susceptibilă să genereze un risc mare pentru drepturile și libertățile persoanelor fizice[15].

- **Principiul protecției datelor începând cu momentul conceperii** [articolul 25 alineatul (1) din RGPD]: Protecția datelor începând cu momentul conceperii este o garanție esențială care trebuie evaluată de autoritățile de supraveghere în contextul dezvoltării și implementării unui model de IA.

2.2 Noțiuni de bază

18. Ca observație preliminară, CEPD dorește să ofere clarificări cu privire la terminologia și conceptele pe care le folosește în prezentul aviz și numai în scopul prezentului aviz:

- „**Date de la prima parte**” se referă la datele cu caracter personal pe care operatorul le-a cules de la persoanele vizate.

- „**Date de la terți**” se referă la datele cu caracter personal pe care operatorii nu le-au obținut de la persoanele vizate, ci le-au cules sau primit de la un terț, de exemplu de la un broker de date sau culese prin extragere de date de pe web.

- „**Extragerea de date de pe web (web scraping)**” este o tehnică folosită frecvent pentru culege informații din surse online accesibile publicului. Informațiile extrase, de exemplu, din servicii precum canale de știri, platforme de comunicare socială, discuții pe forumuri și site-uri personale pot conține date cu caracter personal.

- Cererea se referă la **„ciclul de viață” al modelelor de IA**, precum și la diverse etape privind, printre altele, „crearea”, „dezvoltarea”, „antrenarea”, „actualizarea”, „perfecționarea”, „exploatarea” sau „post-antrenarea” modelelor de IA. CEPD recunoaște că, în funcție de circumstanțe, astfel de etape pot avea loc în dezvoltarea și implementarea modelelor de IA și pot include prelucrarea datelor cu caracter personal în diverse scopuri de prelucrare. Cu toate acestea, în sensul prezentului aviz, CEPD consideră că este important să se simplifice clasificarea etapelor susceptibile de a avea loc. Prin urmare, în sensul prezentului aviz, CEPD se referă la „**faza de dezvoltare**” și la „**faza de implementare**”. Dezvoltarea unui model de IA acoperă toate etapele dinaintea oricărei implementări a modelului de IA și include, printre altele, dezvoltarea de coduri, culegerea de date cu caracter personal de antrenament, prelucrarea prealabilă a datelor cu caracter personal de antrenament și antrenarea. Implementarea unui model de IA cuprinde toate etapele legate de utilizarea unui model de IA și poate include orice operațiuni efectuate după faza de dezvoltare. CEPD rămâne conștient de varietatea cazurilor de utilizare și de potențialele lor consecințe în ceea ce privește prelucrarea datelor cu caracter personal; prin urmare, autoritățile de supraveghere trebuie să analizeze dacă observațiile furnizate în acest aviz sunt relevante pentru prelucrarea pe care o evaluează.

- CEPD subliniază, de asemenea, că, atunci când este necesar, termenul „**antrenare**” se referă la partea din faza de dezvoltare în care modelele de IA învață din date pentru a-și îndeplini sarcina preconizată (așa cum se explică în secțiunea următoare din aviz).

[15] Orientările GL29 privind evaluarea impactului asupra protecției datelor (EIPD) și determinarea dacă prelucrarea este „susceptibilă de a genera un risc ridicat” în sensul Regulamentului 2016/679, revizuite și adoptate la 4 octombrie 2017, aprobate de CEPD la 25 mai 2018.

- Noțiunea și obiectul **modelelor de IA**, în înțelesul CEPD în scopul acestui aviz, sunt specificate în continuare în secțiunea dedicată următoare.

2.3 Modelele de IA în contextul avizului

19. Regulamentul UE privind inteligența artificială[16] definește un „sistem de inteligență artificială" ca fiind *„un sistem bazat pe o mașină care este conceput să funcționeze cu diferite niveluri de autonomie și care poate prezenta adaptabilitate după implementare, și care, urmărind obiective explicite sau implicite, deduce, din datele de intrare pe care le primește, modul de generare a unor rezultate precum previziuni, conținut, recomandări sau decizii care pot influența mediile fizice sau virtuale"* [17]. Considerentul 12 din Regulamentul privind inteligența artificială explică mai mult noțiunea de „sistem de IA". O caracteristică esențială a sistemelor de IA este capabilitatea lor de a face deducții. Tehnicile care permit deducții în timpul construirii unui sistem de IA sunt învățarea automată, metodele bazate pe logică și pe cunoștințe.

20. „Modelele de IA", pe de altă parte, sunt definite doar indirect în Regulamentul privind inteligența artificială: *„Deși modelele de IA sunt componente esențiale ale sistemelor de IA, ele nu constituie sisteme de IA în sine. Modelele de IA necesită adăugarea de componente suplimentare, cum ar fi, de exemplu, o interfață cu utilizatorul, pentru a deveni sisteme de IA. Modelele de IA sunt, de regulă, integrate în sistemele de IA și fac parte din acestea"*[18].

21. CEPD înțelege că definiția unui model de IA propusă în cerere este mai restrânsă decât cea din Regulamentul privind inteligența artificială, deoarece aceasta se referă la „modelul AI" ca fiind *„pentru a cuprinde produsul rezultat din mecanismele de antrenare care sunt aplicate unui set de date de formare, în contextul inteligenței artificiale, al învățării automate, al învățării profunde sau al altor contexte de procesare conexe"* și precizează în continuare că *„Termenul se aplică modelelor de IA care sunt destinate să fie supuse unei antrenări, ajustări și/sau dezvoltări suplimentare, precum și modelelor de IA care nu sunt."*[19]

22. Pe această bază, CEPD a adoptat prezentul aviz, înțelegând că un sistem de inteligență artificială se va baza pe un model de IA pentru a-și îndeplini obiectivul preconizat prin încorporarea modelului într-un cadru mai larg (de exemplu, un sistem de IA pentru serviciul clienți ar putea folosi un model de inteligență artificială antrenat pe date istorice de conversație pentru a da răspunsuri la întrebările utilizatorilor).

23. În plus, modelele de IA (sau „**modelele**") relevante pentru prezentul aviz sunt cele dezvoltate printr-un proces de antrenare. Acest proces de antrenare face parte din faza de dezvoltare, în care modelele învață din date pentru a-și îndeplini sarcina preconizată. Prin urmare, procesul de antrenare necesită un set de date din care modelul va identifica și va „învăța" tipare. În aceste cazuri, modelul va folosi diferite tehnici pentru a construi o reprezentare a cunoștințelor extrase din setul de date de antrenare. Acest lucru este valabil în special în cazul învățării automate.

24. În practică, orice model de IA este un algoritm, a cărui funcționare este determinată de un set de elemente. De exemplu, modelele de învățare adâncă sunt adesea sub forma unei rețele neuronale cu

[16] Regulamentul (UE) 2024/1689 al Parlamentului European și al Consiliului din 13 iunie 2024 de stabilire a unor norme armonizate privind inteligența artificială și de modificare a Regulamentelor (CE) nr. 300/2008, (UE) nr. 167/2013, (UE) nr. 168/2013, (UE) 2018/858, (UE) 2018/1139 și (UE) 2019/2144 și a Directivelor 2014/90/UE, (UE) 2016/797 și (UE) 2020/1828 (Regulamentul privind inteligența artificială) (Text cu relevanță pentru SEE).
[17] Vezi articolul 3 alineatul (1) din Regulamentul privind inteligența artificială.
[18] Considerentul 97 din Regulamentul privind inteligența artificială.
[19] Cerere, p. 3.

mai multe straturi formate din noduri conectate prin margini care au greutăți, care sunt ajustate în timpul antrenării ca să învețe relațiile dintre intrări și rezultate. Caracteristicile unui model simplu de învățare adâncă ar fi: (I) tipul și mărimea fiecărui strat, (ii) greutatea atribuită fiecărei margini (numite și „parametri"), (iii) funcțiile de activare[20] dintre straturi și, eventual, (iv) alte operațiuni care pot avea loc între straturi. De exemplu, când se antrenează un model simplu de învățare profundă pentru clasificarea de imagini, intrările („**pixelii de imagine**") vor fi asociate cu rezultatele, iar greutățile pot fi ajustate în așa fel încât să producă rezultatul corect de cele mai mute ori.

25. Alte exemple de modele de învățare adâncă sunt LLM-urile și inteligența artificială generativă, care se folosesc, de exemplu, pentru a genera conținut asemănător celui uman și a crea date noi.

26. **Pe baza considerațiilor de mai sus, conform cererii, obiectul prezentului aviz tratează doar subsetul de modele de IA care sunt rezultatul antrenării acestor modele cu date cu caracter personal.**

3 Cu privire la temeinicia cererii

3.1 Cu privire la natura modelelor de IA în raport cu definiția datelor cu caracter personal

27. Articolul 4 alineatul (1) din RGPD definește datele cu caracter personal ca fiind „*orice informație referitoare la o persoană fizică identificată sau identificabilă.*" (și anume, persoana vizată). În plus, considerentul 26 din RGPD prevede că principiile de protecție a datelor nu ar trebui să se aplice informațiilor anonime, și anume informațiilor care nu se referă la o persoană fizică identificată sau identificabilă, luând în considerare „*toate mijloacele [...] pe care este probabil, în mod rezonabil să le utilizeze*" operatorul sau altă persoană. Acest lucru presupune: (i) date care nu au fost niciodată legate de o persoană identificată sau identificabilă și (ii) date cu caracter personal care au fost anonimizate în așa fel încât persoana vizată nu este sau nu mai este identificabilă.

28. În consecință, la întrebarea 1[21] din cerere se poate răspunde analizând dacă un model de IA rezultat în urma unui antrenament care implică prelucrarea de date cu caracter personal trebuie considerat, în toate cazurile, anonim. Pe baza formulării întrebării, CEPD se va referi în această secțiune la procesul de „antrenare" a unui model de IA.

29. În primul rând, CEPD ar dori să prezinte următoarele considerații generale. Modelele de IA, indiferent că sunt antrenate sau nu cu date cu caracter personal, sunt în general concepute pentru a face predicții sau a trage concluzii, adică sunt concepute pentru a face deducții. În plus, modelele de IA antrenate cu date cu caracter personal sunt adesea concepute pentru a face deducții despre persoane diferite de cele ale căror date cu caracter personal au fost folosite pentru a antrena modelul de IA. Unele modele de IA sunt concepute însă în mod special pentru a furniza date cu caracter personal referitoare la persoane ale căror date cu caracter personal au fost folosite pentru a antrena modelul sau, într-un anumit mod, pentru a pune la dispoziție aceste date. În aceste cazuri, asemenea modele de IA vor include în mod inerent (și, de obicei, în mod necesar) informații referitoare la o persoană fizică identificată sau identificabilă și vor implica deci prelucrarea de date cu caracter personal. Prin urmare, aceste tipuri de modele de IA nu pot fi considerate anonime. Acesta ar fi cazul, de exemplu, (i) al unui model generativ ajustat pe baza înregistrărilor vocale ale unei persoane pentru a-i imita vocea sau (ii)

[20] Adică funcții care calculează, pe baza intrărilor și greutăților, rezultatul unui nod neuronal care va fi apoi trimis la stratul următor al rețelei neuronale.
[21] „*Se consideră că modelul final de IA, care a fost antrenat utilizând date cu caracter personal, în toate cazurile, nu corespunde definiției datelor cu caracter personal [așa cum prevede articolul 4 alineatul (1) din RGPD]?*"

al oricărui model conceput pentru a răspunde cu date personale din formare când i se solicită informații referitoare la o anumită persoană.

30. Pe baza considerațiilor de mai sus, răspunzând la întrebarea 1 din cerere, CEPD se concentrează asupra situației modelelor de IA care nu sunt concepute pentru a furniza date cu caracter personal legate de datele de antrenare.

31. CEPD consideră că, chiar și atunci când un model de IA nu a fost conceput în mod intenționat pentru a produce informații referitoare la o persoană fizică identificată sau identificabilă din datele de antrenare, informațiile din setul de date de antrenare, inclusiv datele cu caracter personal, pot rămâne în continuare „absorbite" în parametrii modelului, și anume reprezentate prin obiecte matematice. Acestea pot fi diferite de punctele originale de date de antrenare, dar pot păstra totuși informațiile originale ale acestor date, care pot fi în cele din urmă extractibile sau obținute din model în alt mod, direct sau indirect. Ori de câte ori informațiile referitoare la persoanele fizice identificate sau identificabile ale căror date cu caracter personal au fost utilizate pentru a antrena modelul pot fi obținute dintr-un model de IA prin mijloace care pot fi utilizate în mod rezonabil, se poate concluziona că un asemenea model nu este anonim.

32. În acest sens, în cerere se precizează că *„Publicațiile de cercetare existente evidențiază unele vulnerabilități potențiale care pot exista în modelele de IA și care ar putea duce la prelucrarea datelor cu caracter personal,*[22] *precum și prelucrarea datelor cu caracter personal care poate avea loc când modelele sunt implementate pentru a fi utilizate cu alte date, fie prin interfețe de programare a aplicațiilor (**„API"**), fie prin interfețe „prompte"*[23]".

33. În aceeași ordine de idei, cercetarea privind extragerea datelor de antrenament este deosebit de dinamică[24]. Ea arată că în unele cazuri se pot folosi mijloace care pot în mod rezonabil să extragă date cu caracter personal din unele modele de IA sau pur și simplu să se obțină în mod accidental date cu caracter personal prin interacțiuni cu un model de IA (de exemplu, ca parte a unui sistem de IA). Eforturile continue de cercetare în acest domeniu vor contribui la evaluarea mai aprofundată a riscurilor reziduale de regurgitare[25] și de extragere a datelor cu caracter personal în orice caz dat.

---

[22] De exemplu atacuri de tip deducere a apartenenței (OWASP) și atacuri de inversare a modelului (OWASP & Veale et al, 2018).

[23] Cerere, p.1-2.

[24] Vezi în acest sens, de exemplu: (i) Veale M., Binns R., Edwards L., 2018, *Algorithms that remember: model inversion attacks and data protection law*. Phil. Trans. R. Soc. A 376: 20180083, disponibil la http://dx.doi.org/10.1098/rsta.2018.0083; (ii) Brown H., Lee K., Mireshghallah F., Shokri R., și Tramèr F., *What Does it Mean for a Language Model to Preserving Privacy?*, 2022, ACM Digital Library, FAccT'22, 20 iunie 2022, Seul, Republica Coreea, disponibil la: https://dl.acm.org/doi/abs/10.1145/3531146.3534642 (iii) Vassilev A., Oprea A., Fordyce A., Anderson H., Adversarial *Machine Learning A Taxonomy and Terminology of Attacks and Mitigations*, ianuarie 2024, Institutul Național de Standarde și Tehnologie, disponibil la: https://nvlpubs.nist.gov/nistpubs/ai/NIST.AI.100-2e2023.pdf Carlini N., Tramèr F., Wallace E., Jagielski M., Herbert-Voss A., Lee K., Roberts A., Brown T., Song D., Erlingsson U., Oprea A., Raffel C., *Extracting Training Data from Large Language Models*, arXiv: 2012.07805v2 [cs.CR] 15 iunie 2021, disponibil la: https://arxiv.org/pdf/2012.07805 (v) Fredrikson M., Jha S., Ristenpart T., *Model Inversion Attacks the Exploit Confidence Information and Basic Countermeasures (Extracting Inversion Attacks the Exploit Confidence Information a nd Basic Countermeasures*), Biblioteca digitală ACM, 12 octombrie 2015, disponibil la https://dl.acm.org/doi/abs/10.1145/2810103.2813677; (vi) Zhang Y., Jia R., Pei H., Wang W., Li B., Song D., *The Secret revealer: Generative Model-Inversion Attacks Against Deep Neural Networks*, arXiv: 1911.07135v2 [cs.LG] 18 aprilie 2020, disponibil la https://arxiv.org/pdf/1911.07135.

[25] Pentru un sistem de IA bazat pe inteligență artificială generativă, regurgitarea corespunde situației în care rezultatele ar trimite direct la datele de antrenare.

34. **Pe baza considerațiilor de mai sus, CEPD consideră că modelele de IA antrenate pe bază de date cu caracter personal nu pot fi considerate, în toate cazurile, anonime. În schimb, determinarea caracterului anonim al unui model de inteligență artificială trebuie evaluată, pe bază de criterii specifice, de la caz la caz.**

3.2 Cu privire la situațiile în care modelele de IA ar putea fi considerate anonime și demonstrația aferentă

35. În ceea ce privește întrebarea 1 din cerere[26], CEPD este rugat să precizeze situațiile în care un model de IA, care a fost antrenat folosind date cu caracter personal, poate fi considerat anonim. În ceea ce privește întrebarea 1(i)(a) din cerere[27], CEPD este rugat să precizeze ce dovezi și/sau documente trebuie să ia în considerare autoritățile de supraveghere când evaluează dacă un model de IA este anonim.

3.2.1 Considerații generale privind anonimizarea în contextul de față

36. Folosirea expresiei „*orice informație*" în definiția „*datelor cu caracter personal*" de la articolul 4 alineatul (1) din RGPD reflectă scopul de a atribui acestui concept un domeniu larg de aplicare, care cuprinde toate tipurile de informații furnizate cu privire la care sintagma „*se referă*" la persoana vizată, care sunt identificate sau pot fi identificate în mod direct sau indirect.

37. Informațiile se pot referi la o persoană fizică chiar și atunci când sunt organizate sau codificate tehnic (de exemplu, într-un format care poate fi citit numai automat, fie că este privat sau deschis) într-un mod care nu face imediat evidentă relația cu persoana fizică respectivă. În aceste cazuri se pot folosi aplicații software pentru a identifica, recunoaște și extrage ușor anumite date. Acest lucru este valabil în special pentru modelele de IA în care parametrii reprezintă relații statistice între datele de antrenare și în care s-ar putea extrage date cu caracter personal exacte sau inexacte (din cauza deducției statistice), fie direct din relațiile dintre datele incluse în model, fie prin interogarea modelului respectiv.

38. Întrucât modelele de IA nu conțin, în general, înregistrări care pot fi izolate sau legate în mod direct, ci parametri care reprezintă relații probabilistice între datele conținute în model, s-ar putea deduce[28]

[26] „*În ce situații poate apărea acest lucru?*"
[27] „*Dacă da, cum se pot demonstra măsurile luate pentru a se asigura că modelul de IA nu prelucrează date cu caracter personal?*"
[28] (i) Carlini N., Chien S., Nasr M., Song S., Terzis A., Tramer F., *Membership Inference Attacks From First Principles,* arXiv:2112.03570, disponibil la https://arxiv.org/abs/2112.03570;
(ii) Crețu A.M, Guépin F. și De Montjoye Y.A, *Correlation inference attacks against machine learning models*. Hung. Adv.10, eadj9260(2024). DOI:10.1126/sciadv.adj9260 disponibil la https://www.science.org/doi/10.1126/sciadv.adj9260;
(iii) Dana L., Pydi M. S., Chevaleyre Y., *Memorization in Attention-only Transformers* arXiv:2411.10115v1 [cs.AI] 15 noiembrie 2024, disponibil la adresa: https://arxiv.org/abs/2411.10115;
(iv) Gehrke M., Liebenow J., Mohammadi E. & Braun T. et al. *Lifting in Support of Privacy-Preserving Probabilistic Inference*. Künstl Intell, 13 iunie 2024, disponibil la adresa: https://doi.org/10.1007/s13218-024-00851-y;
(v) Hu H., *Membership Inference Attacks and Defenses on Machine Learning Models Literature*, disponibil la adresa: https://github.com/HongshengHu/membership-inference-machine-learning-literature;
(vi) Nasr M., Carlini N., Hayase J., Jagielski M., Cooper A. F., Ippolito D., Choquette-Choo C. A., Wallace E., Tramèr F., și Lee K., Scalable *Extraction of Training Data from (Production) Language Models, arXiv*:2311.17035 28 noiembrie 2023, disponibil la adresa: https://arxiv.org/abs/2311.17035
(vii) Shokri R., Stronati M., Song C., Shmatikov V., *Membership Inference Attacks against Machine Learning Models* arXiv:1610.05820v2 [cs.CR], 31 martie 2017, disponibil la adresa: https://arxiv.org/abs/1610.05820;

informații din model, de exemplu deducția apartenenței, în scenarii realiste. Prin urmare, pentru ca o autoritate de supraveghere să fie de acord cu operatorul că un anumit model de IA poate fi considerat anonim, trebuie să verifice cel puțin dacă a primit suficiente dovezi că, prin mijloace rezonabile: (i) datele cu caracter personal, legate de datele de antrenare, nu pot fi extrase[29] din model; și (ii) orice rezultat produs la interogarea modelului nu se referă la persoanele vizate ale căror date cu caracter personal au fost folosite pentru antrenarea modelului.

39. În evaluarea îndeplinirii acestor condiții, autoritățile de supraveghere trebuie să ia în considerare trei elemente.

40. În primul rând, autoritățile de supraveghere trebuie să ia în considerare elementele identificate în cele mai recente avize ale grupului de lucru „Articolul 29" și/sau în orientările CEPD pe această temă. În ceea ce privește anonimizarea la data prezentului aviz, autoritățile de supraveghere trebuie să ia în considerare elementele din Avizul 05/2014 al Grupului de lucru „Articolul 29" privind tehnicile de anonimizare (**„Avizul nr. 5/2014 al Grupului de lucru «Articolul 29»"**), care prevede că, dacă din presupusul set de date anonim nu se pot individualiza, corela și deduce informații, datele pot fi considerate anonime[30]. De asemenea, se precizează că, „*ori de câte ori o propunere nu îndeplinește unul dintre criterii, trebuie efectuată o evaluare aprofundată a riscurilor de identificare*"[31]. **Având în vedere probabilitatea de extragere și deducție menționată mai sus, CEPD consideră că probabilitatea ca modelele de IA să necesite o asemenea evaluare aprofundată a riscurilor de identificare este foarte mare.**

41. În al doilea rând, această evaluare trebuie făcută luând în considerare „*toate mijloacele [...] pe care este probabil, în mod rezonabil să le utilizeze*" operatorul sau altă persoană pentru a identifica persoanele[32], iar determinarea acestor mijloace trebuie să se bazeze pe factori obiectivi, după cum se explică în considerentul 26 din RGPD, care pot fi:
    a. caracteristicile datelor de antrenare în sine, ale modelului de IA și ale procedurii de antrenare[33];
    b. contextul în care este lansat și/sau prelucrat modelul de IA[34];
    c. informațiile suplimentare care ar permite identificarea și care pot fi puse la dispoziția persoanei respective;

(viii) Staab R., Vero M., Mislav Balunović, Martin Vechev, 2024, *Beyond Memorization: Violating Privacy Via Inference with Large Language Models*, arXiv: 2310.07298v2, 6 mai 2024, disponibil la adresa: https://arxiv.org/abs/2310.07298:
(ix) Wu F., Cui L., Yao S., Yu S., *InferenceAttacks in Machine Learning as a Service: A Taxonomy, Review, and Promising Directions* arXiv: 2406.02027v1 [cs.LG], 27 iunie 2024, disponibil la adresa https://arxiv.org/abs/2406.02027v1:
(x) Zhang J., Das D., Kamath G., Tramèr F., „ *Membership Inference Attacks Cannot Prove to a Model Was Trained On Your Data* arXiv: 2409.19798v1, [cs.LG], 29 septembrie 2024, disponibil la adresa https://arxiv.org/abs/2409.19798:
(xi) Zhou Z., Xiang J., Chen C., și Su S., *Quantifying and Analysing entity-level memorisation in Large Language Models*, arXiv: 2308.15727v2 [cs.CL] 5 noiembrie 2023, disponibil la adresa: https://arxiv.org/abs/2308.15727.

[29] Extragerea include, în special, cazul în care datele cu caracter personal sunt deduse din modelul de IA în sine, cu utilizare redusă sau inexistentă a interfețelor de interogare.
[30] Avizul 05/2014 al Grupului de lucru „Articolul 29", p. 24.
[31] Avizul 05/2014 al Grupului de lucru „Articolul 29", p. 24.
[32] Hotărârea CJUE din 19 octombrie 2016, cauza C-582/14, *Breyer/Bundesrepublik Deutschland* (ECLI:EU:C:2016:779), punctul 43.
[33] Aici sunt cuprinse caracteristici ca: unicitatea înregistrărilor din datele de formare, precizia informațiilor, agregarea, randomizarea și, în special, modul în care acestea afectează vulnerabilitatea la identificare.
[34] Aceasta include elemente contextuale, de exemplu limitarea accesului la anumite persoane și garanții juridice.

d. costurile și timpul de care persoana ar avea nevoie pentru a obține astfel de informații suplimentare (în cazul în care nu îi sunt deja disponibile)[35]; și
e. tehnologia disponibilă la momentul prelucrării, precum și evoluțiile tehnologice[36].

42. În al treilea rând, autoritățile de supraveghere trebuie să analizeze dacă operatorii au evaluat riscul de identificare de către operator și de către diferite tipuri de *„alte persoane”*, inclusiv terți nedoriți care accesează modelul de IA, analizând și dacă se poate considera în mod rezonabil că acestea sunt în măsură, în mod rezonabil, să obțină acces sau să prelucreze datele în cauză.

43. **În concluzie, CEPD consideră că, pentru ca un model de IA să fie considerat anonim, utilizând mijloace rezonabile, atât (i) probabilitatea extragerii directe (inclusiv probabilistice) a datelor cu caracter personal referitoare la persoanele ale căror date cu caracter personal au fost utilizate la antrenarea modelului, cât și (ii) probabilitatea obținerii, în mod intenționat sau nu, a unor astfel de date cu caracter personal din interogări, trebuie să fie nesemnificativă[37] pentru orice persoană vizată. În mod implicit, autoritățile de supraveghere trebuie să aibă în vedere că este probabil ca modelele de IA să necesite o evaluare aprofundată a probabilității identificării pentru a ajunge la o concluzie cu privire la posibilul lor caracter anonim. Această probabilitate trebuie evaluată luând în considerare *„toate mijloacele [...] pe care este probabil, în mod rezonabil să le utilizeze”* operatorul sau altă persoană, și trebuie să ia în considerare și (re)utilizarea sau divulgarea neintenționată a modelului.**

3.2.2 Elemente de evaluare a probabilității reziduale de identificare

44. Deși s-ar putea lua măsuri atât în etapele de dezvoltare, cât și în cele de implementare, pentru a reduce probabilitatea obținerii de date cu caracter personal de la un model de IA, evaluarea anonimatului unui model de IA trebuie să ia în considerare și accesul direct la model.

45. În plus, autoritățile de supraveghere trebuie să evalueze, de la caz la caz, dacă măsurile luate de operator pentru a asigura și a dovedi că un model de IA este anonim sunt adecvate și eficace.

46. În special, concluzia evaluării unei autorități de supraveghere ar putea fi diferită între un model de IA disponibil public, care este accesibil unui număr necunoscut de persoane cu o gamă necunoscută de metode pentru a încerca să extragă date cu caracter personal, și un model de IA intern accesibil doar angajaților. Deși, în ambele cazuri, autoritățile de supraveghere trebuie să verifice dacă operatorii și-au îndeplinit obligația de asumare a răspunderii prevăzută la articolul 5 alineatul (2) și la articolul 24 din RGPD, *„toate mijloacele [...] pe care este probabil, în mod rezonabil să le utilizeze*” alte persoane pot avea un impact asupra gamei și naturii scenariilor posibile de luat în considerare. Prin urmare, în funcție de contextul dezvoltării și implementării modelului, autoritățile de supraveghere pot avea în vedere diferite niveluri de testare și rezistență la atacuri.

47. În acest sens, CEPD oferă mai jos o listă neprescriptivă și neexhaustivă de elemente posibile pe care autoritățile de supraveghere le pot lua în considerare când evaluează cererea de anonimat a unui operator. Alte abordări sunt posibile dacă oferă un nivel echivalent de protecție, în special ținând seama de stadiul tehnologiei.

[35] Hotărârea CJUE din 7 martie 2024, cauza C-479/22 P, *OC/Comisia Europeană* (ECLI:EU:C:2024:215), punctul 50.
[36] Hotărârea CJUE din 7 martie 2024, cauza C-479/22 P, *OC/Comisia Europeană* (ECLI:EU:C:2024:215), punctul 50.
[37] Hotărârea CJUE din 19 octombrie 2016, cauza C-582/14, *Breyer/Bundesrepublik Deutschland* (ECLI:EU:C:2016:779), punctul 46, și hotărârea CJUE din 7 martie 2024, cauza C-479/22 P, *OC/Comisia Europeană* (ECLI:EU:C:2024:215), punctul 51.

48. Prezența sau absența elementelor enumerate mai jos nu este un criteriu concludent pentru evaluarea anonimatului unui model de IA.

3.2.2.1 Proiectarea modelului de IA

49. În ceea ce privește proiectarea modelului de IA, autoritățile de supraveghere trebuie să evalueze metodele folosite de operatori în faza de dezvoltare. În acest sens, trebuie luate în considerare aplicarea și eficacitatea a patru domenii-cheie (identificate mai jos).

Selectarea surselor

50. Primul domeniu de evaluare implică examinarea selecției surselor utilizate pentru antrenarea modelului de IA. Ea cuprinde evaluarea, de către autoritățile de supraveghere, a măsurilor luate pentru a evita sau a limita culegerea de date cu caracter personal, și anume, printre altele, (i) caracterul adecvat al criteriilor de selecție; (ii) relevanța și caracterul adecvat al surselor alese, având în vedere scopul (scopurile) preconizat(e); și (iii) dacă au fost excluse sursele neadecvate.

Pregătirea și minimizarea datelor

51. Al doilea domeniu de evaluare se referă la pregătirea datelor pentru faza de antrenare. Autoritățile de supraveghere trebuie să examineze, în special: (i) dacă s-a luat în considerare utilizarea datelor anonime și/sau a datelor cu caracter personal supuse pseudonimizării; și (ii) în cazul în care s-a decis să nu se utilizeze astfel de măsuri, motivele acestei decizii, ținând seama de scopul urmărit; (iii) strategiile și tehnicile de minimizare a datelor utilizate pentru a limita volumul de date cu caracter personal incluse în procesul de antrenare; și (iv) procesele de filtrare a datelor aplicate înainte de antrenarea modelului, menite să elimine datele cu caracter personal irelevante.

Opțiuni metodologice cu privire la antrenare

52. Al treilea domeniu de evaluare privește selectarea de metode robuste în dezvoltarea modelelor de IA. Autoritățile de supraveghere trebuie să evalueze opțiunile metodologice care pot reduce considerabil sau elimina caracterul identificabil, inclusiv, printre altele: (i) dacă metodologia respectivă folosește metode de regularizare pentru a îmbunătăți generalizarea modelului și a reduce supraajustarea; și, în mod esențial, (ii) dacă operatorul a aplicat tehnici adecvate și eficiente de protejare a vieții private (de exemplu, confidențialitatea diferențială).

Măsuri privind rezultatele modelului

53. Ultimul domeniu de evaluare se referă la metode sau măsuri adăugate modelului de IA în sine care s-ar putea să nu aibă un impact asupra riscului de extragere directă a datelor cu caracter personal pentru model de către orice persoană care îl accesează direct, dar care poate reduce probabilitatea de a obține date cu caracter personal legate de datele de antrenament din interogări.

3.2.2.2 Analiza modelului de IA

54. Pentru ca autoritățile de supraveghere să evalueze soliditatea modelului de IA conceput în ce privește anonimizarea, un prim pas este să se asigure că proiectarea a fost dezvoltată conform planificării și face obiectul unei administrări tehnice eficace. Autoritățile de supraveghere trebuie să evalueze dacă operatorii au efectuat audituri bazate pe documente (interne sau externe) care cuprind o evaluare a măsurilor alese și a impactului lor pentru a limita probabilitatea identificării. Aceasta ar putea cuprinde analiza rapoartelor de revizuire a codului, precum și o analiză teoretică care să documenteze caracterul adecvat al măsurilor alese pentru a reduce probabilitatea de reidentificare a modelului respectiv.

3.2.2.3 Testarea modelului de IA și rezistența la atacuri

55. În sfârșit, autoritățile de supraveghere trebuie să ia în considerare obiectul, frecvența, cantitatea și calitatea testelor pe care operatorul le-a efectuat asupra modelului. În special, autoritățile de supraveghere trebuie să țină seama de faptul că testarea reușită care acoperă atacuri cunoscute pe

scară largă, de ultimă generație, poate fi doar o dovadă a rezistenței la aceste atacuri. Până la data acestui aviz, aceasta ar putea include, printre altele, teste structurate împotriva: (I) deducției atributelor și a apartenenței; (ii) exfiltrării; (iii) regurgitării datelor de antrenare; (iv) inversiunii modelului; sau (v) atacurilor de reconstrucție.

3.2.2.4 Documentația

56. Articolele 5, 24, 25 și 30 din RGPD și, în cazurile de risc probabil mare pentru drepturile și libertățile persoanelor vizate, articolul 35 din RGPD, impun operatorilor să-și documenteze în mod adecvat operațiunile de prelucrare. Acest lucru se aplică și prelucrărilor care ar include antrenarea unui model de IA, chiar dacă obiectivul prelucrării este anonimizarea. Autoritățile de supraveghere trebuie să ia în considerare o astfel de documentație și orice evaluare periodică a riscurilor aferente prelucrării efectuate de operatori, deoarece acestea sunt etape fundamentale pentru a demonstra că nu sunt prelucrate date cu caracter personal.

57. **CEPD consideră că autoritățile de supraveghere trebuie să ia în considerare documentația ori de câte ori trebuie evaluată o declarație de anonimat cu privire la un anumit model de IA. CEPD observă că, dacă o autoritate de supraveghere nu poate să confirme, după evaluarea cererii de anonimat, inclusiv în lumina documentației, că s-au luat măsuri eficace pentru a anonimiza modelul de IA, autoritatea de supraveghere ar fi în măsură să considere că operatorul nu și-a îndeplinit obligațiile de răspundere care îi revin în temeiul articolului 5 alineatul (2) din RGPD. Prin urmare, trebuie avută în vedere și respectarea altor dispoziții din RGPD.**

58. În mod ideal, autoritățile de supraveghere trebuie să verifice dacă documentația operatorului conține:

    a. informații referitoare la EIPD, inclusiv orice evaluări și decizii care au stabilit că nu a fost necesară o EIPD;

    b. orice consiliere sau feedback furnizat de responsabilul cu protecția datelor („**RPD**”) (în cazul în care un RPD a fost – sau ar fi trebuit – numit);

    c. informații despre măsurile tehnice și organizatorice luate în timpul proiectării modelului de IA pentru a reduce probabilitatea identificării, inclusiv modelul de amenințare și evaluările riscurilor pe care se bazează aceste măsuri. Aceasta trebuie să includă măsurile specifice pentru fiecare sursă de seturi de date de antrenament, inclusiv URL-urile-sursă relevante și descrierile măsurilor luate (sau deja luate de furnizorii terți de seturi de date);

    d. măsurile tehnice și organizatorice luate în toate etapele de-a lungul ciclului de viață al modelului, care au contribuit sau au verificat lipsa de date cu caracter personal în model;

    e. documentația care demonstrează rezistența teoretică a modelului de IA la tehnici de reidentificare, precum și controalele concepute pentru a limita sau a evalua succesul și impactul principalelor atacuri (regurgitare, atacuri de deducție a apartenenței, exfiltrare etc.). Aceste măsuri cuprind, în special: (i) raportul dintre cantitatea de date de antrenare și numărul de parametri din model, inclusiv analiza impactului acestuia asupra modelului [38] ; (ii)

[38] Ricciato F., *A Cautionary Reflection on (pseudo-) Synthetic Data from Deep Learning on Personal Data (A Cautionary Reflection on (pseudo-) Synthetic Data from Deep Learning on Personal Data*, Privacy in Statistical Databases Conference (PSD 2024), Antibes, Franța, septembrie 2024, slide-uri disponibile la adresa: https://cros.ec.europa.eu/system/files/2024-10/20240926_PSD2024_Ricciato_v6_1.pdf și Belkin M., Hsu D., Ma S., & Mandal S. (2019), *Reconciling modern machine-learning practice and the classical bias-variance trade-off*. Lucrările Academiei Naționale de Științe, 24 iulie 2019, 116(32) 15849-15854, disponibile la adresa: https://www.pnas.org/doi/10.1073/pnas.1903070116

măsurători privind probabilitatea de reidentificare pe baza stadiului actual al tehnologiei; (iii) rapoarte privind modul în care a fost testat modelul (de cine, când, cum și în ce măsură) și (iv) rezultatele testelor;

f. documentația furnizată operatorului (operatorilor) care implementează modelul și/sau persoanelor vizate, în special documentația referitoare la măsurile luate pentru a reduce probabilitatea de identificare și privind posibilele riscuri reziduale.

3.3 Cu privire la oportunitatea interesului legitim ca temei juridic pentru prelucrarea datelor cu caracter personal în contextul dezvoltării și implementării modelelor de IA

59. Pentru a răspunde la întrebările 2 și 3 din cerere, CEPD va prezenta mai întâi observații generale cu privire la unele aspecte importante pe care autoritățile de supraveghere trebuie să le ia în considerare, indiferent de temeiul legal pentru prelucrare, când evaluează cum pot demonstra operatorii conformitatea cu RGPD în contextul modelelor de IA. CEPD, bazându-se pe Orientările nr. 1/2024 privind prelucrarea datelor cu caracter personal în temeiul articolului 6 alineatul (1) litera (f) din RGPD[39], va analiza apoi cele trei etape necesare evaluării interesului legitim în contextul dezvoltării și implementării modelelor de IA.

3.3.1 Observații generale

60. CEPD reamintește că RGPD nu stabilește nicio ierarhie între diferitele temeiuri legale prevăzute la articolul 6 alineatul (1) din RGPD[40].

61. Articolul 5 din RGPD stabilește principiile referitoare la prelucrarea datelor cu caracter personal. CEPD le evidențiază pe cele semnificative pentru prezentul aviz și care trebuie luate în considerare de autoritățile de supraveghere cel puțin când evaluează anumite modele de IA, precum și cele mai relevante cerințe din alte dispoziții ale RGPD, ținând seama de obiectul prezentului aviz.

62. **Principiul responsabilității** [articolul 5 alineatul (2) din RGPD] – Acest principiu prevede că operatorul este responsabil de respectarea RGPD și este în măsură să demonstreze respectarea lui. În acest sens, rolurile și responsabilitățile părților care prelucrează date cu caracter personal în contextul dezvoltării sau implementării unui model de IA trebuie evaluate înainte să aibă loc prelucrarea, pentru a defini de la început obligațiile operatorilor sau ale operatorilor asociați și ale persoanelor împuternicite de aceștia (dacă este cazul).

63. **Principiile legalității, echității și transparenței** [articolul 5 alineatul (1) litera (a) din RGPD] - Când evaluează legalitatea prelucrării în contextul modelelor de IA, în lumina articolului 6 alineatul (1) din RGPD, CEPD consideră că este util să distingă diferitele etape ale prelucrării datelor cu caracter personal[41]. Principiul echității, care este strâns legat de principiul transparenței, impune ca datele cu caracter personal să nu fie prelucrate prin metode neloiale sau prin ingerință sau într-un mod *„nejustificat prejudiciabil, discriminatoriu ilegal, neașteptat sau înșelător pentru persoana vizată”*[42].

[39] Vezi Orientările CEPD nr. 1/2024 privind prelucrarea datelor cu caracter personal pe baza articolului 6 alineatul (1) litera (f) din RGPD, versiunea 1.0, adoptate la 8 octombrie 2024.
[40] Ibid., punctul 1.
[41] Raportul CEPD privind activitatea desfășurată de grupul operativ ChatGPT, adoptat la 23 mai 2024, punctul 14.
[42] Raportul CEPD privind activitatea desfășurată de Grupul operativ ChatGPT, adoptat la 23 mai 2024, punctul 23; Orientările CEPD nr. 4/2019 privind articolul 25 – Asigurarea protecției datelor începând cu momentul conceperii și în mod implicit, versiunea 2.0, adoptate la 20 octombrie 2020, punctul 69; Orientările Grupului de lucru

Având în vedere complexitatea tehnologiilor implicate, informațiile privind prelucrarea datelor cu caracter personal în cadrul modelelor de IA trebuie, prin urmare, furnizate într-un mod accesibil, inteligibil și ușor de utilizat[43]. Transparența cu privire la prelucrarea datelor cu caracter personal include, în special, respectarea obligațiilor de informare prevăzute la articolele 12-14 din RGPD[44], care necesită, de asemenea, în cazul unui proces decizional automatizat, inclusiv crearea de profiluri, informații semnificative cu privire la logica implicată, precum și importanța și consecințele preconizate ale prelucrării pentru persoana vizată[45]. Având în vedere că fazele de dezvoltare a modelelor de inteligență artificială pot implica culegerea unor cantități mari de date din surse accesibile public (de exemplu prin tehnici de extragere de date), recurgerea la excepția prevăzută la articolul 14 alineatul (5) litera (b) din RGPD este strict limitată la cazurile în care cerințele acestei dispoziții sunt pe deplin îndeplinite[46].

64. **Principiile limitării scopului și reducerii la minimum a datelor** [articolul 5 alineatul (1) litera (b) și litera (c) din RGPD] – conform principiului reducerii la minimum a datelor, dezvoltarea și implementarea modelelor de IA necesită ca datele cu caracter personal să fie adecvate, relevante și necesare în raport cu scopul. Aceasta poate include prelucrarea datelor cu caracter personal pentru a evita riscul de posibile părtiniri și erori atunci când acest lucru este identificat în mod clar și specific în cadrul scopului, iar datele cu caracter personal sunt necesare în acest scop (de exemplu, nu pot fi realizate în mod eficace prin prelucrarea altor date, inclusiv a datelor sintetice sau anonimizate)[47]. GL 29 a subliniat deja că „*scopul colectării trebuie să fie identificat în mod clar și specific* [...]”[48]. Când se evaluează dacă scopul urmărit este legitim, specific și explicit și dacă prelucrarea respectă principiul reducerii la minimum a datelor, trebuie identificată mai întâi activitatea de prelucrare în cauză. În special, diferitele etape din etapele de dezvoltare sau de implementare pot constitui activități de prelucrare identice sau diferite și pot implica operatori succesivi sau operatori asociați. În unele cazuri se poate determina scopul care va fi urmărit în cursul implementării modelului de IA într-o etapă timpurie de dezvoltare. Chiar și când nu este cazul, trebuie să fie deja clar un anumit context pentru această implementare și, prin urmare, trebuie luat în considerare cum influențează acest context scopul dezvoltării. Când revizuiesc scopul prelucrării într-o anumită etapă de dezvoltare, autoritățile de supraveghere trebuie să se aștepte de la operator(i) la un anumit grad de detaliere și la o explicație a modului în care aceste detalii contribuie la scopul prelucrării. Aceasta poate include, de exemplu, informații despre tipul de model de IA dezvoltat, funcționalitățile lui preconizate și orice alt context relevant deja cunoscut în etapa respectivă. Contextul implementării poate include, de asemenea, de exemplu, dacă un model este dezvoltat pentru implementare internă, dacă operatorul intenționează să vândă sau să distribuie

„Articolul 29” privind transparența în temeiul Regulamentului 2016/679, revizuite și adoptate la 11 aprilie 2018, aprobate de CEPD la 25 mai 2018, punctul 2.

[43] Orientările Grupului de lucru Articolul 29 privind transparența în temeiul Regulamentului 2016/679, revizuite și adoptate la 11 aprilie 2018, aprobate de CEPD la 25 mai 2018, punctul 5.

[44] Vezi și considerentul 39 din RGPD potrivit căruia „*ar trebui să fie transparent pentru persoanele fizice că sunt colectate, utilizate, consultate sau prelucrate în alt mod datele cu caracter personal care le privesc și în ce măsură datele cu caracter personal sunt sau vor fi prelucrate [...]*”.

[45] Articolul 13 alineatul (2) litera (f) din RGPD și articolul 14 alineatul (2) litera (g) din RGPD.

[46] Raportul CEPD privind activitatea desfășurată de grupul operativ ChatGPT, adoptat la 23 mai 2024, punctul 27.

[47] În plus, articolul 10 alineatul (5) din Regulamentul privind inteligența artificială prevede norme specifice pentru prelucrarea categoriilor speciale de date cu caracter personal în legătură cu sistemele de inteligență artificială cu risc ridicat, în scopul de a asigura detectarea și corectarea prejudecăților.

[48] Avizul nr. 3/2013 al Grupului de lucru „Articolul 29” privind limitările legate de scop (WP203), p. 15-16.

modelul la terți după dezvoltarea lui, inclusiv dacă modelul este destinat în principal implementării în scopuri de cercetare sau comerciale.

65. **Drepturile persoanelor vizate** (capitolul III din RGPD) - În pofida necesității ca autoritățile de supraveghere să se asigure că toate drepturile persoanelor vizate sunt respectate atunci când sunt dezvoltate modele de inteligență artificială și implementate de operatori, CEPD reamintește că, ori de câte ori un operator invocă interesul legitim ca temei legal, dreptul de opoziție prevăzut la articolul 21 din RGPD se aplică și trebuie asigurat[49].

3.3.2 Considerații cu privire la cele trei etape ale evaluării interesului legitim în contextul dezvoltării și implementării modelelor de IA

66. Pentru a determina dacă o anumită prelucrare a datelor cu caracter personal se poate baza pe articolul 6 alineatul (1) litera (f) din RGPD, autoritățile de supraveghere trebuie să verifice dacă operatorii au evaluat cu atenție și au documentat dacă sunt îndeplinite următoarele trei condiții cumulative: (i) urmărirea unui interes legitim de către operator sau de către un terț; (ii) prelucrarea este necesară pentru urmărirea interesului legitim; și (iii) interesele sau drepturile și libertățile fundamentale ale persoanelor vizate nu prevalează asupra interesului legitim[50].

3.3.2.1 Prima etapă - Urmărirea unui interes legitim de către operator sau de către un terț

67. Un interes este interesul mai larg sau beneficiul pe care un operator sau un terț îl poate avea în a se implica într-o anumită activitate de prelucrare[51]. Deși RGPD și CJUE au recunoscut mai multe interese ca legitime[52], evaluarea legitimității unui anumit interes trebuie să fie rezultatul unei analize de la caz la caz.

68. După cum a reamintit CEPD în Orientările sale privind interesul legitim[53], un interes poate fi considerat legitim dacă sunt îndeplinite în mod cumulativ următoarele trei criterii:

    a. Interesul este legal[54];

---

[49] Conform articolului 21 din RGPD, dacă o persoană vizată se opune, din motive legate de situația sa particulară, prelucrării datelor cu caracter personal care o privesc, operatorul nu mai prelucrează datele cu caracter personal, cu excepția cazului în care operatorul demonstrează că există motive legitime și imperioase pentru prelucrare care prevalează asupra intereselor, drepturilor și libertăților persoanei vizate sau pentru constatarea, exercitarea sau apărarea unui drept în justiție. Prin urmare, cele două aspecte care trebuie luate în considerare de autoritățile de supraveghere sunt dacă operatorul poate să demonstreze existența unor astfel de motive legitime imperioase și prioritare și dacă poate fi exercitat dreptul de opoziție.

[50] CJUE, hotărârea din 4 iulie 2023, cauza C-252/21, *Meta v. Bundeskartellamt* (ECLI:EU:C:2023:537), punctul 106; CJUE, hotărârea din 11 decembrie 2019, cauza C-708/18, *Asociația de Proprietari bloc M5A-Scara A* (ECLI:EU:C:2019:1064), punctul 40. Vezi și Orientările CEPD nr. 1/2024 privind prelucrarea datelor cu caracter personal în temeiul articolului 6 alineatul (1) litera (f) din RGPD, versiunea 1.0 adoptată la 8 octombrie 2024, punctul 12 și următoarele. După cum se reamintește în aceste orientări, această *„evaluare trebuie efectuată la începutul prelucrării, cu implicarea responsabilului cu protecția datelor (RPD) (dacă este desemnat) și trebuie documentată de operator conform principiului responsabilității prevăzut la articolul 5 alineatul (2) din RGPD"*.

[51] Orientările CEPD nr. 1/2024 privind prelucrarea datelor cu caracter personal în temeiul articolului 6 alineatul (1) litera (f) din RGPD, versiunea 1.0, adoptate la 8 octombrie 2024, punctul 14.

[52] Orientările CEPD nr. 1/2024 privind prelucrarea datelor cu caracter personal în temeiul articolului 6 alineatul (1) litera (f) din RGPD, versiunea 1.0, adoptate la 8 octombrie 2024, punctul 16.

[53] Orientările CEPD nr. 1/2024 privind prelucrarea datelor cu caracter personal în temeiul articolului 6 alineatul (1) litera (f) din RGPD, versiunea 1.0, adoptate la 8 octombrie 2024, punctul 17.

[54] CJUE, hotărârea din 4 octombrie 2024, cauza C-621/22, *Koninklijke Nederlandse Lawn Tennisbond* (ECLI:EU:C:2024:857), punctul 49, în care CJUE a subliniat că un interes legitim nu poate fi contrar legii. În acest

b. Interesul este articulat în mod clar și precis; și

c. Interesul este real și prezent, nu speculativ.

69. Sub rezerva celorlalte două etape impuse de evaluarea interesului legitim, următoarele exemple pot constitui un interes legitim în contextul modelelor de IA: (i) dezvoltarea serviciului unui agent conversațional pentru a asista utilizatorii; (ii) dezvoltarea unui sistem de IA pentru a detecta conținut sau comportament fraudulos; și (iii) îmbunătățirea detectării amenințărilor într-un sistem informatic.

3.3.2.2 A doua etapă - Analiza necesității prelucrării datelor pentru urmărirea interesului legitim

70. A doua etapă a evaluării constă în a stabili dacă prelucrarea datelor cu caracter personal este necesară în scopul interesului (intereselor) legitim(e) urmărit(e)[55] („testul necesității").

71. Considerentul 39 din RGPD prevede că „*Datele cu caracter personal ar trebui prelucrate doar dacă scopul prelucrării nu poate fi îndeplinit în mod rezonabil prin alte mijloace*". Potrivit CJUE și orientărilor anterioare ale CEPD, condiția referitoare la necesitatea prelucrării trebuie examinată în lumina drepturilor și libertăților fundamentale ale persoanelor vizate și în coroborare cu principiul minimizării datelor consacrat la articolul 5 alineatul (1) litera (c) din RGPD[56].

72. Metodologia menționată de CJUE ia în considerare contextul prelucrării, precum și efectele asupra operatorului și asupra persoanelor vizate. Prin urmare, evaluarea necesității implică două elemente:

sens, CEPD subliniază că, după caz, cadrele legislative trebuie luate în considerare când se evaluează legalitatea unui anumit interes. Vezi de exemplu: Articolul 26 alineatul (3) și articolul 28 din Regulamentul (UE) 2022/2065 al Parlamentului European și al Consiliului din 19 octombrie 2022 privind o piață unică pentru serviciile digitale și de modificare a Directivei 2000/31/CE (Regulamentul privind serviciile digitale) („DSA") privind publicitatea direcționată interzisă destinată minorilor, articolul 5 alineatul (1) și alineatul (2) din Regulamentul privind inteligența artificială referitor la practicile de IA interzise (practici de manipulare și sub pragul de conștiință), prelucrarea care încalcă drepturile de proprietate intelectuală și dispozițiile Directivei (UE) 2019/790 privind drepturile de autor și drepturile conexe pe piața unică digitală.

[55] Orientările CEPD nr. 1/2024 privind prelucrarea datelor cu caracter personal în temeiul articolului 6 alineatul (1) litera (f) din RGPD, versiunea 1.0, adoptate la 8 octombrie 2024, punctele 28-30.

[56] CJUE, hotărârea din 4 iulie 2023, cauza C-252/21, *Meta c. Bundeskartellamt* (ECLI:EU:C:2023:537), punctele 108 și 109, făcând trimitere și la CJUE, hotărârea din 11 decembrie 2019, cauza C-708/18, *Asociația de Proprietari bloc M5A-Scara A* (ECLI:EU:C:2019:1064), punctul 48; CJUE, hotărârea din 9 noiembrie 2010, cauzele conexate C-92/09 și C-93/09, Volker und Markus Schecke (ECLI:EU:C:2010:662), punctele 85 și 86; CJUE, hotărârea din 22 iunie 2021, cauza C-439/19, *Latvijas Republikas Saeima* (ECLI:EU:C:2021:504), punctele 98, 109, 110, 113. Vezi, de exemplu: Orientările CEPD nr. 3/2019 privind prelucrarea datelor cu caracter personal prin mijloace video, versiunea 2.0, adoptate la 29 ianuarie 2020, punctele 24-26 și 73; Orientările CEPD nr. 2/2019 privind prelucrarea datelor cu caracter personal în temeiul articolului 6 alineatul (1) litera (b) din RGPD în contextul furnizării de servicii online persoanelor vizate, versiunea 2.0, adoptate la 8 octombrie 2019, punctele 23-25; Avizul CEPD nr. 11/2024 privind utilizarea recunoașterii faciale pentru simplificarea fluxului de pasageri din aeroport, versiunea 1.1, adoptat la 23 mai 2024, punctul 27.

(i) dacă activitatea de prelucrare va permite urmărirea scopului[57] și (ii) dacă nu există o metodă mai puțin intruzivă de a urmări acest scop[58].

73. De exemplu, și, după caz, volumul preconizat de date cu caracter personal implicate în modelul de IA trebuie evaluat în lumina alternativelor mai puțin intruzive care pot fi disponibile în mod rezonabil pentru a atinge la fel de eficient scopul interesului legitim urmărit. Dacă urmărirea scopului este posibilă și printr-un model de IA care nu implică prelucrarea de date cu caracter personal, atunci prelucrarea datelor cu caracter personal trebuie considerată ca nefiind necesară. Acest lucru este deosebit de relevant pentru dezvoltarea modelelor de IA. Când evaluează dacă este îndeplinită condiția necesității, autoritățile de supraveghere trebuie să acorde o atenție deosebită volumului de date cu caracter personal prelucrate și dacă urmărirea interesului legitim în cauză este proporțională, având în vedere, de asemenea, principiul reducerii la minimum a datelor.

74. Evaluarea necesității trebuie să țină seama și de contextul mai larg al prelucrării preconizate a datelor cu caracter personal. Existența unor mijloace mai puțin intruzive pentru drepturile și libertățile fundamentale ale persoanelor vizate poate varia în funcție de existența unei relații directe a operatorului cu persoanele vizate (date ale primei părți) sau nu (date ale terților). CJUE a furnizat câteva considerații de care trebuie ținut cont când se analizează necesitatea prelucrării datelor primei părți în scopul interesului (intereselor) legitim(e) urmărit(e) (deși în contextul divulgării unor astfel de date către terți)[59].

75. Aplicarea unor garanții tehnice pentru protecția datelor cu caracter personal poate contribui și la îndeplinirea testului de necesitate. Aceasta ar putea include, de exemplu, măsuri de punere în aplicare precum cele identificate în secțiunea 3.2.2, în așa fel încât anonimizarea nu este atinsă, dar care reduce totuși ușurința cu care pot fi identificate persoanele vizate. CEPD constată că unele dintre aceste măsuri, când nu sunt necesare pentru respectarea RGPD, pot constitui garanții suplimentare, astfel cum se analizează în continuare în subsecțiunea „măsuri de atenuare", din secțiunea 3.3.2.3[60].

---

[57] Vezi CJUE, hotărârea din 16 decembrie 2008, cauza C-524/06, *Heinz Huber împotriva Bundesrepublik Deutschland* (ECLI:EU:C:2008:724), punctul 66. De asemenea, în aceeași cauză, vezi concluziile avocatului general Poiares Maduro în cauza C-524/06, *Heinz Huber împotriva Bundesrepublik Deutschland* (ECLI:EU:C:2008:194), punctul 16, care precizează: *„în speță, criteriul adecvat este cel al eficienței și că instanța națională este cea care trebuie să îl aplice. Aceasta trebuie să își pună întrebarea dacă există alte moduri de prelucrare a datelor prin care autoritățile competente în domeniul imigrării pot să asigure aplicarea normelor privind regimul dreptului de ședere. Dacă răspunsul la această întrebare este afirmativ, stocarea și prelucrarea centralizate ale datelor cetățenilor Uniunii trebuie să fie declarate nelegale. Nu este necesar ca sistemul alternativ să fie cel mai eficient sau cel mai adecvat; este suficient numai ca acesta să poată funcționa în mod corespunzător. Cu alte cuvinte, chiar dacă registrul central este mai eficient, mai accesibil sau mai ușor de utilizat decât alternativele sale (precum registrele locale descentralizate), acestea din urmă trebuie preferate dacă pot fi utilizate pentru a indica statutul cetățenilor Uniunii în ceea ce privește dreptul de ședere".*

[58] Vezi CJUE, hotărârea din 27 septembrie 2017, cauza C-73/16, *Peter Puškár* (ECLI:EU:C:2017:725), punctul 113: *„Revine, așadar, instanței de trimitere sarcina de a verifica dacă întocmirea listei în litigiu și înscrierea în aceasta a numelui persoanelor în cauză sunt de natură să realizeze obiectivele urmărite prin acestea și dacă nu există alte mijloace mai puțin restrictive pentru atingerea acestor obiective*"; vezi și Concluziile avocatului general Rantos în cauza C-252/21, *Meta/Bundeskartellamt*, ECLI:EU:C:2022:704, punctul 61, în care se precizează: *„[...] Prin urmare, este necesar să existe o legătură strânsă între prelucrare și interesul urmărit, în absența unor alternative care să fie mai favorabile protecției datelor, întrucât nu este suficient ca prelucrarea să fie pur și simplu utilă operatorului*".

[59] CJUE, hotărârea din 4 octombrie 2024, cauza C-621/22, *Koninklijke Nederlandse Lawn Tennisbond* (ECLI:EU:C:2024:857), punctele 51-53.

[60] Vezi Orientările CEPD nr. 1/2024 privind prelucrarea datelor cu caracter personal în temeiul articolului 6 alineatul (1) litera (f) din RGPD, versiunea 1.0, adoptate la 8 octombrie 2024, punctul 57.

3.3.2.3 A treia etapă – Testul comparativ

76. A treia etapă a evaluării interesului legitim este „**exercițiul comparativ”** (numit în acest document și „**testul comparativ**”)[61]. Această etapă constă în identificarea și descrierea diferitelor drepturi și interese opuse aflate în joc[62], și anume, pe de o parte, interesele, drepturile și libertățile fundamentale ale persoanelor vizate și, pe de alta, interesele operatorului sau ale unui terț. Trebuie analizate apoi circumstanțele specifice ale cazului pentru a demonstra că interesul legitim este un temei legal adecvat pentru activitățile de prelucrare în cauză[63].

Interesele, drepturile și libertățile fundamentale ale persoanelor vizate

77. Articolul 6 alineatul (1) litera (f) din RGPD prevede că, la evaluarea diferitelor componente în contextul testului comparativ, operatorul trebuie să ia în considerare interesele, drepturile și libertățile fundamentale ale persoanelor vizate. Interesele persoanelor vizate sunt cele care pot fi afectate de prelucrarea în cauză. În contextul fazei de dezvoltare a unui model de IA, acestea pot include, dar nu se limitează la interesul de autodeterminare și de păstrare a controlului asupra propriilor date personale (de exemplu, datele culese pentru dezvoltarea modelului). În contextul implementării unui model de IA, interesele persoanelor vizate pot include, dar fără a se limita la acestea, interese în menținerea controlului asupra propriilor date personale (de exemplu, datele prelucrate după implementarea modelului), interese financiare (de exemplu, când un model de IA este utilizat de persoana vizată pentru a genera venituri sau este utilizat de o persoană în contextul activității sale profesionale), beneficii personale (de exemplu, când un model de IA se folosește pentru a îmbunătăți accesibilitatea anumitor servicii) sau interese socioeconomice (de exemplu, când un model de IA permite accesul la o asistență medicală mai bună sau facilitează exercitarea unui drept fundamental, de exemplu accesul la educație)[64].

78. Cu cât un interes este definit mai precis în funcție de scopul urmărit al prelucrării, cu atât mai bine va permite să se înțeleagă clar realitatea beneficiilor și a riscurilor care trebuie luate în considerare în testul comparativ.

79. Cât privește drepturile și libertățile fundamentale ale persoanelor vizate, dezvoltarea și implementarea modelelor de IA pot genera riscuri grave la adresa drepturilor protejate de Carta drepturilor fundamentale a UE („**Carta UE**”), inclusiv, dar fără a se limita la, dreptul la viață privată și de familie (articolul 7 din Carta UE) și dreptul la protecția datelor cu caracter personal (articolul 8 din Carta UE). Aceste riscuri pot apărea în faza de dezvoltare, de exemplu când datele cu caracter personal sunt extrase împotriva voinței persoanelor vizate sau fără știrea lor. Aceste riscuri pot apărea și în faza de implementare, de exemplu când datele cu caracter personal sunt prelucrate de model (sau ca parte a acestuia) într-un mod care contravine drepturilor persoanelor vizate sau când se poate deduce, întâmplător sau prin atacuri (de exemplu, prin deducerea apartenenței, extragere sau inversiunea modelului), care sunt datele cu caracter personal conținute în baza de date pentru învățare. Aceste situații prezintă un risc pentru viața privată a persoanelor vizate ale căror date ar putea apărea în faza

[61] Vezi Orientările CEPD nr. 1/2024 privind prelucrarea datelor cu caracter personal în temeiul articolului 6 alineatul (1) litera (f) din RGPD, versiunea 1.0, adoptate la 8 octombrie 2024, punctele 31-60.
[62] Vezi Orientările CEPD nr. 1/2024 privind prelucrarea datelor cu caracter personal în temeiul articolului 6 alineatul (1) litera (f) din RGPD, versiunea 1.0, adoptate la 8 octombrie 2024, punctul 32.
[63] Vezi Orientările CEPD nr. 1/2024 privind prelucrarea datelor cu caracter personal în temeiul articolului 6 alineatul (1) litera (f) din RGPD, versiunea 1.0, adoptate la 8 octombrie 2024, punctul 32, făcând trimitere și la CJUE, hotărârea din 4 iulie 2023, cauza C-252/21, *Meta v. Bundeskartellamt* (ECLI:EU:C:2023:537), punctul 110.
[64] Vezi Orientările CEPD nr. 1/2024 privind prelucrarea datelor cu caracter personal în temeiul articolului 6 alineatul (1) litera (f) din RGPD, versiunea 1.0, adoptate la 8 octombrie 2024, punctul 38.

de implementare a sistemului de IA (de exemplu, risc reputațional, furt de identitate sau fraudă, risc de securitate în funcție de natura datelor).

80. În funcție de caz, pot exista riscuri și pentru alte drepturi fundamentale. De exemplu, culegerea de date la scară largă și fără discriminare de către modelele de IA în faza de dezvoltare poate induce persoanelor vizate un sentiment de supraveghere, în special având în vedere dificultățile de a împiedica extragerea datelor publice. Acest lucru poate determina persoanele să se autocenzureze și poate prezenta riscuri de subminare a libertății lor de exprimare (articolul 11 din Carta UE). În faza de implementare, riscurile pentru libertatea de exprimare sunt prezente și când modelele de IA se folosesc pentru a bloca publicarea conținutului de către persoanele vizate. În plus, un model de IA care recomandă persoanelor vulnerabile conținut inadecvat poate prezenta riscuri pentru sănătatea lor psihică [articolul 3 alineatul (1) din Carta UE]. În alte cazuri, utilizarea modelelor de IA poate avea consecințe negative asupra dreptului individului de a se angaja în muncă (articolul 15 din Carta UE), de exemplu când cererile de locuri de muncă sunt preselectate cu un model de IA. În același mod, un model de IA poate prezenta riscuri pentru dreptul la nediscriminare (articolul 21 din Carta UE), dacă discriminează persoanele pe baza anumitor caracteristici personale (de exemplu, cetățenia sau sexul). În plus, implementarea modelelor de IA poate prezenta, de asemenea, riscuri pentru securitatea și siguranța persoanelor (de exemplu, când modelul de IA este folosit cu intenție răuvoitoare), precum și riscuri pentru integritatea lor fizică și psihică[65].

81. Implementarea modelelor de IA poate avea și un impact pozitiv asupra anumitor drepturi fundamentale, de exemplu, modelul poate sprijini dreptul la integritatea psihică a persoanei (articolul 3 din Cartă), de exemplu când un model de IA se folosește pentru a identifica conținut dăunător online; sau modelul poate facilita accesul la anumite servicii esențiale sau poate facilita exercitarea drepturilor fundamentale, de exemplu accesul la informații (articolul 11 din Carta UE) sau accesul la educație (articolul 14 din Carta UE).

Impactul prelucrării asupra persoanelor vizate

82. Prelucrarea datelor cu caracter personal care are loc în timpul dezvoltării și implementării modelelor de IA poate afecta persoanele vizate în diferite moduri, care pot fi pozitive sau negative[66]. De exemplu, dacă o activitate de prelucrare implică beneficii pentru persoana vizată, ele pot fi luate în considerare în testul comparativ. Deși existența acestor beneficii poate duce la concluzia unei autorități de supraveghere că interesele, drepturile și libertățile fundamentale ale persoanelor vizate nu prevalează asupra intereselor operatorului sau ale unui terț, această concluzie poate fi doar rezultatul unei analize de la caz la caz, luând în considerare toți factorii corespunzători.

83. Impactul prelucrării asupra persoanelor vizate poate fi influențat de (i) natura datelor prelucrate de modele; (ii) contextul prelucrării; și (iii) consecințele suplimentare pe care le poate avea prelucrarea[67].

84. În ceea ce privește **natura datelor prelucrate**, trebuie reamintit că – pe lângă categoriile speciale de date cu caracter personal și datele referitoare la condamnări penale și infracțiuni care beneficiază de protecție suplimentară în temeiul articolelor 9 și, respectiv, 10 din RGPD – prelucrarea altor categorii de date cu caracter personal poate avea consecințe semnificative pentru persoanele vizate. În acest context, prelucrarea anumitor tipuri de date cu caracter personal care dezvăluie informații foarte

[65] Orientările nr. 1/2024 privind prelucrarea datelor cu caracter personal în temeiul articolului 6 alineatul (1) litera (f) din RGPD, versiunea 1.0, adoptate la 8 octombrie 2024, punctul 46.
[66] Vezi Orientările CEPD nr. 1/2024 privind prelucrarea datelor cu caracter personal în temeiul articolului 6 alineatul (1) litera (f) din RGPD, versiunea 1.0, adoptate la 8 octombrie 2024, punctul 39.
[67] Vezi Orientările CEPD nr. 1/2024 privind prelucrarea datelor cu caracter personal în temeiul articolului 6 alineatul (1) litera (f) din RGPD, versiunea 1.0, adoptate la 8 octombrie 2024, punctul 32.

private (de exemplu, date financiare sau date de localizare) pentru dezvoltarea și implementarea unui model de IA ar trebui considerată ca având un posibil impact grav asupra persoanelor vizate. În faza de implementare, consecințele unei asemenea prelucrări pentru persoanele vizate pot fi, de exemplu, economice (de exemplu, discriminarea în contextul ocupării forței de muncă) și/sau reputaționale (de exemplu, defăimarea).

85. În ce privește **contextul prelucrării,** în primul rând trebuie identificate elementele care ar putea crea riscuri pentru persoanele vizate (de exemplu, cum a fost dezvoltat modelul, cum poate fi utilizat modelul și/sau dacă măsurile de securitate luate pentru protecția datelor cu caracter personal sunt adecvate). Natura modelului și utilizările operaționale preconizate joacă un rol esențial în identificarea acestor cauze potențiale.

86. De asemenea, trebuie evaluată gravitatea acestor riscuri pentru persoanele vizate. Printre altele se pot lua în considerare modul în care sunt prelucrate datele cu caracter personal (de exemplu, dacă sunt combinate cu alte seturi de date), care este amploarea prelucrării și cantitatea de date cu caracter personal prelucrate[68] (de exemplu, volumul total de date, volumul de date pentru fiecare persoană vizată, numărul de persoane vizate afectate)[69], statutul persoanei vizate (de exemplu, copiii sau alte persoane vizate vulnerabile) și relația lor cu operatorul (de exemplu, dacă persoana vizată este un client). De exemplu, utilizarea extragerii de date web în faza de dezvoltare poate duce - în lipsă de garanții suficiente - la efecte considerabile asupra persoanelor fizice, din cauza volumului mare de date culese, a numărului mare de persoane vizate și a culegerii nediscriminatorii de date cu caracter personal.

87. **Consecințele suplimentare** pe care le-ar putea avea prelucrarea trebuie, de asemenea, luate în considerare când se evaluează impactul prelucrării asupra persoanelor vizate. Acestea trebuie evaluate de autoritățile de supraveghere de la caz la caz, în funcție de faptele specifice în cauză.

88. Asemenea consecințe pot include (dar nu se limitează la) riscuri de încălcare a drepturilor fundamentale ale persoanelor vizate, astfel cum se descrie în subsecțiunea anterioară[70]. Riscurile pot varia ca probabilitate și gravitate și pot rezulta din prelucrarea datelor cu caracter personal care ar putea duce la daune fizice, materiale sau morale, în special când prelucrarea poate da naștere la discriminare[71].

89. În cazul în care implementarea unui model de IA implică prelucrarea datelor cu caracter personal atât ale (i) persoanelor vizate ale căror date cu caracter personal sunt incluse în setul de date utilizat în faza de dezvoltare, cât și ale (ii) persoanelor vizate ale căror date cu caracter personal sunt prelucrate în faza de implementare, autoritățile de supraveghere trebuie să distingă și să ia în considerare riscurile care afectează interesele, drepturile și libertățile fiecăreia dintre aceste categorii de persoane vizate când verifică testul comparativ efectuat de un operator.

90. **În sfârșit, analiza posibilelor consecințe suplimentare ale prelucrării trebuie să ia în considerare și probabilitatea de materializare a acestor consecințe suplimentare**. Evaluarea acestei probabilități trebuie efectuată luând în considerare măsurile tehnice și organizatorice în vigoare și circumstanțele specifice ale cazului. De exemplu, autoritățile de supraveghere pot analiza dacă s-au luat măsuri pentru

[68] Vezi Orientările CEPD nr. 1/2024 privind prelucrarea datelor cu caracter personal în temeiul articolului 6 alineatul (1) litera (f) din RGPD, versiunea 1.0, adoptate la 8 octombrie 2024, punctul 43.
[69] CJUE, hotărârea din 4 iulie 2023, cauza C-252/21, *Meta v. Bundeskartellamt* (ECLI:EU:C:2023:537), punctul 116.
[70] Vezi subsecțiunea „Interesele, drepturile și libertățile fundamentale ale persoanelor vizate" de mai sus.
[71] Vezi secțiunea 2.3 din Orientările CEPD nr. 1/2024 privind prelucrarea datelor cu caracter personal în temeiul articolului 6 alineatul (1) litera (f) din RGPD, versiunea 1.0, adoptate la 8 octombrie 2024. Vezi și considerentul 75 din RGPD pentru exemple suplimentare.

a evita o potențială utilizare abuzivă a modelului de IA. Pentru modelele de IA care pot fi folosite în diverse scopuri, de exemplu inteligența artificială generativă, aceasta poate include controale care să limiteze pe cât posibil folosirea lor la practici dăunătoare, de exemplu: crearea de deepfake-uri; chatbot-uri care se folosesc la dezinformare, phishing și alte tipuri de fraudă; și agenți IA/IA manipulativi (în special când sunt antropomorfi sau furnizează informații înșelătoare).

Așteptările rezonabile ale persoanelor vizate

91. Pe baza considerentului 47 din RGPD, *„[î]n orice caz, existența unui interes legitim ar necesita o evaluare atentă, care să stabilească inclusiv dacă o persoană vizată poate preconiza în mod rezonabil, în momentul și în contextul colectării datelor cu caracter personal, posibilitatea prelucrării în acest scop. Interesele și drepturile fundamentale ale persoanei vizate ar putea prevala în special în raport cu interesul operatorului de date atunci când datele cu caracter personal sunt prelucrate în circumstanțe în care persoanele vizate nu preconizează în mod rezonabil o prelucrare ulterioară”*[72].

92. Așteptările rezonabile joacă un rol-cheie în testul comparativ, nu în ultimul rând din cauza complexității tehnologiei folosite în modelele de IA și a faptului că pentru persoanele vizate poate fi dificil să înțeleagă varietatea de utilizări potențiale ale unui model de IA și prelucrarea datelor implicată[73]. În acest scop, informațiile furnizate persoanelor vizate pot fi luate în considerare pentru a evalua dacă persoanele vizate se pot aștepta în mod rezonabil ca datele lor cu caracter personal să fie prelucrate. Cu toate acestea, deși omiterea de informații poate contribui la faptul că persoanele vizate nu se așteaptă la o anumită prelucrare, simpla îndeplinire a cerințelor de transparență prevăzute în RGPD nu este suficientă în sine pentru a considera că persoanele vizate se pot aștepta în mod rezonabil la o anumită prelucrare[74]. În plus, simplul fapt că informațiile referitoare la faza de dezvoltare a unui model de IA sunt incluse în politica de confidențialitate a operatorului nu înseamnă neapărat că persoanele vizate se pot aștepta în mod rezonabil ca acest lucru să se întâmple; mai degrabă, acest lucru trebuie analizat de autoritățile de supraveghere în funcție de circumstanțele specifice ale cazului și luând în considerare toți factorii relevanți.

93. Când se evaluează așteptările rezonabile ale persoanelor vizate în legătură cu prelucrarea care are loc în faza de dezvoltare, este important să se facă referire la elementele menționate în Orientările CEPD privind interesul legitim[75]. În plus, în cadrul obiectului prezentului aviz, este important de luat în considerare contextul mai larg al prelucrării. Acesta poate include, dar nu limitativ, dacă datele cu caracter personal au fost sau nu disponibile publicului, natura relației dintre persoana vizată și operator (și dacă există o legătură între cei doi), natura serviciului, contextul în care au fost culese datele cu caracter personal, sursa din care au fost culese datele (de exemplu, site-ul sau serviciul în care au fost culese datele cu caracter personal și setările de confidențialitate pe care le oferă),

[72] Vezi și CJUE, hotărârea din 4 iulie 2023, cauza C-252/21, *Meta v. Bundeskartellamt* (ECLI:EU:C:2023:537), punctul 112; CJUE, hotărârea din 11 decembrie 2019, cauza C-708/18, *Asociația de Proprietari bloc M5A-Scara A* (ECLI:EU:C:2019:1064), punctul 58; CJUE, hotărârea din 4 octombrie 2024, cauza C-621/22, *Koninklijke Nederlandse Lawn Tennisbond* (ECLI:EU:C:2024:857), punctul 55.

[73] De exemplu, în hotărârea din 4 iulie 2023, cauza C-252/21, *Meta c. Bundeskartellamt* (ECLI:EU:C:2023:537), punctul 123, deși CJUE a constatat că „îmbunătățirea produsului” nu poate fi exclusă, în principiu, ca interes legitim, aceasta a mai constatat că este *„îndoielnic ca [....] obiectivul privind îmbunătățirea produsului să poată, ținând seama de amploarea acestei prelucrări și de impactul important al acesteia asupra utilizatorului, precum și de împrejurarea că acesta din urmă nu se poate aștepta în mod rezonabil ca datele respective să fie prelucrate de Meta Platforms Ireland, să prevaleze asupra intereselor și a drepturilor fundamentale ale unui asemenea utilizator, cu atât mai mult în ipoteza în care acesta este un copil*”.

[74] Orientările nr. 1/2024 privind prelucrarea datelor cu caracter personal în temeiul articolului 6 alineatul (1) litera (f) din RGPD, versiunea 1.0, adoptate la 8 octombrie 2024, punctul 53.

[75] Orientările nr. 1/2024 privind prelucrarea datelor cu caracter personal în temeiul articolului 6 alineatul (1) litera (f) din RGPD, versiunea 1.0, adoptate la 8 octombrie 2024, punctele 50-54.

potențialele utilizări ulterioare ale modelului și dacă persoanele vizate sunt conștiente că datele lor cu caracter personal sunt online.

94. În faza de dezvoltare a modelului, așteptările rezonabile ale persoanelor vizate pot fi diferite în funcție de punerea sau nu la dispoziția publicului a datelor prelucrate pentru dezvoltarea modelului de către persoanele vizate. În plus, așteptările rezonabile pot diferi și în funcție de furnizarea directă sau nu către operator a datelor (de exemplu, în contextul utilizării serviciului) sau obținerea lor de către operator din altă sursă (de exemplu, printr-un terț sau prin extragerea de date web). În ambele cazuri, măsurile luate pentru a informa persoanele vizate cu privire la activitățile de prelucrare trebuie luate în considerare când se evaluează așteptările rezonabile.

95. În faza de implementare a modelului AI, este la fel de important să se ia în considerare așteptările rezonabile ale persoanelor vizate în contextul capacităților specifice ale modelului. De exemplu, pentru modelele de IA care se pot adapta în funcție de datele de intrare furnizate, poate fi relevant să se ia în considerare dacă persoanele vizate erau conștiente că au furnizat date cu caracter personal pentru ca modelul de IA să-și poată adapta răspunsurile la nevoile lor și să poată obține servicii adaptate. În plus, ar putea fi relevant și să se analizeze dacă această activitate de prelucrare ar afecta doar serviciul furnizat persoanelor vizate (de exemplu, personalizarea conținutului pentru un anumit utilizator) sau dacă ar fi folosit pentru a modifica serviciul furnizat tuturor clienților (de exemplu, pentru a îmbunătăți modelul în general). Ca și în etapa de dezvoltare, poate fi, de asemenea, deosebit de relevant să se analizeze dacă există o legătură directă între persoanele vizate și operator. O asemenea legătură directă poate, de exemplu, să permită operatorului să furnizeze cu ușurință persoanelor vizate informații cu privire la activitatea de prelucrare și la model, ceea ce ar putea influența ulterior așteptările rezonabile ale acestor persoane vizate.

Măsuri de atenuare

96. Atunci când interesele, drepturile și libertățile persoanelor vizate par să prevaleze asupra interesului sau intereselor legitime urmărite de operator sau de un terț, operatorul poate lua în considerare introducerea unor măsuri de atenuare pentru a limita impactul prelucrării asupra acestor persoane vizate. Măsurile de atenuare sunt garanții care trebuie să fie adaptate la circumstanțele cazului și să depindă de diferiți factori, inclusiv de utilizarea preconizată a modelului de IA. Aceste măsuri de atenuare ar urmări să asigure că interesele operatorului sau ale terțului nu vor fi anulate, pentru ca operatorul să se poată baza pe acest temei legal.

97. După cum se reamintește în Orientările CEPD privind interesul legitim, măsurile de atenuare nu trebuie confundate cu măsurile pe care operatorul este obligat prin lege să le adopte oricum pentru a asigura respectarea RGPD, indiferent dacă prelucrarea se bazează pe articolul 6 alineatul (1) litera (f) din RGPD[76]. Acest lucru este deosebit de important pentru măsurile care, de exemplu, trebuie să respecte principiile RGPD, de exemplu principiul minimizării datelor.

98. Lista măsurilor prezentate mai jos nu este exhaustivă și nu este prescriptivă, iar aplicarea măsurilor trebuie luată în considerare pe baza unei evaluări de la caz la caz. Deși, în funcție de circumstanțe, unele dintre măsurile de mai jos pot fi obligatorii pentru a respecta obligațiile specifice ale RGPD, când nu este cazul, ele pot fi luate în considerare ca garanții suplimentare. În plus, unele dintre măsurile menționate mai jos se referă la domenii care sunt supuse unei evoluții rapide și unor noi dezvoltări și trebuie luate în considerare de autoritățile de supraveghere când se ocupă de un caz specific.

[76] Orientările nr. 1/2024 privind prelucrarea datelor cu caracter personal în temeiul articolului 6 alineatul (1) litera (f) din RGPD, versiunea 1.0, adoptate la 8 octombrie 2024, punctul 57.

99. **<u>În ceea ce privește faza de dezvoltare a modelelor de IA</u>**, pot fi luate mai multe măsuri pentru a atenua riscurile prezentate de prelucrarea datelor atât ale primelor părți, cât și ale terților (inclusiv pentru a atenua riscurile legate de practicile de extragere de date de pe site-uri). Pe baza celor de mai sus, CEPD oferă câteva exemple de măsuri care se pot lua pentru a atenua riscurile identificate în testul comparativ și care trebuie luate în considerare de autoritățile de supraveghere când evaluează, de la caz la caz, anumite modele de IA.

100. **Măsuri tehnice:**

a. Măsurile menționate la secțiunea 3.2.2 care sunt adecvate pentru a atenua riscurile în joc, când aceste măsuri nu duc la anonimizarea modelului și nu sunt necesare pentru a respecta alte obligații RGPD sau în conformitate cu testul de necesitate (a doua etapă a evaluării interesului legitim).

101. În plus față de acestea, alte măsuri relevante pot include:

b. măsuri de pseudonimizare: ar putea include, de exemplu, măsuri de prevenire a oricărei combinații de date bazate pe identificatori individuali. Aceste măsuri pot să nu fie adecvate când autoritatea de supraveghere consideră că operatorul a demonstrat necesitatea rezonabilă de a culege date diferite despre o anumită persoană pentru dezvoltarea sistemului sau modelului de IA respectiv.

c. Măsuri de mascare a datelor cu caracter personal sau de înlocuire a lor cu date cu caracter personal false în setul de instruire (de exemplu, înlocuirea numelor și a adreselor de e-mail cu nume false și adrese de e-mail false). Această măsură poate fi deosebit de adecvată atunci când conținutul material real al datelor nu este relevant pentru prelucrarea globală (de exemplu, în antrenarea LLM).

102. **Măsuri care facilitează exercitarea drepturilor individuale:**

a. Respectarea unei perioade rezonabile de timp între culegerea unui set de date de antrenare și utilizarea lui. Această garanție suplimentară poate permite persoanelor vizate să-și exercite drepturile în această perioadă, perioada de timp rezonabilă fiind evaluată în funcție de circumstanțele fiecărui caz.

b. Propunerea unei „clauze de neparticipare” necondiționate încă de la început, de exemplu acordând persoanelor vizate un drept discreționar de opoziție înainte să aibă loc prelucrarea, pentru a întări controlul persoanelor fizice asupra datelor lor, ceea ce depășește condițiile prevăzute la articolul 21 din RGPD[77].

c. permiterea persoanelor vizate să-și exercite dreptul la ștergerea datelor chiar și atunci când nu se aplică motivele specifice enumerate la articolul 17 alineatul (1) din RGPD[78];

d. Permiterea persoanelor vizate să prezinte reclamații privind regurgitarea sau memorarea datelor cu caracter personal, precum și circumstanțele și mijloacele prin care reclamațiile pot fi reproduse, permițând operatorilor să reproducă și să evalueze tehnicile relevante de dezvățare pentru a răspunde reclamațiilor.

103. **Măsuri de transparență:** în unele cazuri, măsurile de atenuare pot fi măsuri care să asigure o mai mare transparență în ceea ce privește dezvoltarea modelului de IA. Unele măsuri, pe lângă respectarea

[77] Ibid.
[78] Ibid.

obligațiilor prevăzute în RGPD, pot contribui la depășirea asimetriei informațiilor și pot permite persoanelor vizate să înțeleagă mai bine prelucrarea implicată în faza de dezvoltare:

a. Publicarea de comunicări publice și ușor accesibile care depășesc informațiile solicitate în temeiul articolului 13 sau 14 din RGPD, de exemplu prin furnizarea de detalii suplimentare privind criteriile de culegere și seturile de date utilizate, ținând seama de protecția specială a copiilor și a persoanelor vulnerabile.

b. Forme alternative de informare a persoanelor vizate, de exemplu: campanii media cu diferite canale mass-media pentru a informa persoanele vizate, campanii de informare prin e-mail, folosirea de vizualizări grafice, întrebări frecvente, etichete de transparență și carduri-model a căror sistematizare ar putea structura prezentarea informațiilor privind modelele de IA, precum și rapoartele anuale de transparență pe bază voluntară.

104. **Măsuri specifice de atenuare în contextul extragerii de date de pe site-uri:** Având în vedere că, după cum s-a menționat mai sus, extragerea datelor de pe site-uri generează riscuri specifice[79], s-ar putea identifica măsuri specifice de atenuare în acest context. După caz, pot fi luate în considerare de autoritățile de supraveghere, în plus față de măsurile de atenuare menționate mai sus, când investighează operatorii care efectuează activități de extragere de date de pe web.

105. Măsurile specifice, când nu sunt necesare în a doua etapă a evaluării interesului legitim, se pot dovedi utile pentru atenuarea riscului în contextul extragerii de date web. Acestea pot fi **măsuri tehnice**, de exemplu:

a. să se excludă conținutul de date din publicații care ar putea include date cu caracter personal care implică riscuri pentru anumite persoane sau categorii de persoane (de exemplu, persoane care ar putea fi victime de abuzuri, prejudecăți sau chiar vătămări fizice dacă informațiile ar fi făcute publice);

b. să se asigure că anumite categorii de date nu sunt culese sau că anumite surse sunt excluse de la culegerea datelor; aceasta ar putea include, de exemplu, anumite site-uri care sunt deosebit de intruzive din cauza sensibilității obiectului lor.

c. să se excludă culegerea de pe site-uri (sau secțiuni ale site-urilor) care se opun în mod clar extragerii de date web și reutilizării conținutului lor în scopul creării de baze de date de formare pentru inteligența artificială (de exemplu, respectând fișierele robots.txt sau ai.txt sau alte mecanisme recunoscute pentru a exprima excluderea de la crawling sau extragerea automată a datelor).

d. Să se impună alte limite relevante privind culegerea, inclusiv, eventual, a unor criterii bazate pe perioade de timp.

106. În contextul extragerii de date de pe web, exemple de măsuri specifice **care facilitează exercitarea drepturilor persoanelor fizice și transparența** pot fi: crearea unei liste de excludere voluntară, gestionată de operator și care permite persoanelor vizate să se opună culegerii datelor lor pe anumite

[79] Aceste practici pot ridica și probleme suplimentare, care nu sunt abordate în prezentul aviz, vezi, de exemplu, Pagallo U., Ciani Sciolla J., *Anatomy of web data scraping: ethics, standards, and the troubles of the law.* European Journal of Privacy Law & Technologies, (2023) 2 p. 1-19, disponibil la : https://doi.org/10.57230/EJPLT232PS.

site-uri sau platforme online prin furnizarea de informații care le identifică pe site-urile respective, inclusiv înainte de culegerea datelor[80].

107. **<u>Considerații specifice privind măsurile de atenuare în faza de desfășurare</u>:** Deși unele dintre măsurile menționate mai sus pot fi relevante și pentru faza de desfășurare, în funcție de circumstanțe, CEPD furnizează mai jos o listă neexhaustivă de măsuri suplimentare de sprijin care pot fi puse în aplicare și care trebuie evaluate de autoritățile de supraveghere de la caz la caz.

    a. **Măsuri tehnice** pot fi instituite, de exemplu, pentru a preveni stocarea, regurgitarea sau generarea de date cu caracter personal, în special în contextul modelelor generative de IA (cum ar fi filtrele de ieșire), și/sau pentru a reduce riscul reutilizării ilegale de către modelele de IA cu scop general (de exemplu, filigranarea digitală a rezultatelor generate de IA).

    b. **Măsuri care facilitează sau accelerează exercitarea drepturilor persoanelor fizice** în faza de implementare, dincolo de ceea ce prevede legea, în special în ceea ce privește, fără a se limita la acestea, exercitarea dreptului la ștergerea datelor cu caracter personal din datele de ieșire ale modelului sau eliminarea duplicărilor, precum și tehnicile ulterioare antrenării care încearcă să elimine sau să suprime datele cu caracter personal.

108. Când investighează implementarea unui anumit model de IA, autoritățile de supraveghere trebuie să analizeze dacă operatorul a publicat testul comparativ pe care l-a efectuat, deoarece acest lucru poate mări transparența și corectitudinea. După cum se menționează în Orientările CEPD privind interesul legitim, se pot lua în considerare alte măsuri pentru a furniza persoanelor vizate informații din testul comparativ înainte de orice culegere de date cu caracter personal[81]. De asemenea, CEPD reiterează[82] că un element care trebuie luat în considerare este dacă operatorul a implicat responsabilul cu protecția datelor, după caz.

3.4 Cu privire la impactul posibil al unei prelucrări ilegale în dezvoltarea unui model de IA asupra legalității prelucrării sau funcționării ulterioare a modelului de IA

109. În această secțiune a avizului se răspunde la întrebarea 4 din cerere. Prin această întrebare se solicită clarificări cu privire la posibilul impact al unei prelucrări ilegale în faza de dezvoltare asupra prelucrării ulterioare (de exemplu, în faza de implementare a modelului de IA) sau asupra funcționării modelului. Întrebarea urmărește să abordeze atât situația în care un astfel de model de IA prelucrează date cu caracter personal care sunt păstrate în model [întrebarea 4(i) din cerere], cât și situația în care nu mai este implicată nicio prelucrare a datelor cu caracter personal în implementarea modelului de IA (adică modelul este anonim) [întrebarea 4(ii) din cerere].

110. Înainte de a aborda anumite scenarii specifice, CEPD prezintă următoarele considerații generale.

111. În primul rând, clarificările furnizate în această secțiune se vor concentra pe prelucrarea datelor cu caracter personal în faza de dezvoltare, efectuată fără a respecta principiul legalității, așa cum prevede articolul 5 alineatul (1) litera (a) din RGPD și, în mod specific, articolul 6 din RGPD (denumit în

[80] Cu excepția cazului în care operatorul demonstrează motive legitime întemeiate pentru prelucrare, care prevalează asupra intereselor, drepturilor și libertăților persoanei vizate sau pentru stabilirea, exercitarea sau apărarea unor acțiuni în justiție.
[81] Orientările CEPD nr. 1/2024 privind prelucrarea datelor cu caracter personal în temeiul articolului 6 alineatul (1) litera (f) din RGPD, versiunea 1.0, adoptate la 8 octombrie 2024, punctul 68.
[82] Orientările CEPD nr. 1/2024 privind prelucrarea datelor cu caracter personal în temeiul articolului 6 alineatul (1) litera (f) din RGPD, versiunea 1.0, adoptate la 8 octombrie 2024, punctul 12.

continuare „**ilegalitatea**”)[83]. În aceeași ordine de idei, considerațiile CEPD se vor concentra pe impactul caracterului ilegal al prelucrării în faza de dezvoltare asupra legalității [și anume, respectarea articolului 5 alineatul (1) litera (a) din RGPD și a articolului 6 din RGPD] a prelucrării sau funcționării ulterioare a modelului. CEPD subliniază însă că prelucrarea efectuată în faza de dezvoltare poate duce și la încălcarea altor dispoziții ale RGPD, de exemplu lipsa de transparență față de persoanele vizate sau protecția datelor prin concepție și/sau implicit, care nu sunt analizate în prezentul aviz.

112. În al doilea rând, când se abordează această chestiune, principiul responsabilității, care impune operatorilor să fie responsabili și să demonstreze conformitatea, printre altele, cu articolul 5 alineatul (1) din RGPD și articolul 6 din RGPD[84], joacă un rol esențial. Acest lucru este valabil și pentru nevoia de a evalua ce organizație este operator pentru activitatea de prelucrare în cauză și dacă apar situații de exercitare în comun a competenței de operator (deoarece pot fi legate în mod indisolubil)[85]. Având în vedere importanța circumstanțelor de fapt ale fiecărui caz, inclusiv în ceea ce privește rolul jucat de fiecare parte implicată în prelucrare, considerațiile CEPD ar trebui înțelese ca observații generale care trebuie evaluate de la caz la caz de către autoritățile de supraveghere.

113. În al treilea rând, CEPD subliniază că, în conformitate cu articolul 51 alineatul (1) din RGPD, autoritățile de supraveghere sunt „*responsabile de monitorizarea aplicării [RGPD], în vederea protejării drepturilor și libertăților fundamentale ale persoanelor fizice în ceea ce privește prelucrarea și în vederea facilitării liberei circulații a datelor cu caracter personal în cadrul Uniunii”*. Prin urmare, este de competența autorităților de supraveghere să evalueze legalitatea prelucrării și să-și exercite competențele acordate prin RGPD conform cadrului lor național[86]. În aceste cazuri, autoritățile de supraveghere se bucură de puteri discreționare pentru a evalua posibilele încălcări și a alege măsuri adecvate, necesare și proporționale, dintre cele menționate la articolul 58 din RGPD, în funcție de circumstanțele fiecărui caz în parte[87].

114. **Când se constată o încălcare, autoritățile de supraveghere pot impune măsuri corective, cum ar fi obligarea operatorilor, ținând seama de circumstanțele fiecărui caz, să ia măsuri pentru a remedia ilegalitatea prelucrării inițiale.** Acestea pot fi, de exemplu, emiterea unei amenzi, impunerea unei limitări temporare a prelucrării, ștergerea unei părți a setului de date care a fost prelucrat în mod ilegal sau, dacă acest lucru nu este posibil, în funcție de faptele în cauză, având în vedere proporționalitatea măsurii, ordonând ștergerea întregului set de date utilizat pentru dezvoltarea modelului de IA și/sau a modelului de IA în sine. Când evaluează proporționalitatea măsurii avute în vedere, autoritățile de supraveghere pot lua în considerare măsurile care pot fi aplicate de operator pentru a remedia ilegalitatea prelucrării inițiale (de exemplu, recalificarea).

[83] CJUE, hotărârea din 4 mai 2023, cauza C-60/22, *Bundesrepublik Deutschland* (ECLI:EU:C:2023:373), punctele 55-57.
[84] CJUE, hotărârea din 4 mai 2023, cauza C-60/22, *Bundesrepublik Deutschland* (ECLI:EU:C:2023:373), punctul 53.
[85] CEPD, Orientările nr. 7/2020 privind conceptele de operator de date și persoană împuternicită de operator în cadrul RGPD, versiunea 2.1, adoptate la 7 iulie 2021, punctul 55.
[86] Este posibil să fie necesar să se țină seama de normele naționale specifice. Vezi, de exemplu, articolul 2-decies din Codul italian privind protecția datelor (Decretul legislativ nr. 196/2003), care stabilește că datele prelucrate cu încălcarea normelor de protecție a datelor nu pot fi utilizate. Acest lucru nu aduce atingere altor cadre legale naționale, de exemplu dreptul penal.
[87] Vezi, în acest sens, considerentul 129 din RGPD, precum și CJUE, hotărârea din 26 septembrie 2024, cauza C-768-21, T*R v Land Hessen* (ECLI:EU:C:2024:785), punctul 37; CJUE, hotărârea din 7 decembrie 2023, în cauzele conexate C-26/22 și C-64/22, SCHUFA Holding (Libération de reliquat de dette) (ECLI:EU:C:2023:958), punctul 57; și CJUE, hotărârea din 14 martie 2024, cauza C-46/23, *Újpesti Polgármesteri Hivatal* (ECLI:EU:C:2024:239), punctul 34.

115. CEPD subliniază, de asemenea, că, atunci când datele cu caracter personal sunt prelucrate în mod ilegal, persoanele vizate pot solicita ștergerea datelor lor cu caracter personal, sub rezerva condițiilor prevăzute la articolul 17 din RGPD, și că autoritățile de supraveghere pot dispune ștergerea din oficiu a datelor cu caracter personal[88].

116. Când evaluează dacă o măsură este adecvată, necesară și proporțională, autoritățile de supraveghere pot lua în considerare, printre alte elemente, riscurile pentru persoanele vizate, gravitatea încălcării, fezabilitatea tehnică și financiară a măsurii, precum și volumul de date cu caracter personal implicate.

117. În cele din urmă, CEPD reamintește că măsurile luate de autoritățile de supraveghere în temeiul RGPD nu aduc atingere măsurilor luate de autoritățile competente în temeiul Regulamentului privind inteligența artificială și/sau în temeiul altor cadre legale aplicabile (de exemplu, legislația privind răspunderea civilă).

118. În secțiunile următoare, CEPD va aborda trei scenarii acoperite de întrebarea 4 din cerere, în care diferențele constau în păstrarea sau nu în model a datelor cu caracter personal prelucrate pentru elaborarea modelului și/sau în efectuarea sau nu a prelucrării ulterioare de același operator sau de alt operator.

3.4.1 Scenariul 1. Un operator prelucrează în mod ilegal date cu caracter personal pentru a dezvolta modelul, datele cu caracter personal sunt păstrate în model și sunt prelucrate ulterior de același operator (de exemplu, în contextul implementării modelului)

119. Acest scenariu se referă la întrebarea 4 (i) din cerere, în situația în care un operator prelucrează în mod ilegal date cu caracter personal [și anume, prin nerespectarea articolului 5 alineatul (1) litera (a) din RGPD și a articolului 6 din RGPD] pentru a dezvolta un model de IA, modelul de IA păstrează informații referitoare la o persoană fizică identificată sau identificabilă și deci nu este anonim. Datele cu caracter personal sunt apoi prelucrate de același operator (de exemplu, în contextul implementării modelului). În ceea ce privește acest scenariu, CEPD prezintă următoarele considerații.

120. Competența autorității de supraveghere de a impune măsuri corective cu privire la prelucrarea inițială (așa cum se explică la punctele 113, 114 și 115 de mai sus) ar avea, în principiu, un impact asupra prelucrării ulterioare (de exemplu, dacă autoritatea de supraveghere dispune ca operatorul să șteargă datele cu caracter personal care au fost prelucrate ilegal, aceste măsuri corective nu i-ar permite acestuia să prelucreze ulterior datele cu caracter personal care au făcut obiectul măsurilor).

121. În ce privește în mod specific impactul prelucrării ilegale în faza de dezvoltare asupra prelucrării ulterioare (de exemplu, în faza de implementare), CEPD reamintește că este de competența autorităților de supraveghere să efectueze o analiză de la caz la caz, care să țină cont de circumstanțele specifice fiecărui caz.

122. **Dacă fazele de dezvoltare și implementare implică scopuri separate (constituind astfel activități de prelucrare separate) și măsura în care lipsa temeiului legal pentru activitatea de prelucrare inițială afectează legalitatea prelucrării ulterioare trebuie evaluate de la caz la caz, în funcție de contextul cazului.**

[88] În acest sens, Avizul nr. 39/2021 al CEPD cu privire la posibilitatea ca articolul 58 alineatul (2) litera (g) din RGPD să servească drept temei legal pentru ca o autoritate de supraveghere să dispună din oficiu ștergerea datelor cu caracter personal într-o situație în care o astfel de cerere nu a fost depusă de persoana vizată, punctul 28. Vezi, în acest sens, și CJUE, hotărârea din 14 martie 2024, cauza C-46/23, *Újpesti Polgármesteri Hivatal* (ECLI:EU:C:2024:239), punctul 42.

123. De exemplu, în ceea ce privește în mod specific temeiul juridic al articolului 6 alineatul (1) litera (f) din RGPD, când prelucrarea ulterioară se bazează pe un interes legitim, ilegalitatea prelucrării inițiale trebuie luată în considerare în evaluarea interesului legitim (de exemplu, în ceea ce privește riscurile pentru persoanele vizate sau faptul că persoanele vizate nu se pot aștepta la o astfel de prelucrare ulterioară). În aceste cazuri, ilegalitatea prelucrării în faza de dezvoltare poate afecta legalitatea prelucrării ulterioare.

3.4.2 Scenariul 2. Un operator prelucrează ilegal date cu caracter personal pentru a dezvolta modelul, datele cu caracter personal sunt păstrate în model și sunt prelucrate de alt operator în contextul implementării modelului.

124. Acest scenariu se referă la întrebarea 4 (i) din cerere. Diferă de scenariul 1 (în secțiunea 3.4.1 din aviz), întrucât datele cu caracter personal sunt prelucrate ulterior de alt operator în contextul implementării modelului de IA.

125. CEPD reamintește că stabilirea rolurilor atribuite acestor actori diferiți în temeiul cadrului de protecție a datelor este un pas esențial pentru a identifica obligațiile care decurg din RGPD care se aplică și cine este responsabil pentru aceste obligații și că situațiile de control comun ar trebui, de asemenea, luate în considerare când se evaluează responsabilitățile fiecărei părți în temeiul RGPD. Prin urmare, observațiile de mai jos trebuie considerate elemente generale care trebuie luate în considerare de autoritățile de supraveghere, după caz. În ceea ce privește acest scenariu 2, CEPD prezintă următoarele considerații.

126. În primul rând, trebuie reamintit că, în conformitate cu articolul 5 alineatul (1) litera (a) din RGPD, citit în lumina articolului 5 alineatul (2) din RGPD, fiecare operator trebuie să asigure legalitatea prelucrării pe care o efectuează și să o poată demonstra. Prin urmare, autoritățile de supraveghere trebuie să evalueze legalitatea prelucrării efectuate de (i) operatorul care a dezvoltat inițial modelul de IA și (ii) operatorul care a achiziționat modelul de IA și prelucrează el însuși datele cu caracter personal.

127. În al doilea rând, considerațiile de la punctele 113, 114 și 115 de mai sus sunt relevante în acest caz în ceea ce privește competența autorităților de supraveghere de a interveni în legătură cu prelucrarea inițială. Articolul 17 alineatul (1) litera (d) din RGPD (ștergerea datelor prelucrate ilegal) și articolul 19 din RGPD (obligația de notificare privind rectificarea sau ștergerea datelor cu caracter personal sau restricționarea prelucrării) pot, de asemenea, în funcție de circumstanțele cazului, să fie relevante în acest context, de exemplu în ceea ce privește notificarea pe care operatorul care dezvoltă modelul trebuie să o efectueze către operatorul care implementează modelul.

128. În al treilea rând, în ce privește posibilul impact al ilegalității prelucrării inițiale asupra celei ulterioare efectuate de alt operator, această evaluare trebuie efectuată de autoritățile de supraveghere de la caz la caz.

129. **Autoritățile de supraveghere trebuie să ia în considerare dacă operatorul care implementează modelul a efectuat o evaluare adecvată, ca parte a obligațiilor sale de responsabilitate[89] pentru a demonstra conformitatea cu articolul 5 alineatul (1) litera (a) și cu articolul 6 din RGPD, pentru a se asigura că modelul de IA nu a fost dezvoltat prin prelucrarea ilegală de date cu caracter personal.** Această evaluare de către autoritățile de supraveghere trebuie să ia în considerare dacă operatorul a evaluat unele criterii neexhaustive, de exemplu sursa datelor, și dacă modelul de IA este rezultatul unei

[89] Articolul 5 alineatul (2) și articolul 24 din RGPD.

încălcări a RGPD, în special dacă a fost stabilit de o autoritate de supraveghere sau de o instanță, astfel încât operatorul care utilizează modelul să nu poată ignora că prelucrarea inițială a fost ilegală.

130. Operatorul trebuie să ia în considerare, de exemplu, dacă datele provin dintr-o încălcare a securității datelor cu caracter personal sau dacă prelucrarea a făcut obiectul constatării unei încălcări de către o autoritate de supraveghere sau o instanță. **Gradul de evaluare a operatorului și nivelul de detaliere așteptat de autoritățile de supraveghere pot varia în funcție de diverși factori, inclusiv tipul și gradul de riscuri generate de prelucrarea din modelul de IA în timpul implementării acestuia în raport cu persoanele vizate ale căror date au fost utilizate pentru dezvoltarea modelului.**

131. CEPD observă că Regulamentul privind inteligența artificială impune furnizorilor de sisteme de inteligență artificială cu risc ridicat să întocmească o declarație UE de conformitate[90] și că o astfel de declarație conține o mențiune conform căreia sistemul de IA respectiv respectă legislația UE privind protecția datelor[91]. CEPD ia act de faptul că o asemenea declarație pe propria răspundere nu poate constitui o constatare concludentă a respectării RGPD. Autoritățile de supraveghere pot lua însă în considerare acest lucru când investighează un anumit model de IA.

132. Aceleași considerații formulate la punctul 123 de mai sus sunt relevante și în acest caz. Când autoritățile de supraveghere verifică dacă și cum a evaluat operatorul caracterul adecvat al interesului legitim ca temei legal pentru prelucrarea pe care o efectuează, ilegalitatea prelucrării inițiale trebuie luată în considerare ca parte a evaluării interesului legitim, de exemplu prin evaluarea riscurilor potențiale care pot apărea pentru persoanele vizate ale căror date cu caracter personal au fost prelucrate ilegal pentru a dezvolta modelul. Diferitele aspecte, fie de natură tehnică (de exemplu, existența unor filtre sau limitări de acces plasate în timpul dezvoltării modelului, pe care operatorul ulterior nu le poate eluda sau influența și care pot împiedica accesul la datele cu caracter personal sau divulgarea lor), fie de natură juridică (de exemplu, natura și gravitatea ilegalității prelucrării inițiale) trebuie luate în considerare în mod corespunzător în cadrul testului comparativ.

3.4.3 Scenariul 3 Un operator prelucrează ilegal date cu caracter personal pentru a dezvolta modelul, apoi se asigură că modelul este anonimizat, înainte ca același operator sau alt operator să inițieze altă prelucrare a datelor cu caracter personal în contextul implementării

133. Acest scenariu se referă la întrebarea 4 (ii) din cerere și se referă la un caz în care un operator prelucrează ilegal date cu caracter personal pentru a dezvolta modelul de IA, dar o face într-un mod care asigură anonimizarea datelor cu caracter personal, înainte ca același operator sau alt operator să inițieze altă prelucrare a datelor cu caracter personal în contextul implementării. În primul rând, CEPD reamintește că autoritățile de supraveghere sunt competente și au competența de a interveni în ceea ce privește prelucrarea legată de anonimizarea modelului, precum și prelucrarea efectuată în faza de dezvoltare. Astfel, autoritățile de supraveghere pot, în funcție de circumstanțele specifice ale cazului, să impună măsuri corective cu privire la această prelucrare inițială (după cum se explică la punctele 113, 114 și 115 de mai sus).

134. Dacă se poate demonstra că funcționarea ulterioară a modelului de IA nu implică prelucrarea datelor cu caracter personal, CEPD consideră că RGPD nu s-ar aplica[92]. Prin urmare, ilegalitatea prelucrării inițiale nu trebuie să afecteze funcționarea ulterioară a modelului. CEPD subliniază însă că simpla afirmare a anonimatului modelului nu este suficientă pentru a-l excepta de la aplicarea RGPD și

[90] Articolul 16 litera (g) și articolul 47 din Regulamentul privind inteligența artificială.
[91] Anexa V punctul 5 din Regulamentul privind inteligența artificială.
[92] Considerentul 26 din RGPD.

menționează că autoritățile de supraveghere trebuie să o evalueze ținând cont, de la caz la caz, de considerațiile furnizate de CEPD pentru a răspunde la întrebarea 1 din cerere.

135. **Când operatorii prelucrează ulterior datele cu caracter personal colectate în faza de implementare, după ce modelul a fost anonimizat, RGPD se va aplica în legătură cu aceste activități de prelucrare. În aceste cazuri, în ceea ce privește RGPD, legalitatea prelucrării efectuate în faza de implementare nu trebuie să fie afectată de ilegalitatea prelucrării inițiale.**

4 Observații finale

136. Prezentul aviz se adresează tuturor autorităților de supraveghere și va fi publicat în temeiul articolului 64 alineatul (5) litera (b) din RGPD.

Pentru Comitetul European pentru Protecția Datelor

Președinte

Anu Talus