CEPD-AEPD

Aviz comun 5/2021

privind propunerea de regulament al Parlamentului European și al Consiliului de stabilire a unor norme armonizate privind inteligența artificială (Legea privind inteligența artificială)

18 iunie 2021

Rezumat

La 21 aprilie 2021, Comisia Europeană a prezentat propunerea sa de regulament al Parlamentului European și al Consiliului de stabilire a unor norme armonizate privind inteligența artificială (denumită în continuare „propunerea”). CEPD și AEPD salută preocuparea legiuitorului privind abordarea utilizării inteligenței artificiale (IA) în cadrul Uniunii Europene (UE) și subliniază că propunerea are **implicații importante în ceea ce privește protecția datelor**.

CEPD și AEPD iau notă de faptul că **temeiul juridic** al propunerii este, în primul rând, articolul 114 din Tratatul privind funcționarea Uniunii Europene (TFUE). În plus, propunerea se întemeiază, de asemenea, pe articolul 16 din TFUE, în măsura în care conține norme specifice privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal, în special restricții privind utilizarea sistemelor de IA pentru identificarea biometrică la distanță „în timp real” în spațiile accesibile publicului în scopul aplicării legii. CEPD și AEPD reamintesc că, în conformitate cu jurisprudența Curții de Justiție a UE (CJUE), articolul 16 din TFUE oferă un temei juridic adecvat în cazurile în care protecția datelor cu caracter personal este unul dintre obiectivele sau componentele esențiale ale normelor adoptate de legiuitorul UE. Aplicarea articolului 16 din TFUE implică, de asemenea, **necesitatea de a asigura o supraveghere independentă a respectării** cerințelor privind prelucrarea datelor cu caracter personal, astfel cum se prevede și la articolul 8 din Carta drepturilor fundamentale a UE.

În ceea ce privește **domeniul de aplicare al propunerii,** CEPD și AEPD salută călduros faptul că aceasta include furnizarea și utilizarea sistemelor de IA de către instituțiile, organele sau agențiile UE. Cu toate acestea, **excluderea cooperării internaționale în materie de aplicare a legii din domeniul de aplicare** al propunerii ridică motive serioase de îngrijorare pentru CEPD și AEPD, întrucât o astfel de excludere creează un risc semnificativ de eludare (de exemplu, țări terțe sau organizații internaționale care operează aplicații cu grad ridicat de risc de care depind autoritățile publice din UE).

CEPD și AEPD **salută abordarea bazată pe riscuri** care stă la baza propunerii. Cu toate acestea, această abordare ar trebui clarificată, iar conceptul de „risc pentru drepturile fundamentale” ar trebui aliniat la RGPD și la Regulamentul (UE) 2018/1725 (RPDUE), deoarece intervin aspecte legate de protecția datelor cu caracter personal.

CEPD și AEPD sunt de acord cu propunerea conform căreia clasificarea unui **sistem de IA ca având risc ridicat nu înseamnă neapărat că este legal** *per se* și poate fi implementat de utilizator ca atare. **Este posibil ca operatorul să trebuiască să respecte și alte cerințe care decurg din legislația UE** privind protecția datelor. În plus, respectarea obligațiilor legale care decurg din legislația Uniunii (inclusiv în ceea ce privește protecția datelor cu caracter personal) ar trebui să fie o condiție prealabilă pentru intrarea pe piața europeană ca produs cu marcaj CE. În acest scop, CEPD și AEPD consideră că **cerința de a asigura conformitatea cu RGPD și RPDUE ar trebui inclusă în titlul III capitolul 2**. În plus, CEPD și AEPD consideră necesară adaptarea procedurii de evaluare a conformității din propunere, astfel încât părțile terțe să efectueze întotdeauna evaluări *ex ante* ale conformității sistemelor de IA cu grad ridicat de risc.

Având în vedere riscul ridicat de discriminare, propunerea interzice „evaluarea comportamentului social” atunci când este realizată „într-o anumită perioadă de timp” sau „de către autoritățile publice sau în numele acestora”. Cu toate acestea, întreprinderile private, cum ar fi platformele de comunicare socială și furnizorii de servicii cloud, pot, de asemenea, să prelucreze cantități mari de date cu caracter personal și să realizeze o evaluare a comportamentului social. Prin urmare, **viitorul Regulament privind IA ar trebui să interzică orice tip de evaluare a comportamentului social**.

Identificarea biometrică la distanță a indivizilor în spațiile accesibile publicului prezintă un risc ridicat de intruziune în viața privată a persoanelor, cu efecte grave asupra așteptărilor persoanelor de a fi anonime în spațiile publice. Din aceste motive, CEPD și AEPD **solicită interzicerea generală a oricărei utilizări a IA pentru recunoașterea automatizată a trăsăturilor umane în spații accesibile publicului,** cum ar fi recunoașterea facială, a mersului, amprentelor, ADN-ului, vocii, apăsării de taste și a altor semnale biometrice sau comportamentale, în orice context. Se recomandă, de asemenea, **interzicerea sistemelor de IA care utilizează date biometrice pentru a clasifica indivizii în grupuri** bazate pe etnie, sex, orientare politică sau sexuală sau pe alte criterii pentru care discriminarea este interzisă în temeiul articolului 21 din Carta drepturilor fundamentale. În plus, CEPD și AEPD consideră că utilizarea IA **pentru a deduce emoțiile unei persoane fizice este extrem de nedorită și ar trebui interzisă.**

CEPD și AEPD salută **desemnarea AEPD drept autoritate competentă și autoritate de supraveghere a pieței pentru supravegherea instituțiilor, agențiilor și organelor Uniunii**. Cu toate acestea, rolul și sarcinile AEPD ar trebui clarificate mai detaliat, în special în ceea ce privește rolul său de autoritate de supraveghere a pieței. În plus, viitorul Regulament privind IA ar trebui să stabilească în mod clar **independența autorităților de supraveghere** în îndeplinirea sarcinilor lor de supraveghere și de asigurare a respectării legii.

Desemnarea autorităților de protecție a datelor (APD) drept autorități naționale de supraveghere ar asigura o abordare mai armonizată în materie de reglementare, ar contribui la interpretarea coerentă a dispozițiilor privind prelucrarea datelor și ar evita contradicțiile între statele membre în ceea ce privește aplicarea legii. În consecință, CEPD și AEPD consideră că **autoritățile de protecție a datelor ar trebui desemnate drept autorități naționale de supraveghere în temeiul articolului 59 din propunere.**

Propunerea atribuie un rol predominant Comisiei în cadrul „Comitetului european pentru inteligența artificială" (European Artificial Intelligence Board – EAIB). Un astfel de rol intră în conflict cu nevoia de a avea un organism european pentru IA independent de orice influență politică. Pentru a-i asigura independența, viitorul Regulament privind IA **ar trebui să acorde mai multă autonomie EAIB** și să se asigure că acesta poate acționa din proprie inițiativă.

Având în vedere răspândirea sistemelor de IA în cadrul pieței unice și probabilitatea apariției unor cazuri transfrontaliere, este esențial să se asigure o aplicare armonizată a legii și o alocare adecvată a competențelor între autoritățile naționale de supraveghere. CEPD și AEPD sugerează să se aibă în vedere **un mecanism care să garanteze un punct unic de contact pentru persoanele vizate de legislație, precum și pentru întreprinderi, pentru fiecare sistem de IA.**

În ceea ce privește **spațiile de testare,** CEPD și AEPD **recomandă clarificarea domeniului de aplicare și a obiectivelor acestora**. De asemenea, propunerea ar trebui să precizeze în mod clar că temeiul juridic al unor astfel de spații de testare ar trebui să respecte cerințele stabilite în cadrul existent de protecție a datelor.

Sistemul de certificare prezentat în propunere **nu include o legătură clară cu legislația UE privind protecția datelor,** precum și cu alte legi ale UE și ale statelor membre aplicabile fiecărui „domeniu" de sistem de IA cu grad ridicat de risc și nu ia în considerare **principiile reducerii la minimum a datelor și protecției datelor începând cu momentul conceperii** ca unul dintre aspectele care trebuie luate în considerare **înainte de obținerea marcajului CE**. Prin urmare, CEPD și AEPD recomandă modificarea propunerii pentru a clarifica relația dintre certificatele eliberate în temeiul regulamentului menționat și

certificările, sigiliile și mărcile de protecție a datelor. În cele din urmă, autoritățile pentru protecția datelor ar trebui să fie implicate în elaborarea și stabilirea de standarde armonizate și specificații comune.

În ceea ce privește **codurile de conduită**, CEPD și AEPD consideră că **este necesar să se clarifice** dacă protecția datelor cu caracter personal trebuie să fie considerată printre „cerințele suplimentare" care pot fi abordate de aceste coduri de conduită și să se asigure că „specificațiile și soluțiile tehnice" nu intră în conflict cu normele și principiile cadrului existent al UE privind protecția datelor.

CUPRINS

1 INTRODUCERE 6

2 ANALIZA PRINCIPIILOR-CHEIE ALE PROPUNERII 8

2.1 Domeniul de aplicare al propunerii și relația cu cadrul juridic existent 8

2.2 Abordarea bazată pe riscuri 9

2.3 Utilizări interzise ale IA 12

2.4 Sisteme de IA cu grad ridicat de risc 14

2.4.1 Necesitatea unei evaluări *ex ante* a conformității de către terți externi 14

2.4.2 Domeniul de aplicare al regulamentului trebuie să acopere și sistemele de IA aflate deja în uz 15

2.5 Guvernanța și Comitetul european pentru inteligența artificială 15

2.5.1 Guvernanța 15

2.5.2 Comitetul european pentru inteligența artificială 17

3 INTERACȚIUNEA CU CADRUL DE PROTECȚIE A DATELOR 18

3.1 Relația dintre propunere și legislația existentă a UE privind protecția datelor 18

3.2 Spațiul de testare și prelucrarea ulterioară a datelor (articolele 53 și 54 din propunere) 19

3.3 Transparență 21

3.4 Prelucrarea categoriilor speciale de date și a datelor referitoare la infracțiuni 22

3.5 Mecanisme de asigurare a conformității 22

3.5.1 Certificare 22

3.5.2 Coduri de conduită 23

4 CONCLUZIE 25

Comitetul european pentru protecția datelor și Autoritatea Europeană pentru Protecția Datelor,

având în vedere articolul 42 alineatul (2) din Regulamentul (UE) 2018/1725 din 23 octombrie 2018 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal de către instituțiile, organele, oficiile și agențiile Uniunii și privind libera circulație a acestor date și de abrogare a Regulamentului (CE) nr. 45/2001 și a Deciziei nr. 1247/2002/CE[1],

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[2],

având în vedere solicitarea unui aviz comun al Autorității Europene pentru Protecția Datelor și al Comitetului european pentru protecția datelor din 22 aprilie 2021 privind propunerea de regulament de stabilire a unor norme armonizate privind inteligența artificială (Legea privind inteligența artificială),

ADOPTĂ PREZENTUL AVIZ COMUN

1 INTRODUCERE

1. Apariția sistemelor de inteligență artificială („IA”) reprezintă un pas foarte important în evoluția tehnologiilor și în modul în care oamenii interacționează cu acestea. IA este un set de tehnologii esențiale care ne vor schimba profund viața de zi cu zi, fie din punct de vedere societal, fie din punct de vedere economic. În următorii ani, sunt așteptate decizii categorice privind IA, deoarece aceasta ne ajută să depășim unele dintre cele mai mari provocări cu care ne confruntăm în prezent în multe domenii, de la sănătate la mobilitate sau de la administrația publică la educație.

2. Cu toate acestea, evoluțiile promise nu sunt lipsite de riscuri. În realitate, riscurile sunt foarte relevante, având în vedere că, în mare măsură, efectele individuale și societale ale sistemelor de IA nu au mai fost experimentate. Generarea de conținut, efectuarea de previziuni sau luarea unei decizii în mod automatizat, așa cum fac sistemele de IA, prin intermediul tehnicilor de învățare automată sau al regulilor logice și probabilistice de deducție, nu sunt aceleași ca în cazul desfășurării acestor activități de către oameni, prin intermediul unui raționament creativ sau teoretic și purtând întreaga responsabilitate pentru consecințe.

3. IA va mări numărul de previziuni care pot fi realizate în multe domenii, pornind de la corelații măsurabile între date, invizibile pentru ochiul uman, dar vizibile pentru mașini, făcând viața mai ușoară și rezolvând un număr mare de probleme, dar, în același timp, ne va eroda capacitatea de a oferi o interpretare cauzală a rezultatelor, astfel încât noțiunile de transparență, control uman, responsabilitate și răspundere pentru rezultate vor fi puse sub semnul întrebării.

[1] JO L 295, 21.11.2018, p. 39–98.
[2] Referirile la „statele membre” din acest document trebuie înțelese ca referiri la „statele membre ale SEE”.

4. Datele (cu sau fără caracter personal) din IA reprezintă, în multe cazuri, premisele principale ale deciziilor autonome, care vor afecta inevitabil viața persoanelor la diferite niveluri. Acesta este motivul pentru care CEPD și AEPD, încă din această etapă, declară ferm că propunerea de regulament de stabilire a unor norme armonizate privind inteligența artificială (Legea privind inteligența artificială) (denumită în continuare „propunerea”)[3] are **implicații importante în ceea ce privește protecția datelor**.

5. Atribuirea sarcinii de decizie mașinilor, pe baza datelor, va crea riscuri pentru drepturile și libertățile persoanelor fizice, va afecta viața privată a acestora și ar putea dăuna grupurilor sau chiar societăților în ansamblu. CEPD și AEPD subliniază că drepturile la viață privată și la protecția datelor cu caracter personal, aflate în conflict cu prezumția autonomiei decizionale a mașinii care stă la baza conceptului de IA, reprezintă un pilon al valorilor UE, astfel cum sunt recunoscute în Declarația Universală a Drepturilor Omului (articolul 12), în Convenția europeană a drepturilor omului (articolul 8) și în Carta drepturilor fundamentale a UE (denumită în continuare „Carta”) (articolele 7 și 8). Reconcilierea perspectivei de creștere oferite de aplicațiile de IA și a rolului central și supremației oamenilor față de mașini reprezintă un obiectiv foarte ambițios, dar necesar.

6. CEPD și AEPD salută implicarea în reglementare a tuturor părților interesate din lanțul valoric al IA și introducerea unor cerințe specifice pentru furnizorii de soluții, deoarece acestea joacă un rol semnificativ în produsele care utilizează sistemele lor. Cu toate acestea, responsabilitățile diferitelor părți – utilizatorul, furnizorul, importatorul sau distribuitorul unui sistem de IA – trebuie să fie clar delimitate și atribuite. În special, la prelucrarea datelor cu caracter personal, ar trebui să se acorde o atenție deosebită coerenței acestor roluri și responsabilități cu noțiunile de operator de date și de persoană împuternicită de operator care intră sub incidența cadrului de protecție a datelor, deoarece cele două norme nu sunt congruente.

7. Propunerea acordă un loc important noțiunii de supraveghere umană (articolul 14), pe care CEPD și AEPD o salută. Cu toate acestea, după cum s-a menționat anterior, din cauza impactului potențial puternic al anumitor sisteme de IA asupra unor persoane fizice sau grupuri de persoane, adevăratul rol central al omului ar trebui să implice supravegherea umană înalt calificată și prelucrarea legală, în măsura în care aceste sisteme se bazează pe prelucrarea datelor cu caracter personal sau prelucrează date cu caracter personal pentru a-și îndeplini sarcinile, astfel încât să se asigure respectarea dreptului de a nu face obiectul unei decizii bazate exclusiv pe prelucrarea automată.

8. În plus, având în vedere că multe aplicații de IA utilizează date în mod intensiv, propunerea ar trebui să promoveze adoptarea unei abordări de protecție a datelor începând cu momentul conceperii și în mod implicit la toate nivelurile, încurajând punerea în aplicare eficace a principiilor de protecție a datelor (astfel cum se prevede la articolul 25 din RGPD și la articolul 27 din RPDUE) prin intermediul tehnologiilor de ultimă generație.

[3] COM(2021)206 final.

9. În cele din urmă, CEPD și AEPD subliniază că acest aviz comun este furnizat doar ca o analiză preliminară a propunerii, fără a aduce atingere niciunei evaluări și opinii suplimentare privind efectele propunerii și compatibilitatea acesteia cu legislația UE privind protecția datelor.

2 ANALIZA PRINCIPIILOR-CHEIE ALE PROPUNERII

2.1 Domeniul de aplicare al propunerii și relația cu cadrul juridic existent

10. Conform expunerii de motive, **temeiul juridic** al propunerii este, în primul rând, articolul 114 din TFUE, care prevede adoptarea de măsuri pentru a asigura instituirea și funcționarea pieței interne[4]. În plus, propunerea se întemeiază, de asemenea, pe articolul 16 din TFUE, *în măsura în care conține norme specifice privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal*, în special restricții privind utilizarea sistemelor de IA pentru identificarea biometrică la distanță „în timp real" în spațiile accesibile publicului în scopul aplicării legii[5].

11. CEPD și AEPD reamintesc că, în conformitate cu jurisprudența CJUE, articolul 16 din TFUE oferă un temei juridic adecvat în cazurile în care protecția datelor cu caracter personal este unul dintre obiectivele sau componentele esențiale ale normelor adoptate de legiuitorul UE[6]. Aplicarea articolului 16 din TFUE implică, de asemenea, necesitatea de a asigura o supraveghere independentă a respectării cerințelor privind prelucrarea datelor cu caracter personal, astfel cum se prevede și la articolul 8 din Cartă.

12. AEPD și CEPD reamintesc că există deja un cadru cuprinzător privind protecția datelor adoptat în temeiul articolului 16 din TFUE, constând în Regulamentul general privind protecția datelor (RGPD)[7], Regulamentul privind protecția datelor de către instituțiile, oficiile, organele și agențiile Uniunii Europene (RPDUE)[8] și Directiva privind protecția datelor în materie de aplicare a legii (Law Enforcement Directive - LED)[9]. Conform propunerii, numai restricțiile suplimentare privind prelucrarea datelor biometrice incluse în propunere pot fi considerate ca fiind întemeiate pe articolul 16 din TFUE și, prin urmare, având același temei juridic ca RGPD,

[4] Expunere de motive, p. 5.
[5] Expunere de motive, p. 6. A se vedea, de asemenea, considerentul (2) din propunere.
[6] Avizul din 26 iulie 2017, *PNR Canada*, procedura de aviz 1/15, ECLI:EU:C:2017:592, punctul 96.
[7] Regulamentul (UE) 2016/679 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 (Regulamentul general privind protecția datelor) JO L 119, 4.5.2016, p. 1–88.
[8] Regulamentul (UE) 2018/1725 al Parlamentului European și al Consiliului din 23 octombrie 2018 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal de către instituțiile, organele, oficiile și agențiile Uniunii și privind libera circulație a acestor date și de abrogare a Regulamentului (CE) nr. 45/2001 și a Deciziei nr. 1247/2002/CE, JO L 295, 21.11.2018, p. 39–98.
[9] Directiva (UE) 2016/680 a Parlamentului European și a Consiliului din 27 aprilie 2016 privind protecția persoanelor fizice referitor la prelucrarea datelor cu caracter personal de către autoritățile competente în scopul prevenirii, depistării, investigării sau urmăririi penale a infracțiunilor sau al executării pedepselor și privind libera circulație a acestor date și de abrogare a Deciziei-cadru 2008/977/JAI a Consiliului, JO L 119, 4.5.2016, p. 89–131.

RPDUE sau LED. Acest lucru are implicații importante pentru relația dintre propunere și RGPD, RPDUE și, în general, LED, astfel cum se arată mai jos.

13. În ceea ce privește **domeniul de aplicare al propunerii**, CEPD și AEPD salută călduros faptul că propunerea se extinde la utilizarea sistemelor de IA de către instituțiile, organele sau agențiile UE. Având în vedere că utilizarea sistemelor de IA de către aceste entități poate avea, de asemenea, un impact semnificativ asupra drepturilor fundamentale ale persoanelor fizice, similar utilizării în statele membre ale UE, este indispensabil ca noul cadru de reglementare privind IA să se aplice atât statelor membre ale UE, cât și instituțiilor, oficiilor, organelor și agențiilor UE, pentru a asigura o abordare coerentă în întreaga Uniune. Întrucât instituțiile, oficiile, organele și agențiile UE pot acționa atât ca furnizori, cât și ca utilizatori ai sistemelor de IA, AEPD și CEPD consideră că este pe deplin oportun ca aceste entități să fie incluse în domeniul de aplicare al propunerii în temeiul articolului 114 din TFUE.

14. Cu toate acestea, CEPD și AEPD au motive serioase de îngrijorare cu privire la excluderea cooperării internaționale în materie de aplicare a legii din domeniul de aplicare prevăzut la articolul 2 alineatul (4) din propunere. Această excludere creează un risc semnificativ de eludare (de exemplu, țări terțe sau organizații internaționale care operează aplicații cu grad ridicat de risc de care depind autoritățile publice din UE).

15. Dezvoltarea și utilizarea sistemelor de IA va implica, în multe cazuri, prelucrarea datelor cu caracter personal. Este extrem de important să se asigure claritatea relației dintre prezenta propunere și legislația existentă a UE privind protecția datelor. Propunerea nu aduce atingere și completează RGPD, RPDUE și LED. Deși considerentele propunerii clarifică faptul că utilizarea sistemelor de IA ar trebui să respecte în continuare legislația privind protecția datelor, **CEPD și AEPD recomandă cu fermitate clarificarea, la articolul 1 din propunere, a faptului că legislația Uniunii privind protecția datelor cu caracter personal**, în special RGPD, RPDUE, Directiva privind viața privată și comunicațiile electronice[10] și LED, se aplică oricărei prelucrări a datelor cu caracter personal care intră în domeniul de aplicare al propunerii. Un considerent corespunzător ar trebui, de asemenea, să clarifice faptul că propunerea nu urmărește să aducă atingere aplicării legislației UE existente care reglementează prelucrarea datelor cu caracter personal, inclusiv sarcinile și competențele autorităților independente de supraveghere competente să monitorizeze respectarea acestor instrumente.

2.2 Abordarea bazată pe riscuri

16. CEPD și AEPD **salută abordarea bazată pe riscuri** care stă la baza propunerii. Propunerea s-ar aplica tuturor sistemelor de IA, inclusiv celor care nu implică prelucrarea datelor cu caracter personal, dar care pot avea totuși un impact asupra intereselor sau a drepturilor și libertăților fundamentale.

[10] Directiva 2002/58/CE a Parlamentului European și a Consiliului din 12 iulie 2002 privind prelucrarea datelor cu caracter personal și protecția vieții private în sectorul comunicațiilor electronice (Directiva privind viața privată și comunicațiile electronice), astfel cum a fost modificată prin Directiva 2006/24/CE și Directiva 2009/136/CE.

17. CEPD și AEPD iau act de faptul că unele dintre dispozițiile propunerii exclud riscurile pentru grupurile de persoane sau pentru societate în ansamblu (de exemplu, efectele colective cu o relevanță deosebită, cum ar fi discriminarea de grup sau exprimarea opiniilor politice în spațiile publice). CEPD și AEPD recomandă ca riscurile societale/de grup prezentate de sistemele de IA să fie de asemenea evaluate și atenuate.

18. CEPD și AEPD sunt de părere că abordarea bazată pe riscuri a propunerii ar trebui clarificată, iar conceptul de „risc pentru drepturile fundamentale" **ar trebui aliniat la RGPD**, în măsura în care intervin aspecte legate de protecția datelor cu caracter personal. Indiferent dacă sunt utilizatori finali, persoane vizate sau alte persoane vizate de sistemul de IA, absența oricărei trimiteri în text la persoana afectată de sistemul de IA apare ca o omisiune a propunerii. În realitate, obligațiile impuse actorilor față de persoanele afectate ar trebui să rezulte mai concret din protecția persoanei și a drepturilor acesteia. Astfel, CEPD și AEPD îndeamnă legiuitorii să abordeze în mod explicit în propunere **drepturile și căile de atac aflate la dispoziția persoanelor** care fac obiectul sistemelor de IA.

19. CEPD și AEPD iau notă de alegerea de a furniza o listă exhaustivă a **sistemelor de IA cu grad ridicat de risc**. Această alegere ar putea crea un efect alb-negru, cu capacități scăzute de atracție a situațiilor extrem de riscante, subminând abordarea globală bazată pe riscuri care stă la baza propunerii. De asemenea, această listă a sistemelor de IA cu grad ridicat de risc prezentată în anexele II și III la propunere nu conține anumite tipuri de cazuri de utilizare care implică riscuri semnificative, cum ar fi utilizarea IA pentru stabilirea primei de asigurare sau pentru evaluarea tratamentelor medicale sau în scopuri de cercetare în domeniul sănătății. CEPD și AEPD subliniază, de asemenea, că aceste anexe vor trebui actualizate periodic pentru a se asigura că domeniul lor de aplicare este adecvat.

20. Propunerea impune **furnizorilor** de sisteme de IA să efectueze o evaluare a riscurilor; cu toate acestea, în majoritatea cazurilor, operatorii (de date) vor fi **utilizatorii,** mai degrabă decât furnizorii de sisteme de IA (de exemplu, un utilizator al unui sistem de recunoaștere facială este un „operator" și, prin urmare, nu este obligat să respecte cerințele privind furnizorii de IA cu grad ridicat de risc în temeiul propunerii).

21. În plus, **nu va fi întotdeauna posibil ca un furnizor să evalueze toate utilizările** sistemului de IA. Astfel, evaluarea inițială a riscurilor va fi de natură mai generală decât cea efectuată de utilizatorul sistemului de IA. Chiar dacă evaluarea inițială a riscurilor efectuată de furnizor nu indică faptul că sistemul de IA este „cu grad ridicat de risc" în temeiul propunerii, acest lucru nu ar trebui să excludă **o evaluare ulterioară (mai detaliată)** [evaluarea impactului asupra protecției datelor în temeiul articolului 35 din RGPD, al articolului 39 din RPDUE sau în temeiul articolului 27 din LED], **care ar trebui să fie efectuată de utilizatorul sistemului**, având în vedere contextul de utilizare și cazurile specifice de utilizare. Interpretarea posibilității ca, în temeiul RGPD, al RPDUE și al LED, un tip de prelucrare să genereze un risc ridicat trebuie să fie efectuată independent de propunere. Cu toate acestea, clasificarea unui sistem de IA ca prezentând un „grad ridicat de risc" din cauza impactului său asupra drepturilor

fundamentale[11] **generează o prezumție de „risc ridicat" în temeiul RGPD, al RPDUE și al LED, în măsura în care datele cu caracter personal sunt prelucrate.**

22. **CEPD și AEPD sunt de acord cu propunerea conform căreia clasificarea unui sistem de IA ca având risc ridicat nu înseamnă neapărat că este legal *per se* și poate fi implementat de utilizator ca atare. Este posibil ca operatorul să trebuiască să respecte și alte cerințe care decurg din legislația UE privind protecția datelor.** În plus, raționamentul care stă la baza articolului 5 din propunere, potrivit căruia, spre deosebire de sistemele interzise, sistemele cu grad ridicat de risc pot fi permise în principiu, trebuie să fie abordat și eliminat din propunere, cu atât mai mult cu cât marcajul CE propus nu implică faptul că prelucrarea asociată a datelor cu caracter personal este legală.

23. Cu toate acestea, respectarea obligațiilor legale care decurg din legislația Uniunii (inclusiv în ceea ce privește protecția datelor cu caracter personal) ar trebui să fie o condiție prealabilă pentru a i se permite intrarea pe piața europeană ca produs cu marcaj CE. În acest scop, CEPD și AEPD **recomandă includerea în titlul III capitolul 2 din propunere a cerinței de a asigura respectarea RGPD și a RPDUE**. Aceste cerințe trebuie auditate (prin audit efectuat de o parte terță) înainte de marcajul CE, în conformitate cu principiul responsabilității. În contextul acestei evaluări efectuate de terți, evaluarea inițială a impactului care urmează să fie efectuată de furnizor va fi deosebit de relevantă.

24. Având în vedere complexitatea generată de dezvoltarea sistemelor de IA, ar trebui subliniat faptul că caracteristicile tehnice ale sistemelor de IA (de exemplu, tipul de abordare bazată pe IA) ar putea genera riscuri mai mari. Prin urmare, orice evaluare a riscurilor sistemului de IA ar trebui să ia în considerare **caracteristicile tehnice,** precum și **cazurile sale specifice de utilizare și contextul** în care funcționează sistemul.

25. Având în vedere cele de mai sus, CEPD și AEPD recomandă specificarea în propunere a faptului că **furnizorul** efectuează o evaluare inițială a riscurilor privind sistemul de IA în cauză, **luând în considerare cazurile de utilizare** [care urmează să fie specificate în propunere – completând, de exemplu, anexa III punctul 1 litera (a), în cazul în care cazurile de utilizare a sistemelor biometrice de IA nu sunt menționate] și că **utilizatorul** sistemului de IA, în calitatea sa de operator de date în temeiul legislației UE privind protecția datelor (dacă este relevant), efectuează evaluarea impactului asupra protecției datelor, astfel cum se prevede la articolul 35 din RGPD, articolul 39 din RPDUE și articolul 27 din LED, luând în considerare nu doar caracteristicile tehnice și **cazul de utilizare**, ci și **contextul specific** în care va funcționa IA.

[11] Agenția pentru Drepturi Fundamentale a Uniunii Europene (FRA) a abordat deja necesitatea de a efectua evaluări ale impactului asupra drepturilor fundamentale atunci când se utilizează IA sau tehnologii conexe. În raportul său din 2020, intitulat „Getting the future right – Artificial intelligence and fundamental rights" (Înțelegerea viitorului – Inteligența artificială și drepturile fundamentale), FRA a identificat „capcanele utilizării IA, de exemplu în ceea ce privește activitățile polițienești bazate pe analiza predictivă, diagnosticarea medicală, serviciile sociale și publicitatea direcționată" și a subliniat că „organizațiile publice și private ar trebui să efectueze evaluări ale modului în care IA ar putea aduce atingere drepturilor fundamentale" pentru a reduce impactul negativ asupra persoanelor.

26. În plus, ar trebui clarificați unii dintre termenii menționați în anexa III la propunere, de exemplu termenul „servicii esențiale private” sau micul furnizor care utilizează IA pentru evaluarea bonității pentru uz propriu.

2.3 Utilizări interzise ale IA

27. CEPD și AEPD consideră că **formele intruzive de IA** – în special cele care pot afecta demnitatea umană – trebuie considerate sisteme de IA interzise în temeiul articolului 5 din propunere, în loc să fie pur și simplu clasificate ca având „un grad de risc ridicat” în anexa III la propunere, cum ar fi cele de la punctul 6. Acest lucru este valabil în special în cazul comparațiilor de date care, pe scară largă, afectează și persoane care nu au prezentat sau au prezentat doar motive minore pentru observarea de către poliție sau prelucrarea care aduce atingere principiului limitării scopului în temeiul legislației privind protecția datelor. Utilizarea IA în domeniul poliției și al aplicării legii necesită norme specifice anumitor domenii, precise, previzibile și proporționale, care trebuie să ia în considerare interesele persoanelor în cauză și efectele asupra funcționării unei societăți democratice.

28. Articolul 5 din propunere riscă să susțină doar declarativ „valorile” și interzicerea sistemelor de IA care contrastează cu aceste valori. Într-adevăr, criteriile menționate la articolul 5 pentru a „califica” sistemele de IA ca fiind interzise **limitează domeniul de aplicare al interdicției** într-o asemenea măsură încât s-ar putea dovedi a fi lipsite de sens în practică [de exemplu, „aduce sau poate aduce prejudicii fizice sau psihologice” la articolul 5 alineatul (1) literele (a) și (b); limitarea la autoritățile publice la articolul 5 alineatul (1) litera (c); formularea vagă și punctele (i) și (ii) de la litera (c); limitarea la identificarea biometrică la distanță „în timp real” fără nicio definiție clară etc.].

29. În special, utilizarea IA pentru „evaluarea comportamentului social”, astfel cum se prevede la articolul 5 alineatul (1) litera (c) din propunere, poate duce la discriminare și contravine valorilor fundamentale ale UE. Propunerea interzice aceste practici numai atunci când sunt desfășurate „într-o anumită perioadă de timp” sau „de către autoritățile publice sau în numele acestora”. Întreprinderile private, în special platformele de comunicare socială și furnizorii de servicii de cloud, pot prelucra cantități mari de date cu caracter personal și pot realiza o evaluare a comportamentului social. Prin urmare, **propunerea ar trebui să interzică orice tip de evaluare a comportamentului social**. Trebuie remarcat faptul că, în contextul aplicării legii, articolul 4 din LED limitează deja în mod semnificativ – dacă nu interzice, în realitate – astfel de activități.

30. **Identificarea biometrică la distanță** a persoanelor fizice în spații accesibile publicului prezintă un risc ridicat de intruziune în viața privată a persoanelor. Prin urmare, CEPD și AEPD **consideră că este necesară o abordare mai strictă**. Utilizarea sistemelor de IA ar putea prezenta probleme grave de proporționalitate, deoarece ar putea implica prelucrarea datelor unui număr nediferențiat și disproporționat de persoane vizate pentru identificarea doar a câtorva persoane (de exemplu, pasagerii din aeroporturi și gări). Caracterul **neconflictual** al sistemelor de identificare biometrică la distanță prezintă, de asemenea, probleme de transparență și aspecte legate de temeiul juridic al prelucrării datelor în temeiul legislației UE (LED, RGPD, RPDUE și alte norme legale aplicabile). Problema modului în care persoanele

pot fi informate în mod corespunzător cu privire la această prelucrare a datelor este încă nerezolvată, la fel cum este și exercitarea efectivă și la timp a drepturilor persoanelor fizice. Același lucru este valabil și pentru **efectul său ireversibil și grav asupra așteptărilor** (rezonabile) **ale persoanelor de a fi anonime în spațiile publice**, ceea ce conduce la un efect negativ direct asupra exercitării libertății de exprimare, de întrunire, de asociere, precum și a libertății de circulație.

31. Articolul 5 alineatul (1) litera (d) din propunere prevede o **listă cuprinzătoare de cazuri excepționale** în care identificarea biometrică la distanță „în timp real" în spațiile accesibile publicului este permisă în scopul aplicării legii. CEPD și AEPD consideră că **această abordare este eronată** în ceea ce privește mai multe aspecte. În primul rând, nu este clar ce ar trebui înțeles ca „o întârziere semnificativă" și cum ar trebui aceasta să fie considerată un factor atenuant, luând în considerare faptul că un sistem de identificare în masă poate identifica mii de persoane în doar câteva ore. În plus, caracterul intruziv al prelucrării datelor nu depinde întotdeauna de efectuarea identificării în timp real sau nu. Identificarea biometrică la distanță ulterioară în contextul unui protest politic ar putea avea un efect semnificativ de descurajare a exercitării drepturilor și libertăților fundamentale, cum ar fi libertatea de întrunire și de asociere și, în general, principiile fundamentale ale democrației. În al doilea rând, caracterul intruziv al prelucrării datelor nu depinde în mod necesar de scopul acesteia. Utilizarea acestui sistem în alte scopuri, cum ar fi securitatea privată, prezintă aceleași amenințări la adresa drepturilor fundamentale de respectare a vieții private și de familie și de protecție a datelor cu caracter personal. În cele din urmă, chiar și cu limitările prevăzute, numărul potențial de suspecți sau de autori de infracțiuni va fi aproape întotdeauna „suficient de mare" pentru a justifica utilizarea continuă a sistemelor de IA pentru detectarea suspecților, în pofida condițiilor suplimentare prevăzute la articolul 5 alineatele (2)-(4) din propunere. Raționamentul care stă la baza propunerii pare să omită faptul că, atunci când se monitorizează zonele deschise, obligațiile care decurg din legislația UE privind protecția datelor trebuie îndeplinite nu numai pentru suspecți, ci și pentru toți cei care, în practică, sunt monitorizați.

32. Din aceste motive, CEPD și AEPD **solicită interzicerea generală a oricărei utilizări a IA pentru recunoașterea automatizată a trăsăturilor umane în spații accesibile publicului, cum ar fi recunoașterea facială, a mersului, amprentelor, ADN-ului, vocii, apăsării de taste și a altor semnale biometrice sau comportamentale, în orice context**. Abordarea actuală a propunerii este de a identifica și a enumera toate sistemele de IA care ar trebui interzise. Astfel, din motive de consecvență, **sistemele de IA pentru identificarea la distanță la scară largă în spațiile online** ar trebui interzise în temeiul articolului 5 din propunere. Ținând seama de LED, RPDUE și RGPD, AEPD și CEPD nu pot identifica modul în care acest tip de practică ar putea îndeplini cerințele privind necesitatea și proporționalitatea și care rezultă, în cele din urmă, din ceea ce CJUE și CEDO consideră că reprezintă interferențe acceptabile cu drepturile fundamentale.

33. În plus, CEPD și AEPD **recomandă interzicerea**, atât pentru autoritățile publice, cât și pentru entitățile private, a **sistemelor de IA care clasifică persoanele pe baza datelor biometrice (de exemplu, recunoașterea facială) în grupuri în funcție de etnie, sex, orientare politică sau sexuală sau alte motive de discriminare interzise în temeiul articolului 21 din Cartă**

sau a sistemelor de IA a căror validitate științifică nu este dovedită sau care sunt în conflict direct cu valorile esențiale ale UE [de exemplu, poligraful, anexa III, alineatul 6 litera (b) și alineatul 7 litera (a)]. În consecință, „**clasificarea biometrică**" ar trebui **interzisă în temeiul articolului 5**.

34. Aceasta **afectează, de asemenea, demnitatea umană, comportamentul viitor fiind stabilit sau clasificat de un calculator, independent de propria voință a persoanei**. Sistemele de IA destinate a fi utilizate de autoritățile de aplicare a legii pentru a efectua evaluări individuale ale persoanelor fizice în ceea ce privește riscul ca o persoană fizică să comită infracțiuni sau să recidiveze, a se vedea anexa III, punctul 6 litera (a) sau pentru a prevedea apariția sau repetarea unei infracțiuni reale sau potențiale pe baza creării de profiluri ale persoanelor fizice sau a evaluării trăsăturilor și caracteristicilor de personalitate sau a comportamentului infracțional din trecut, a se vedea anexa III punctul 6 litera (e) utilizate în conformitate cu scopul preconizat, vor conduce la supunerea fundamentală a procesului de luare a deciziilor polițienești și judiciare, transformând astfel ființele umane afectate în obiecte. Astfel de sisteme de IA care ating esența dreptului la demnitate umană ar trebui interzise în temeiul articolului 5.

35. În plus, CEPD și AEPD consideră că utilizarea IA pentru **a deduce emoțiile unei persoane fizice este extrem de nedorită și ar trebui interzisă,** cu excepția anumitor cazuri de utilizare bine specificate, și anume în scopuri medicale sau de cercetare (de exemplu, în cazul pacienților la care recunoașterea emoției este importantă), întotdeauna cu garanții adecvate și bineînțeles, sub rezerva tuturor celorlalte condiții și limite de protecție a datelor, inclusiv limitarea scopului.

2.4 Sisteme de IA cu grad ridicat de risc

2.4.1 Necesitatea unei evaluări *ex ante* a conformității de către terți externi

36. CEPD și AEPD salută faptul că sistemele de IA care prezintă un risc ridicat trebuie să facă obiectul unei evaluări prealabile a conformității înainte de a putea fi introduse pe piață sau puse în funcțiune în alt mod în UE. În principiu, acest model de reglementare este binevenit, deoarece oferă un bun echilibru între caracterul favorabil inovării și un nivel ridicat de protecție proactivă a drepturilor fundamentale. Pentru a fi utilizate în medii specifice, cum ar fi procesele decizionale ale instituțiilor de servicii publice sau infrastructura critică, trebuie stabilite modalități de investigare a codului sursă complet.

37. Cu toate acestea, CEPD și AEPD pledează pentru adaptarea procedurii de evaluare a conformității în temeiul articolului 43 din propunere, astfel încât evaluarea ***ex ante* a conformității de către o parte terță să fie efectuată, în general, pentru IA cu grad ridicat de risc**. Deși o evaluare a conformității de către o parte terță pentru prelucrarea cu grad ridicat de risc a datelor cu caracter personal nu este o cerință a RGPD sau a RPDUE, riscurile prezentate de sistemele de IA nu sunt încă pe deplin înțelese. Prin urmare, includerea generală a unei obligații de evaluare a conformității de către terți ar consolida și mai mult securitatea juridică și încrederea în toate sistemele de IA cu grad ridicat de risc.

2.4.2 Domeniul de aplicare al regulamentului trebuie să acopere și sistemele de IA aflate deja în uz

38. În conformitate cu articolul 43 alineatul (4) din propunere, sistemele de IA cu grad ridicat de risc ar trebui să facă obiectul unei noi proceduri de evaluare a conformității ori de câte ori are loc o modificare semnificativă. Este corect să se asigure că sistemele de IA respectă cerințele Regulamentului privind IA pe tot parcursul ciclului lor de viață. Sistemele de IA care au fost introduse pe piață sau puse în funcțiune înainte de aplicarea regulamentului propus (sau la 12 luni după aceea pentru sistemele informatice la scară largă enumerate în anexa IX) sunt excluse din domeniul de aplicare, cu excepția cazului în care sistemele respective fac obiectul unor „modificări semnificative” în ceea ce privește proiectul sau scopul preconizat (articolul 83).

39. Cu toate acestea, pragul pentru „modificări semnificative” este neclar. Considerentul (66) din propunere specifică un prag mai scăzut pentru reevaluarea conformității „ori de câte ori apare o modificare care ar putea afecta conformitatea”. Un prag similar ar fi adecvat pentru articolul 83, cel puțin pentru sistemele de IA cu grad ridicat de risc. În plus, pentru a elimina orice lacune în materie de protecție, este necesar ca sistemele de IA deja instituite și aflate în funcțiune – după o anumită etapă de punere în aplicare – să respecte, de asemenea, toate cerințele Regulamentului privind IA.

40. Multiplele posibilități de prelucrare a datelor cu caracter personal și riscurile externe afectează, de asemenea, securitatea sistemelor de IA. Accentul pus de articolul 83 pe „modificările semnificative în ceea ce privește proiectul sau scopul preconizat” nu include o trimitere la modificările riscurilor externe. Prin urmare, la articolul 83 din propunere ar trebui inclusă o trimitere la modificările scenariului de amenințări, care decurg din riscuri externe, de exemplu atacuri cibernetice, atacuri contradictorii și reclamații justificate din partea consumatorilor.

41. În plus, întrucât aplicarea este prevăzută la o perioadă de 24 de luni de la intrarea în vigoare a viitorului regulament, AEPD și CEPD nu consideră oportun să excepteze sistemele de IA deja introduse pe piață pentru o perioadă de timp și mai lungă. Deși propunerea prevede, de asemenea, că cerințele regulamentului sunt luate în considerare la evaluarea fiecărui sistem informatic la scară largă, astfel cum se prevede în actele juridice enumerate în anexa IX, CEPD și AEPD consideră că cerințele privind punerea în funcțiune a sistemelor de IA ar trebui să fie aplicabile de la data aplicării viitorului regulament.

2.5 Guvernanța și Comitetul european pentru inteligența artificială

2.5.1 Guvernanța

42. CEPD și AEPD salută desemnarea AEPD ca autoritate competentă și autoritate de supraveghere a pieței pentru supravegherea instituțiilor, agențiilor și organelor Uniunii atunci când acestea intră în domeniul de aplicare al prezentei propuneri. AEPD este pregătită să își îndeplinească noul rol de autoritate de reglementare în domeniul IA pentru administrația publică a UE. În plus, rolul și sarcinile AEPD nu sunt suficient de detaliate și ar trebui clarificate în continuare în propunere, în special în ceea ce privește rolul său de autoritate de supraveghere a pieței.

43. CEPD și AEPD recunosc alocarea resurselor financiare, care este prevăzută în propunere pentru comitet și AEPD, în calitate de organism de notificare. Cu toate acestea, îndeplinirea noilor atribuții prevăzute pentru AEPD, indiferent dacă aceasta acționează în calitate de organism notificat, ar necesita resurse financiare și umane semnificativ mai mari.

44. În primul rând, deoarece formularea de la articolul 63 alineatul (6) prevede că AEPD „acționează ca autoritate de supraveghere a pieței" pentru instituțiile, agențiile și organele Uniunii care intră în domeniul de aplicare al propunerii, ceea ce nu clarifică dacă AEPD trebuie considerată pe deplin „autoritate de supraveghere a pieței", astfel cum se prevede în Regulamentul (UE) 2019/1020. Acest lucru ridică semne de întrebare cu privire la sarcinile și competențele AEPD în practică. În al doilea rând, și cu condiția ca la prima întrebare să se răspundă afirmativ, nu este clar modul în care rolul AEPD, astfel cum este prevăzut în RPDUE, poate acoperi sarcina prevăzută la articolul 11 din Regulamentul (UE) 2019/1020, care include „supravegherea eficientă a pieței pe teritoriul lor a produselor puse la dispoziție online" sau „controale fizice și de laborator bazate pe eșantioane adecvate". Există riscul ca preluarea noului set de sarcini fără clarificări suplimentare în propunere să pună în pericol îndeplinirea obligațiilor sale de autoritate de supraveghere a protecției datelor.

45. Cu toate acestea, CEPD și AEPD subliniază că unele dispoziții ale propunerii care definesc sarcinile și competențele diferitelor autorități competente în temeiul Regulamentului privind IA, relațiile dintre acestea, natura lor și garanția independenței lor par neclare în această etapă. În timp ce Regulamentul 2019/1020 prevede că autoritatea de supraveghere a pieței trebuie să fie independentă, proiectul de regulament nu impune ca autoritățile de supraveghere să fie independente și chiar le impune să raporteze Comisiei cu privire la anumite sarcini îndeplinite de autoritățile de supraveghere a pieței, care pot fi instituții diferite. Întrucât propunerea prevede, de asemenea, că autoritățile pentru protecția datelor vor fi autoritățile de supraveghere a pieței pentru sistemele de IA utilizate în scopul aplicării legii [articolul 63 alineatul (5)], aceasta înseamnă, de asemenea, că acestea vor fi, eventual prin intermediul autorității lor naționale de supraveghere, supuse obligațiilor de raportare către Comisie [articolul 63 alineatul (2)], ceea ce pare incompatibil cu independența lor.

46. Prin urmare, CEPD și AEPD consideră că aceste dispoziții trebuie clarificate pentru a fi în concordanță cu Regulamentul 2019/1020, RPDUE și RGPD, iar propunerea ar trebui să stabilească în mod clar faptul că autoritățile de supraveghere în temeiul Regulamentului privind IA trebuie să fie complet independente în îndeplinirea sarcinilor lor, deoarece aceasta ar fi o garanție esențială pentru supraveghere și aplicarea corespunzătoare a viitorului regulament.

47. CEPD și AEPD reamintesc că autoritățile de protecție a datelor (APD) aplică deja RGPD și LED la sistemele de IA care implică date cu caracter personal pentru a garanta protecția drepturilor fundamentale și, mai precis, dreptul la protecția datelor. Prin urmare, autoritățile pentru protecția datelor dețin deja, într-o anumită măsură, astfel cum se prevede în propunere pentru autoritățile naționale de supraveghere, o înțelegere a tehnologiilor de IA, a datelor și a calculului datelor, a drepturilor fundamentale, precum și o expertiză în evaluarea riscurilor pentru drepturile fundamentale pe care le prezintă noile tehnologii. În plus, atunci când sistemele de IA se bazează pe prelucrarea datelor cu caracter personal sau prelucrează date cu caracter personal, dispozițiile propunerii sunt direct interconectate cu cadrul juridic privind

protecția datelor, ceea ce va fi cazul pentru majoritatea sistemelor de IA care intră în domeniul de aplicare al regulamentului. Prin urmare, vor exista interconexiuni între competențele autorităților de supraveghere în temeiul propunerii și cele ale autorităților pentru protecția datelor.

48. În consecință, desemnarea APD-urilor drept autorități naționale de supraveghere ar asigura o abordare mai armonizată în materie de reglementare, ar contribui la interpretarea coerentă a dispozițiilor privind prelucrarea datelor și ar evita contradicțiile între statele membre în ceea ce privește aplicarea legii. De asemenea, ar fi în beneficiul tuturor părților interesate din lanțul valoric al IA să aibă un punct de contact unic pentru toate operațiunile de prelucrare a datelor cu caracter personal care intră în domeniul de aplicare al propunerii și să limiteze interacțiunile dintre două organisme de reglementare diferite pentru prelucrarea datelor care sunt vizate de propunere și de RGPD. În consecință, CEPD și AEPD consideră că **APD-urile ar trebui desemnate autorități naționale de supraveghere în temeiul articolului 59 din propunere**.

49. În orice caz, în măsura în care propunerea conține norme specifice privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal adoptate în temeiul articolului 16 din TFUE, respectarea acestor norme, în special a restricțiilor privind utilizarea sistemelor de IA pentru identificarea biometrică la distanță „în timp real” în spațiile accesibile publicului în scopul aplicării legii, **trebuie să fie supusă controlului unor autorități independente**.

50. Cu toate acestea, propunerea nu conține nicio dispoziție explicită care să atribuie competența de a asigura respectarea acestor norme controlului autorităților independente. Singura trimitere la autoritățile competente de supraveghere a protecției datelor în temeiul RGPD sau al LED este prevăzută la articolul 63 alineatul (5) din propunere, dar numai ca organisme de „supraveghere a pieței” și alternativ cu alte autorități. CEPD și AEPD consideră că acest sistem nu asigură respectarea cerinței de control independent prevăzut la articolul 16 alineatul (2) din TFUE și la articolul 8 din Cartă.

2.5.2 Comitetul european pentru inteligența artificială

51. Propunerea instituie un „Comitet european pentru inteligența artificială” (European Artificial Intelligence Board – EAIB). CEPD și AEPD recunosc necesitatea unei aplicări consecvente și armonizate a cadrului propus, precum și a implicării experților independenți în dezvoltarea politicii UE privind IA. În același timp, propunerea prevede acordarea unui rol predominant Comisiei. Într-adevăr, nu numai că aceasta din urmă ar face parte din EAIB, ci ar prezida și ar avea drept de veto pentru adoptarea Regulamentului de procedură al EAIB. Acest lucru contrastează cu necesitatea unui organism european privind IA independent de orice influență politică. Prin urmare, CEPD și AEPD consideră că viitorul regulament privind IA ar trebui să acorde **mai multă autonomie EAIB**, pentru a-i permite să asigure cu adevărat aplicarea coerentă a regulamentului în întreaga piață unică.

52. CEPD și AEPD iau act, de asemenea, de faptul că nu este conferită EAIB nicio competență în ceea ce privește punerea în aplicare a regulamentului propus. Totuși, având în vedere răspândirea sistemelor de IA în cadrul pieței unice și probabilitatea apariției unor cazuri transfrontaliere, este esențial să se asigure o aplicare armonizată a legii și o alocare adecvată a competențelor între autoritățile naționale de supraveghere. Prin urmare, CEPD și AEPD recomandă ca mecanismele de cooperare dintre autoritățile naționale de supraveghere să fie specificate în viitorul regulament privind IA. CEPD și AEPD sugerează să se impună un mecanism care să garanteze un punct unic de contact pentru persoanele vizate de legislație, precum și pentru întreprinderi, pentru fiecare sistem de IA, iar pentru organizațiile a căror activitate acoperă mai mult de jumătate din statele membre ale UE, EAIB să poată desemna autoritatea națională care va fi responsabilă cu punerea în aplicare a Regulamentului privind IA pentru sistemul de IA respectiv.

53. În plus, având în vedere natura independentă a autorităților care alcătuiesc comitetul, acesta din urmă trebuie să aibă dreptul de a acționa din proprie inițiativă și nu numai de a oferi consiliere și asistență Comisiei. Prin urmare, CEPD și AEPD subliniază necesitatea unei extinderi a misiunii atribuite comitetului, care, în plus, nu corespunde sarcinilor enumerate în propunere.

54. Pentru a îndeplini aceste obiective, **EAIB trebuie să dispună de competențe suficiente și adecvate**, iar statutul său juridic ar trebui clarificat. În special, pentru ca domeniul de aplicare material al viitorului regulament să rămână relevant, pare necesar ca autoritățile responsabile cu aplicarea acestuia să fie implicate în evoluția sa. Prin urmare, CEPD și AEPD recomandă ca EAIB să fie împuternicit să propună Comisiei modificări ale anexei I care definește tehnicile și abordările IA și ale anexei III care enumeră sistemele de IA cu grad ridicat de risc menționate la articolul 6 alineatul (2). De asemenea, EAIB ar trebui să fie consultat de către Comisie înainte de orice modificare a anexelor respective.

55. Articolul 57 alineatul (4) din propunere prevede schimburi între comitet și alte organe, oficii, agenții și grupuri consultative ale Uniunii. Ținând seama de activitatea sa anterioară în domeniul IA și de expertiza sa în domeniul drepturilor omului, CEPD și AEPD recomandă ca Agenția pentru Drepturi Fundamentale să fie considerată unul dintre observatorii Comitetului.

3 INTERACȚIUNEA CU CADRUL DE PROTECȚIE A DATELOR

3.1 Relația dintre propunere și legislația existentă a UE privind protecția datelor

56. O relație clar definită între propunere și legislația existentă privind protecția datelor este o condiție prealabilă esențială pentru a asigura și a susține respectarea și aplicarea acquis-ului UE în domeniul protecției datelor cu caracter personal. O astfel de legislație a UE, în special RGPD, RPDUE și LED, trebuie considerată o condiție prealabilă pe care se pot baza alte propuneri legislative, fără a afecta sau a interfera cu dispozițiile existente, inclusiv în ceea ce privește competența autorităților de supraveghere și guvernanța.

57. Prin urmare, în opinia CEPD și a AEPD, este important să se evite în mod clar în propunere orice neconcordanță și orice posibil conflict cu RGPD, RPDUE și LED. Acest lucru nu este necesar numai din motive de securitate juridică, ci și pentru a evita ca propunerea să aibă ca efect periclitarea directă sau indirectă a dreptului fundamental la protecția datelor cu caracter personal, astfel cum este prevăzut la articolul 16 din TFUE și la articolul 8 din Cartă.

58. În special, mașinile cu învățare autonomă ar putea proteja datele cu caracter personal ale persoanelor numai dacă acest lucru este integrat de la început. Posibilitatea imediată de exercitare a drepturilor persoanelor fizice în temeiul articolului 22 (Procesul decizional individual automatizat, inclusiv crearea de profiluri) din RGPD sau al articolului 23 din RPDUE, indiferent de scopurile prelucrării, este, de asemenea, esențială. În acest sens, alte drepturi ale persoanelor vizate legate de dreptul de ștergere, dreptul de rectificare în conformitate cu legislația privind protecția datelor, trebuie să fie prevăzute în sistemele de IA încă de la început, indiferent de abordarea de IA aleasă sau de arhitectura tehnică.

59. Utilizarea datelor cu caracter personal pentru învățarea sistemelor de IA poate conduce la generarea unor modele decizionale părtinitoare la baza sistemului de IA. Astfel, ar trebui să fie necesare diverse garanții și, în special, o supraveghere umană calificată în cadrul unor astfel de procese, pentru a se asigura că drepturile persoanelor vizate sunt respectate și garantate, precum și pentru a se evita orice efecte negative asupra persoanelor fizice. Autoritățile competente ar trebui, de asemenea, să poată propune orientări pentru a evalua prejudecățile din sistemele de IA și pentru a sprijini exercitarea supravegherii umane.

60. Persoanele vizate ar trebui să fie întotdeauna informate atunci când datele lor sunt utilizate pentru învățare și/sau predicție în domeniul IA, cu privire la temeiul juridic al unei astfel de prelucrări, și cu explicarea generală a logicii (procedurii) și a domeniului de aplicare al sistemului de IA. În această privință, dreptul persoanelor fizice la restricționarea prelucrării (articolul 18 din RGPD și articolul 20 din RPDUE), precum și la ștergerea datelor (articolul 16 din RGPD și articolul 19 din RPDUE) ar trebui să fie întotdeauna garantat în aceste cazuri. În plus, operatorul ar trebui să aibă obligația explicită de a informa persoana vizată cu privire la perioadele aplicabile pentru obiecții, restricții, ștergerea datelor etc. Sistemul de IA trebuie să fie în măsură să îndeplinească toate cerințele de protecție a datelor prin măsuri tehnice și organizatorice adecvate. Dreptul la explicații ar trebui să prevadă o transparență suplimentară.

3.2 Spațiul de testare și prelucrarea ulterioară a datelor (articolele 53 și 54 din propunere)

61. În limitele juridice și morale existente, este important să se promoveze inovarea europeană prin intermediul unor instrumente precum un spațiu de testare. Un spațiu de testare oferă posibilitatea de a oferi garanțiile necesare pentru a consolida încrederea în și dependența față de sistemele de IA. În medii complexe, practicienii din domeniul IA pot întâmpina dificultăți în evaluarea comparativă a tuturor intereselor în mod corespunzător. În special pentru întreprinderile mici și mijlocii cu resurse limitate, funcționarea într-un spațiu de testare în materie de reglementare poate oferi informații mai rapide și, prin urmare, poate stimula inovarea.

62. Articolul 53 alineatul (3) din propunere prevede că spațiul de testare nu afectează competențele de supraveghere și corective. În cazul în care această clarificare este utilă, este necesar, de asemenea, să se elaboreze îndrumări sau orientări cu privire la modul în care se poate obține un bun echilibru între calitatea de autoritate de supraveghere, pe de o parte, și furnizarea de orientări detaliate prin intermediul unui spațiu de testare, pe de altă parte.

63. Articolul 53 alineatul (6) descrie faptul că modalitățile și condițiile de funcționare a spațiilor de testare sunt stabilite prin acte de punere în aplicare. Este important să se elaboreze orientări specifice pentru a asigura coerența și sprijinul în crearea și funcționarea spațiilor de testare. Cu toate acestea, actele de punere în aplicare obligatorii ar putea limita capacitatea fiecărui stat membru de a personaliza spațiul de testare în funcție de nevoile și practicile locale. Astfel, CEPD și AEPD recomandă ca EAIB să furnizeze orientări pentru spațiile de testare.

64. Articolul 54 din propunere urmărește să ofere un temei juridic pentru prelucrarea ulterioară a datelor cu caracter personal în vederea dezvoltării anumitor sisteme de IA în interes public în spațiul de testare în materie de reglementare în domeniul IA. Relația dintre articolul 54 alineatul (1) din propunere și articolul 54 alineatul (2) și considerentul (41) din propunere și, prin urmare, legislația existentă a UE privind protecția datelor rămâne neclară. Cu toate acestea, RGPD și RPDUE au deja o bază stabilită pentru „prelucrarea ulterioară”. În special în ceea ce privește cazurile în care este în interesul public să se permită prelucrarea ulterioară; echilibrul dintre interesele operatorului și interesele persoanei vizate nu trebuie să împiedice inovația. Articolul 54 din propunere nu abordează în prezent două aspecte importante: (i) în ce circumstanțe, pe baza căror criterii (suplimentare) sunt evaluate interesele persoanelor vizate și (ii) dacă aceste sisteme de IA vor fi utilizate doar în spațiul de testare. CEPD și AEPD salută cerința unei legislații a Uniunii sau a statelor membre în ceea ce privește prelucrarea datelor cu caracter personal colectate în temeiul LED într-un spațiu de testare, dar recomandă să se precizeze în continuare ceea ce este prevăzut aici, într-un mod care să se alinieze la RGPD și la RPDUE, în principal prin clarificarea faptului că temeiul juridic al unor astfel de spații de testare ar trebui să fie în conformitate cu cerințele stabilite la articolul 23 alineatul (2) din RGPD și la articolul 25 din RPDUE și să precizeze că fiecare utilizare a spațiului de testare trebuie să facă obiectul unei evaluări aprofundate. Acest lucru se aplică, de asemenea, listei complete de condiții de la articolul 54 alineatul (1) literele (b)-(j).

65. Unele considerații suplimentare cu privire la reutilizarea datelor de la articolul 54 din propunere indică faptul că exploatarea unui spațiu de testare implică utilizarea intensivă a resurselor și că, prin urmare, este realist să se estimeze că doar un număr mic de întreprinderi ar avea șansa de a participa. Participarea la spațiul de testare ar putea constitui un avantaj competitiv. Permiterea reutilizării datelor ar necesita o analiză atentă a modului de selectare a participanților pentru a se asigura că aceștia se încadrează în domeniul de aplicare și pentru a evita tratamentul inechitabil. CEPD și AEPD sunt preocupate de faptul că permiterea reutilizării datelor în cadrul spațiului de testare diferă de abordarea bazată pe responsabilitate din RGPD, în care responsabilitatea revine operatorului de date, nu autorității competente.

66. În plus, CEPD și AEPD consideră că, având în vedere obiectivele spațiului de testare, care sunt dezvoltarea, testarea și validarea sistemelor de IA, spațiile de testare nu pot intra în domeniul de aplicare al LED. Deși LED prevede reutilizarea datelor pentru cercetarea științifică, datele prelucrate în acest scop secundar vor face obiectul RGPD sau al RPDUE și nu vor mai face obiectul LED.

67. Nu este clar ce va cuprinde un spațiu de testare în materie de reglementare. Se pune întrebarea dacă spațiul de testare în materie de reglementare propus include o infrastructură informatică în fiecare stat membru, cu anumite temeiuri juridice suplimentare pentru prelucrarea ulterioară a datelor, sau dacă acesta nu face decât să organizeze accesul la expertiză și orientări în materie de reglementare. CEPD și AEPD îndeamnă legiuitorul să clarifice acest concept în propunere și să precizeze în mod clar în propunere că spațiul de testare în materie de reglementare nu implică o obligație a autorităților competente de a furniza infrastructura tehnică. În orice caz, autoritățile competente trebuie să furnizeze resursele financiare și umane în conformitate cu această clarificare.

68. În cele din urmă, CEPD și AEPD subliniază dezvoltarea sistemelor de IA transfrontaliere care vor fi disponibile pentru piața unică digitală europeană în ansamblu. În cazul unor astfel de sisteme de IA, spațiul de testare în materie de reglementare ca instrument de inovare nu ar trebui să devină un obstacol pentru dezvoltarea transfrontalieră. Prin urmare, CEPD și AEPD recomandă o abordare transfrontalieră coordonată, care este încă suficient disponibilă la nivel național pentru toate IMM-urile, oferind un cadru comun în întreaga Europă, fără a fi prea restrictiv. Trebuie găsit un echilibru între coordonarea europeană și procedurile naționale pentru a evita punerea în aplicare contradictorie a viitorului regulament privind IA, care ar împiedica inovarea la nivelul UE.

3.3 Transparență

69. CEPD și AEPD salută înregistrarea sistemelor de IA cu grad ridicat de risc într-o bază de date publică (menționată la articolele 51 și 60 din propunere). Această bază de date ar trebui să fie considerată o oportunitate de a oferi publicului larg informații cu privire la domeniul de aplicare al sistemului de IA și la deficiențele și incidentele cunoscute care ar putea compromite funcționarea acestora și măsurile corective adoptate de furnizori pentru a le aborda și remedia.

70. Un principiu democratic esențial este utilizarea mecanismelor de control și echilibru. Prin urmare, faptul că obligația de transparență nu se aplică sistemelor de IA utilizate pentru detectarea, prevenirea, investigarea sau urmărirea penală a infracțiunilor este o excepție prea largă. Trebuie făcută o distincție între sistemele de IA care sunt utilizate pentru detectare sau prevenire și sistemele de IA care au scopul de investigare pentru a contribui la urmărirea penală a infracțiunilor. Garanțiile pentru prevenire și detectare trebuie să fie mai puternice datorită prezumției de nevinovăție. În plus, CEPD și AEPD regretă absența avertismentelor din propunere, care poate fi interpretată ca o undă verde pentru utilizarea chiar și a unor sisteme sau aplicații de IA nedovedite și cu grad ridicat de risc.

71. În cazurile în care publicului i se poate acorda o transparență redusă sau inexistentă din motive de confidențialitate, chiar și într-o democrație care funcționează bine, ar trebui instituite garanții, iar sistemele de IA respective ar trebui să fie înregistrate la autoritatea de supraveghere competentă și să asigure transparența față de aceasta.

72. Asigurarea transparenței în sistemele de IA este un obiectiv foarte dificil. Abordarea complet cantitativă a procesului de luare a deciziilor din multe sisteme de IA, inerent diferită de abordarea umană bazată în principal pe raționament cauzal și teoretic, poate intra în conflict cu necesitatea de a obține o explicație prealabilă și inteligibilă a rezultatelor mașinii. Regulamentul ar trebui să promoveze modalități noi, mai proactive și mai prompte de a informa utilizatorii sistemelor de IA cu privire la statutul (decizional) al sistemului din orice moment, oferind o avertizare timpurie cu privire la potențialele rezultate dăunătoare, astfel încât persoanele ale căror drepturi și libertăți pot fi afectate de deciziile autonome ale mașinii să poată reacționa sau să poată contesta decizia.

3.4 Prelucrarea categoriilor speciale de date și a datelor referitoare la infracțiuni

73. Prelucrarea categoriilor speciale de date din domeniul aplicării legii este reglementată de dispozițiile cadrului UE privind protecția datelor, inclusiv de LED, precum și de punerea sa în aplicare la nivel național. Propunerea susține că nu oferă un temei juridic general pentru prelucrarea datelor cu caracter personal, inclusiv a categoriilor speciale de date cu caracter personal, a se vedea considerentul (41). În același timp, articolul 10 alineatul (5) din propunere prevede că „furnizorii de astfel de sisteme pot prelucra categoriile speciale de date cu caracter personal”. În plus, aceeași dispoziție necesită garanții suplimentare, oferind, de asemenea, exemple. Prin urmare, propunerea pare să interfereze cu aplicarea RGPD, a LED și a RPDUE. Deși CEPD și AEPD salută încercarea de a asigura garanții adecvate, este necesară o abordare mai coerentă în materie de reglementare, deoarece dispozițiile actuale nu par suficient de clare pentru a crea un temei juridic pentru prelucrarea categoriilor speciale de date și trebuie completate cu măsuri de protecție suplimentare care urmează să fie evaluate. În plus, dacă datele cu caracter personal au fost colectate prin prelucrare în cadrul domeniului de aplicare al LED, vor trebui luate în considerare posibilele garanții și limitări suplimentare care decurg din transpunerile naționale ale LED.

3.5 Mecanisme de asigurare a conformității

3.5.1 Certificare

74. Unul dintre pilonii principali ai propunerii este certificarea. Sistemul de certificare descris în propunere se bazează pe o structură de entități (autorități de notificare/organisme notificate/Comisie) și pe un mecanism de evaluare a conformității/certificare care acoperă cerințele obligatorii aplicabile sistemelor de IA cu grad ridicat de risc și are la bază standardele europene armonizate în temeiul Regulamentului (UE) nr. 1025/2012 și specificațiile comune care urmează să fie stabilite de Comisie. Acest mecanism este diferit de sistemul de certificare menit să asigure conformitatea cu normele și principiile de protecție a datelor, prezentate la articolele 42 și 43 din RGPD. Cu toate acestea, nu este clar modul în care certificatele eliberate de organismele notificate în conformitate cu propunerea pot interacționa cu certificările,

sigiliile și mărcile de protecție a datelor prevăzute de RGPD, spre deosebire de ceea ce se prevede pentru alte tipuri de certificări [a se vedea articolul 42 alineatul (2) în ceea ce privește certificările eliberate în temeiul Regulamentului (UE) 2019/881].

75. În măsura în care sistemele de IA cu grad ridicat de risc se bazează pe prelucrarea datelor cu caracter personal sau prelucrează date cu caracter personal pentru a-și îndeplini sarcinile, aceste neconcordanțe pot genera incertitudini juridice pentru toate organismele vizate, deoarece pot conduce la situații în care sistemele de IA, certificate în temeiul propunerii și marcate cu marcajul CE de conformitate, odată introduse pe piață sau puse în funcțiune, ar putea fi utilizate într-un mod care nu este conform cu normele și principiile protecției datelor.

76. Propunerea nu are o legătură clară cu legislația privind protecția datelor și nici cu alte legi ale UE și ale statelor membre aplicabile fiecărui „domeniu" al sistemului de IA cu grad ridicat de risc specificat în anexa III. În special, propunerea ar trebui să includă principiile reducerii la minimum a datelor și protecției datelor începând cu momentul conceperii ca unul dintre aspectele care trebuie luate în considerare înainte de obținerea marcajului CE, având în vedere posibilul nivel ridicat de interferență a sistemelor de IA cu grad ridicat de risc cu drepturile fundamentale la viață privată și la protecția datelor cu caracter personal, precum și necesitatea de a asigura un nivel ridicat de încredere în sistemul de IA. Prin urmare, CEPD și AEPD recomandă modificarea propunerii pentru a clarifica relația dintre certificatele eliberate în temeiul regulamentului menționat și certificările, sigiliile și mărcile de protecție a datelor. În cele din urmă, autoritățile de protecție a datelor ar trebui să fie implicate în elaborarea și stabilirea unor standarde armonizate și a unor specificații comune.

77. În legătură cu articolul 43 din propunere, referitor la evaluarea conformității, derogarea de la procedura de evaluare a conformității prevăzută la articolul 47 pare să fie foarte largă, incluzând prea multe excepții, cum ar fi motive de siguranță publică sau de protecție a vieții și sănătății persoanelor, protecția mediului și protecția bunurilor industriale și de infrastructură esențiale. Propunem legiuitorilor să le restrângă.

3.5.2 Coduri de conduită

78. În conformitate cu articolul 69 din propunere, Comisia și statele membre încurajează și facilitează elaborarea de coduri de conduită menite să promoveze aplicarea voluntară de către furnizorii de sisteme de IA care nu prezintă un risc ridicat a cerințelor aplicabile sistemelor de IA cu grad ridicat de risc, precum și a cerințelor suplimentare. În conformitate cu considerentul (78) din RGPD, CEPD și AEPD recomandă identificarea și definirea sinergiilor dintre aceste instrumente și codurile de conduită prevăzute de RGPD care sprijină respectarea protecției datelor. În acest context, este relevant să se clarifice dacă protecția datelor cu caracter personal trebuie să fie luată în considerare printre „cerințele suplimentare" care pot fi abordate de codurile de conduită menționate la articolul 69 alineatul (2). De asemenea, este relevant să se asigure că „specificațiile și soluțiile tehnice" abordate de codurile de conduită menționate la articolul 69 alineatul (1), astfel cum sunt concepute să promoveze respectarea cerințelor din proiectul de regulament privind IA, nu intră în conflict cu normele și principiile RGPD și ale RPDUE. Astfel, aderarea la aceste instrumente de către furnizorii de sisteme de IA care nu

prezintă un grad ridicat de risc – în măsura în care aceste sisteme se bazează pe prelucrarea datelor cu caracter personal sau prelucrează date cu caracter personal pentru a-și îndeplini sarcinile – ar reprezenta o valoare adăugată, deoarece acest lucru va asigura faptul că operatorul și persoanele împuternicite de operatori vor fi în măsură să își îndeplinească obligațiile în materie de protecție a datelor în utilizarea sistemelor respective.

79. În același timp, cadrul juridic pentru o IA fiabilă ar urma să fie completat de integrarea codurilor de conduită, astfel încât să se stimuleze încrederea în utilizarea acestei tehnologii într-un mod sigur și în conformitate cu legea, inclusiv cu respectarea drepturilor fundamentale. Cu toate acestea, proiectarea acestor instrumente ar trebui consolidată prin prevederea unor mecanisme menite să verifice dacă aceste coduri oferă „specificații și soluții tehnice" eficace și stabilesc „obiective clare și indicatori-cheie de performanță pentru a măsura realizarea obiectivelor respective" ca parte integrantă a codurilor în cauză. În plus, absența oricărei trimiteri la mecanisme de monitorizare (obligatorii) pentru codurile de conduită menite să verifice dacă furnizorii de sisteme de IA care nu prezintă un grad ridicat de risc respectă dispozițiile acestora, precum și posibilitatea ca furnizorii individuali să elaboreze (și să pună ei înșiși în aplicare) codurile menționate (a se vedea secțiunea 5.2.7 din expunerea de motive) pot slăbi și mai mult eficacitatea și aplicabilitatea acestor instrumente.

80. În cele din urmă, CEPD și AEPD solicită clarificări cu privire la tipurile de inițiative pe care Comisia le poate dezvolta, în conformitate cu considerentul (81) din propunere, „pentru a facilita reducerea barierelor tehnice care împiedică schimbul transfrontalier de date pentru dezvoltarea IA".

4 CONCLUZIE

81. Deși CEPD și AEPD salută propunerea Comisiei și consideră că un astfel de regulament este necesar pentru a garanta drepturile fundamentale ale cetățenilor și rezidenților UE, acestea consideră că propunerea trebuie adaptată în mai multe privințe, pentru a asigura aplicabilitatea și eficiența acesteia.

82. Având în vedere complexitatea propunerii, precum și aspectele pe care aceasta urmărește să le abordeze, mai rămân multe de făcut până când propunerea poate da naștere unui cadru juridic funcțional, care să completeze în mod eficient RGPD în ceea ce privește protejarea drepturilor fundamentale ale omului, promovând în același timp inovarea. CEPD și AEPD vor fi în continuare disponibile pentru a-și oferi sprijinul în acest demers.

Bruxelles, 18 iunie 2021

Pentru Comitetul european pentru protecția datelor	Pentru Autoritatea Europeană pentru Protecția Datelor
Președintele	Autoritatea
Andrea JELINEK	Wojciech Rafał WIEWIÓROWSKI