Consiliul
Uniunii Europene

Bruxelles, 23 aprilie 2021
(OR. en)

8115/21

Dosar interinstituțional:
2021/0106 (COD)

TELECOM 156
JAI 429
COPEN 191
CYBER 108
DATAPROTECT 103
EJUSTICE 41
COSI 69
IXIM 74
ENFOPOL 148
FREMP 103
RELEX 347
MI 271
COMPET 275
IA 60
CODEC 573

NOTĂ DE ÎNSOȚIRE

Sursă:	Secretara Generală a Comisiei Europene, sub semnătura dnei Martine DEPREZ, Directoare
Data primirii:	22 iunie 2021
Destinatar:	Dl Jeppe TRANHOLM-MIKKELSEN, Secretarul General al Consiliului Uniunii Europene
Nr. doc. Csie:	COM(2021) 206 final
Subiect:	Propunere de REGULAMENT AL PARLAMENTULUI EUROPEAN ȘI AL CONSILIULUI DE STABILIRE A UNOR NORME ARMONIZATE PRIVIND INTELIGENȚA ARTIFICIALĂ (LEGEA PRIVIND INTELIGENȚA ARTIFICIALĂ) ȘI DE MODIFICARE A ANUMITOR ACTE LEGISLATIVE ALE UNIUNII

În anexă, se pune la dispoziția delegațiilor documentul COM(2021) 206 final.

Anexă: COM(2021) 206 final

COMISIA
EUROPEANĂ

Bruxelles, 21.4.2021
COM(2021) 206 final

2021/0106 (COD)

Propunere de

REGULAMENT AL PARLAMENTULUI EUROPEAN ȘI AL CONSILIULUI

DE STABILIRE A UNOR NORME ARMONIZATE PRIVIND INTELIGENȚA ARTIFICIALĂ (LEGEA PRIVIND INTELIGENȚA ARTIFICIALĂ) ȘI DE MODIFICARE A ANUMITOR ACTE LEGISLATIVE ALE UNIUNII

{SEC(2021) 167 final} - {SWD(2021) 84 final} - {SWD(2021) 85 final}

EXPUNERE DE MOTIVE

1. CONTEXTUL PROPUNERII

1.1. Temeiurile și obiectivele propunerii

Prezenta expunere de motive însoțește propunerea de regulament de stabilire a unor norme armonizate privind inteligența artificială (Legea privind inteligența artificială). Inteligența artificială (IA) este o familie de tehnologii cu evoluție rapidă, care poate genera o gamă largă de beneficii economice și societale în întregul spectru de industrii și activități sociale. Prin îmbunătățirea previziunilor, optimizarea operațiunilor și a alocării resurselor, precum și prin personalizarea furnizării de servicii, utilizarea inteligenței artificiale poate sprijini rezultatele benefice din punct de vedere social și ecologic și poate oferi avantaje concurențiale esențiale întreprinderilor și economiei europene. Astfel de acțiuni sunt necesare în special în sectoarele cu impact puternic, inclusiv în sectoare precum schimbările climatice, mediul și sănătatea, sectorul public, finanțele, mobilitatea, afacerile interne și agricultura. Totuși, aceleași elemente și tehnici care alimentează beneficiile socioeconomice ale IA pot genera, de asemenea, noi riscuri sau consecințe negative pentru persoane sau pentru societate. Având în vedere rapiditatea schimbărilor tehnologice și posibilele provocări, UE se angajează să depună eforturi pentru o abordare echilibrată. Este în interesul Uniunii să mențină poziția de lider tehnologic al UE și să asigure posibilitatea ca europenii să beneficieze de noile tehnologii dezvoltate și care funcționează în conformitate cu valorile, drepturile fundamentale și principiile Uniunii.

Prezenta propunere dă curs angajamentului politic al președintei von der Leyen care a anunțat în orientările sale politice pentru mandatul 2019-2024 al Comisiei „O Uniune mai ambițioasă”[1] că Comisia va prezenta acte legislative pentru o abordare europeană coordonată a implicațiilor umane și etice ale IA. Ca urmare a acestui anunț, la 19 februarie 2020, Comisia a publicat Cartea albă privind Inteligența artificială – O abordare europeană axată pe excelență și încredere[2]. Cartea albă stabilește opțiuni de politică privind modul în care se poate atinge dublul obiectiv de promovare a utilizării IA și de abordare a riscurilor asociate anumitor utilizări ale unei astfel de tehnologii. Prezenta propunere vizează punerea în aplicare a celui de al doilea obiectiv pentru dezvoltarea unui ecosistem de încredere, propunând un cadru juridic pentru o IA de încredere. Propunerea are la bază valorile și drepturile fundamentale ale UE și urmărește să ofere oamenilor și altor utilizatori încrederea de a adopta soluții bazate pe IA, încurajând, în același timp, întreprinderile să le dezvolte. IA ar trebui să fie un instrument pentru oameni și o forță a binelui în societate, cu scopul final de a ridica nivelul de bunăstare a oamenilor. Normele privind IA disponibile pe piața Uniunii sau care afectează în alt mod populația Uniunii ar trebui, prin urmare, să fie centrate pe oameni, astfel încât aceștia să poată avea încredere că tehnologia este utilizată într-un mod sigur și conform cu legislația, inclusiv cu respectarea drepturilor fundamentale. În urma publicării cărții albe, Comisia a lansat o consultare amplă a părților interesate, întâmpinată cu interes deosebit de numeroase părți interesate care au sprijinit în mare măsură intervenția normativă pentru abordarea provocărilor și a preocupărilor generate de utilizarea tot mai frecventă a IA.

Propunerea răspunde, de asemenea, unor solicitări explicite din partea Parlamentului European (PE) și a Consiliului European, care au cerut în mod repetat luarea de măsuri legislative pentru a asigura buna funcționare a pieței interne a sistemelor de inteligență

[1] https://ec.europa.eu/commission/sites/beta-political/files/political-guidelines-next-commission_ro.pdf.

[2] Comisia Europeană, Cartea albă privind inteligența artificială – O abordare europeană axată pe excelență și încredere, COM(2020) 65 final, 2020.

artificială („sisteme de IA”), în care atât beneficiile, cât și riscurile IA sunt abordate în mod adecvat la nivelul Uniunii. Aceasta vine în sprijinul obiectivului Uniunii de a fi lider mondial în ceea ce privește dezvoltarea unei inteligențe artificiale sigure, de încredere și etice, astfel cum a afirmat Consiliul European[3], și asigură protecția principiilor morale, astfel cum a solicitat în mod expres Parlamentul European[4].

În 2017, Consiliul European a solicitat „o conștientizare a urgenței de a aborda tendințele emergente”, inclusiv „aspecte cum ar fi inteligența artificială [...], garantându-se, în același timp, un nivel ridicat de protecție a datelor, de drepturi digitale și de standarde etice”[5]. În concluziile sale din 2019 referitoare la Planul coordonat privind dezvoltarea și utilizarea inteligenței artificiale *made in Europe*[6], Consiliul a subliniat în continuare importanța asigurării respectării depline a drepturilor cetățenilor Uniunii și a solicitat o revizuire a legislației relevante existente pentru a o adapta scopului pentru noile oportunități și provocări generate de IA. Consiliul European a mai solicitat o determinare clară a aplicațiilor IA care ar trebui considerate ca având un grad ridicat de risc[7].

Cele mai recente concluzii din 21 octombrie 2020 au solicitat, de asemenea, abordarea opacității, a complexității, a părtinirii, a unui anumit grad de imprevizibilitate și a comportamentului parțial autonom al anumitor sisteme de IA, pentru a asigura compatibilitatea acestora cu drepturile fundamentale și a facilita aplicarea normelor juridice[8].

Parlamentul European și-a asumat, de asemenea, un volum considerabil de sarcini în domeniul IA. În octombrie 2020, acesta a adoptat o serie de rezoluții legate de IA, inclusiv privind etica[9], răspunderea[10] și drepturile de autor[11]. În 2021, ele au fost urmate de rezoluții privind IA în materie penală[12] și în sectorul educației, al culturii și al audiovizualului[13]. Rezoluția PE conținând recomandări adresate Comisiei privind cadrul de aspecte etice asociate cu inteligența artificială, robotica și tehnologiile conexe recomandă în mod specific Comisiei să propună măsuri legislative pentru a valorifica oportunitățile și beneficiile IA, dar

---

3 Consiliul European, Reuniunea extraordinară a Consiliului European (1-2 octombrie 2020) – Concluzii, EUCO 13/20, 2020, p. 6.

4 Rezoluția Parlamentului European din 20 octombrie 2020 conținând recomandări adresate Comisiei privind cadrul de aspecte etice asociate cu inteligența artificială, robotica și tehnologiile conexe, 2020/2012 (INL).

5 Consiliul European, *Reuniunea Consiliului European (19 octombrie 2017) – Concluzie* EUCO 14/17, 2017, p. 8.

6 Consiliul Uniunii Europene, *Inteligența artificială b) Concluzii referitoare la Planul coordonat privind inteligența artificială – Adoptare* 6177/19, 2019.

7 Consiliul European, *Reuniunea extraordinară a Consiliului European (1-2 octombrie 2020) – Concluzii* EUCO 13/20, 2020.

8 Consiliul Uniunii Europene, *Concluziile președinției cu privire la Carta drepturilor fundamentale în contextul inteligenței artificiale și al schimbărilor digitale*, 11481/20, 2020.

9 Rezoluția Parlamentului European din 20 octombrie 2020 conținând recomandări adresate Comisiei privind cadrul de aspecte etice asociate cu inteligența artificială, robotica și tehnologiile conexe, 2020/2012 (INL).

10 Rezoluția Parlamentului European din 20 octombrie 2020 conținând recomandări adresate Comisiei privind regimul de răspundere civilă pentru inteligența artificială, 2020/2014 (INL).

11 Rezoluția Parlamentului European din 20 octombrie 2020 referitoare la drepturile de proprietate intelectuală pentru dezvoltarea tehnologiilor din domeniul inteligenței artificiale, 2020/2015 (INI).

12 Proiect de raport al Parlamentului European privind inteligența artificială în dreptul penal și utilizarea sa de către autoritățile polițienești și judiciare în procedurile penale, 2020/2016 (INI).

13 Proiect de raport al Parlamentului European referitor la inteligența artificială în educație, cultură și sectorul audiovizual, 2020/2017 (INI). În acest sens, Comisia a adoptat Planul de acțiune pentru educația digitală 2021-2027: Resetarea educației și formării pentru era digitală, care prevede elaborarea unor orientări etice în domeniul IA și al utilizării datelor în educație – Comunicarea Comisiei COM(2020) 624 final.

și pentru a asigura protecția principiilor etice. Rezoluția include un text al propunerii legislative de regulament privind principiile etice pentru dezvoltarea, implementarea și utilizarea IA, a roboticii și a tehnologiilor conexe. În conformitate cu angajamentul politic asumat de președinta von der Leyen în orientările sale politice în ceea ce privește rezoluțiile adoptate de Parlamentul European în temeiul articolului 225 din TFUE, prezenta propunere ține seama de rezoluția Parlamentului European menționată anterior, cu respectarea deplină a principiilor proporționalității, subsidiarității și unei mai bune legiferări.

În acest context politic, Comisia prezintă cadrul de reglementare propus privind inteligența artificială având următoarele **obiective specifice**:

- asigurarea faptului că sistemele de IA introduse pe piața Uniunii și utilizate sunt sigure și respectă legislația existentă privind drepturile fundamentale și valorile Uniunii;
- asigurarea securității juridice pentru a facilita investițiile și inovarea în domeniul IA;
- consolidarea guvernanței și asigurarea efectivă a respectării legislației existente privind drepturile fundamentale și a cerințelor de siguranță aplicabile sistemelor de IA;
- facilitarea dezvoltării unei piețe unice pentru sisteme de IA legale, sigure și de încredere și prevenirea fragmentării pieței.

Pentru atingerea acestor obiective, propunerea de față prezintă o abordare orizontală echilibrată și proporțională în materie de reglementare a IA care se limitează la cerințele minime necesare pentru abordarea riscurilor și a problemelor legate de IA, fără a limita sau a împiedica în mod nejustificat dezvoltarea tehnologică sau fără a ridica altfel în mod disproporționat costul introducerii pe piață a soluțiilor IA. Propunerea stabilește un cadru juridic robust și flexibil. Pe de o parte, acesta este cuprinzător și adaptat exigențelor viitorului în opțiunile sale de reglementare fundamentale, inclusiv în ceea ce privește cerințele bazate pe principii pe care ar trebui să le respecte sistemele de IA. Pe de altă parte, instituie un cadru de reglementare proporțional, axat pe o abordare de reglementare bine definită bazată pe riscuri, care nu creează restricții inutile în calea comerțului, prin care intervenția juridică este adaptată la acele situații concrete în care există un motiv justificat de îngrijorare sau în care o astfel de îngrijorare poate fi anticipată în mod rezonabil în viitorul apropiat. În același timp, cadrul juridic include mecanisme flexibile care permit adaptarea dinamică a acestuia pe măsură ce tehnologia evoluează și apar situații noi îngrijorătoare.

Propunerea stabilește norme armonizate pentru dezvoltarea, introducerea pe piață și utilizarea sistemelor de IA în Uniune, urmând o abordare proporțională bazată pe riscuri. Aceasta propune o definiție unică a IA adaptată exigențelor viitorului. Anumite practici de IA deosebit de dăunătoare sunt interzise, deoarece contravin valorilor Uniunii, propunându-se în același timp restricții și garanții specifice în legătură cu anumite utilizări ale sistemelor de identificare biometrică la distanță în scopul asigurării respectării legii. Propunerea stabilește o metodologie solidă privind riscurile pentru a defini sisteme de IA „cu grad ridicat de risc” care prezintă riscuri semnificative pentru sănătatea și siguranța persoanelor sau pentru drepturile fundamentale ale acestora. Aceste sisteme de IA vor trebui să respecte un set de cerințe orizontale obligatorii pentru o IA de încredere și să urmeze procedurile de evaluare a conformității înainte să poată fi introduse pe piața Uniunii. Furnizorilor și utilizatorilor acestor sisteme li se impun, de asemenea, obligații previzibile, proporționale și clare pentru a asigura siguranța și respectarea legislației existente care protejează drepturile fundamentale pe parcursul întregului ciclu de viață al sistemelor de IA. Pentru unele sisteme de IA specifice,

sunt propuse doar obligații minime de transparență, în special atunci când se utilizează roboți de chat sau „deepfake-uri”.

Normele propuse vor fi puse în aplicare prin intermediul unui sistem de guvernanță la nivelul statelor membre, bazat pe structurile deja existente, și al unui mecanism de cooperare la nivelul Uniunii prin instituirea unui Comitet european pentru inteligența artificială. De asemenea, sunt propuse măsuri suplimentare pentru a sprijini inovarea, în special prin intermediul spațiilor de testare în materie de reglementare a IA și al altor măsuri de reducere a sarcinii de reglementare și de sprijinire a întreprinderilor mici și mijlocii („IMM-uri”) și a întreprinderilor nou-înființate.

1.2. Coerența cu dispozițiile deja existente în domeniul de politică vizat

Caracterul orizontal al propunerii necesită o coerență deplină cu legislația existentă a Uniunii aplicabilă sectoarelor în care sistemele de IA cu grad ridicat de risc sunt deja utilizate sau este probabil să fie utilizate în viitorul apropiat.

De asemenea, este asigurată coerența cu Carta drepturilor fundamentale a Uniunii Europene și cu legislația secundară existentă a Uniunii privind protecția datelor, protecția consumatorilor, nediscriminarea și egalitatea de gen. Propunerea nu aduce atingere Regulamentului general privind protecția datelor [Regulamentul (UE) 2016/679] și Directivei privind protecția datelor în materie de asigurare a respectării legii [Directiva (UE) 2016/680] și le completează cu un set de norme armonizate aplicabile proiectării, dezvoltării și utilizării anumitor sisteme de IA cu grad ridicat de risc și cu restricții privind anumite utilizări ale sistemelor de identificare biometrică la distanță. În plus, propunerea completează dreptul existent al Uniunii privind nediscriminarea cu cerințe specifice care vizează reducerea la minimum a riscului de discriminare algoritmică, în special în ceea ce privește proiectarea și calitatea seturilor de date utilizate pentru dezvoltarea sistemelor de IA, completate cu obligații de testare, de gestionare a riscurilor, de documentare și de supraveghere umană pe parcursul întregului ciclu de viață al sistemelor de IA. Propunerea nu aduce atingere aplicării dreptului Uniunii în materie de concurență.

În ceea ce privește sistemele de IA cu grad ridicat de risc care sunt componente de siguranță ale produselor, prezenta propunere va fi integrată în legislația sectorială existentă în materie de siguranță pentru a asigura coerența, a evita suprapunerile și a reduce la minimum sarcinile suplimentare. În special, în ceea ce privește sistemele de IA cu grad ridicat de risc legate de produsele reglementate de legislația privind noul cadru legislativ (NCL) (de exemplu, echipamente tehnice, dispozitive medicale, jucării), cerințele pentru sistemele de IA prevăzute în prezenta propunere vor fi verificate ca parte a procedurilor existente de evaluare a conformității în temeiul legislației relevante NCL. În ceea ce privește interacțiunea dintre cerințe, deși riscurile de siguranță specifice sistemelor de IA sunt menite să fie acoperite de cerințele prezentei propuneri, legislația NCL vizează asigurarea siguranței generale a produsului final și, prin urmare, poate conține cerințe specifice privind integrarea în siguranță a unui sistem de IA în produsul final. Propunerea de Regulament privind echipamentele tehnice, care este adoptată în aceeași zi cu prezenta propunere, reflectă pe deplin această abordare. În ceea ce privește sistemele de IA cu grad ridicat de risc legate de produsele reglementate de legislația relevantă din cadrul vechii abordări (de exemplu, aviație, autoturisme), prezenta propunere nu s-ar aplica în mod direct. Cu toate acestea, cerințele esențiale *ex ante* pentru sistemele de IA cu grad ridicat de risc stabilite în prezenta propunere vor trebui să fie luate în considerare atunci când se adoptă acte legislative de punere în aplicare sau acte delegate relevante în temeiul actelor respective.

În ceea ce privește sistemele de IA furnizate sau utilizate de instituțiile de credit reglementate, autoritățile responsabile cu supravegherea legislației Uniunii privind serviciile financiare ar

trebui desemnate drept autorități competente pentru supravegherea cerințelor din prezenta propunere, pentru a asigura o aplicare coerentă a obligațiilor prevăzute în prezenta propunere și în legislația Uniunii privind serviciile financiare, în care sistemele de IA sunt reglementate implicit într-o anumită măsură în raport cu sistemul intern de guvernanță al instituțiilor de credit. Pentru a spori și mai mult coerența, procedura de evaluare a conformității și unele dintre obligațiile procedurale ale furnizorilor în temeiul prezentei propuneri sunt integrate în procedurile prevăzute în Directiva 2013/36/UE cu privire la accesul la activitatea instituțiilor de credit și supravegherea prudențială[14].

Prezenta propunere este, de asemenea, în concordanță cu legislația aplicabilă a Uniunii privind serviciile, inclusiv în ceea ce privește serviciile de intermediere reglementate de Directiva 2000/31/CE[15] privind comerțul electronic și de recenta propunere a Comisiei referitoare la Actul legislativ privind serviciile digitale („*Digital Services Act*" – DSA)[16].

În ceea ce privește sistemele de IA care sunt componente ale sistemelor informatice la scară largă în spațiul de libertate, securitate și justiție gestionat de Agenția Uniunii Europene pentru Gestionarea Operațională a Sistemelor Informatice la Scară Largă în Spațiul de Libertate, Securitate și Justiție (eu-LISA), propunerea nu se va aplica acelor sisteme de IA care au fost introduse pe piață sau puse în funcțiune înainte de a trece un an de la data aplicării prezentului regulament, cu excepția cazului în care înlocuirea sau modificarea respectivelor acte juridice duce la o modificare semnificativă a proiectării sau a scopului preconizat al sistemului sau sistemelor de IA în cauză.

1.3. Coerența cu alte politici ale Uniunii

Propunerea face parte dintr-un pachet cuprinzător mai amplu de măsuri care abordează problemele ridicate de dezvoltarea și utilizarea IA, astfel cum s-a analizat în Cartea albă privind IA. Prin urmare, se asigură coerența și complementaritatea cu alte inițiative în curs sau planificate ale Comisiei care vizează, de asemenea, abordarea acestor probleme, inclusiv revizuirea legislației sectoriale privind produsele (de exemplu, Directiva privind echipamentele tehnice, Directiva privind siguranța generală a produselor) și inițiativele care abordează aspecte legate de răspundere în legătură cu noile tehnologii, inclusiv sistemele de IA. Aceste inițiative se vor baza pe prezenta propunere și o vor completa pentru a aduce claritate juridică și pentru a încuraja dezvoltarea unui ecosistem de încredere în IA în Europa.

Propunerea este coerentă cu strategia digitală generală a Comisiei în ceea ce privește contribuția sa la promovarea tehnologiei în serviciul cetățenilor, unul dintre cei trei piloni principali ai orientării politice și ai obiectivelor anunțate în comunicarea intitulată „Conturarea viitorului digital al Europei"[17]. Aceasta stabilește un cadru coerent, eficace și proporțional pentru a se asigura dezvoltarea IA în moduri care respectă drepturile cetățenilor

---

[14] Directiva 2013/36/UE a Parlamentului European și a Consiliului din 26 iunie 2013 cu privire la accesul la activitatea instituțiilor de credit și supravegherea prudențială a instituțiilor de credit și a firmelor de investiții, de modificare a Directivei 2002/87/CE și de abrogare a Directivelor 2006/48/CE și 2006/49/CE (Text cu relevanță pentru SEE), JO L 176, 27.6.2013, p. 338-436.

[15] Directiva 2000/31/CE a Parlamentului European și a Consiliului din 8 iunie 2000 privind anumite aspecte juridice ale serviciilor societății informaționale, în special ale comerțului electronic, pe piața internă („Directiva privind comerțul electronic"), (JO L 178, 17.7.2000, p. 1-16).

[16] A se vedea Propunerea de REGULAMENT AL PARLAMENTULUI EUROPEAN ȘI AL CONSILIULUI privind o piață unică pentru serviciile digitale (Actul legislativ privind serviciile digitale) și de modificare a Directivei 2000/31/CE, COM/2020/825 final.

[17] Comunicarea Comisiei, „Conturarea viitorului digital al Europei", COM/2020/67 final.

și câștigă încrederea acestora, creând o Europă pregătită pentru era digitală și transformând următorii zece ani în **deceniul digital**[18].

În plus, promovarea inovării bazate pe IA este strâns legată de **Legea privind guvernanța datelor**[19]**,** de **Directiva privind datele deschise**[20] și de alte inițiative din cadrul **Strategiei UE privind datele**[21], care vor institui mecanisme și servicii de încredere pentru reutilizarea, partajarea și punerea în comun a datelor care sunt esențiale pentru dezvoltarea unor modele de IA bazate pe date de înaltă calitate.

Propunerea consolidează, de asemenea, în mod semnificativ rolul Uniunii de a contribui la definirea normelor și a standardelor globale și de a promova o IA de încredere, care să fie în concordanță cu valorile și interesele Uniunii. Aceasta oferă Uniunii o bază solidă pentru a colabora în continuare cu partenerii săi externi, inclusiv cu țările terțe, și în cadrul forurilor internaționale cu privire la aspecte legate de IA.

2. TEMEI JURIDIC, SUBSIDIARITATE ȘI PROPORȚIONALITATE

2.1. Temeiul juridic

Temeiul juridic al propunerii este, în primul rând, articolul 114 din Tratatul privind funcționarea Uniunii Europene (TFUE), care prevede adoptarea de măsuri pentru a asigura instituirea și funcționarea pieței interne.

Prezenta propunere constituie o parte esențială a strategiei UE privind piața unică digitală. Obiectivul principal al prezentei propuneri este de a asigura buna funcționare a pieței interne prin stabilirea unor norme armonizate, în special privind dezvoltarea, introducerea pe piața Uniunii și utilizarea produselor și a serviciilor care utilizează tehnologii IA sau care sunt furnizate ca sisteme de IA autonome. Unele state membre au deja în vedere norme naționale pentru a se asigura că IA este sigură și este dezvoltată și utilizată în conformitate cu obligațiile privind drepturile fundamentale. Acest lucru va genera probabil două probleme principale: i) fragmentarea pieței interne în ceea ce privește elementele esențiale, în special în ceea ce privește cerințele pentru produsele și serviciile IA, comercializarea acestora, utilizarea lor, răspunderea și supravegherea de către autoritățile publice și ii) reducerea substanțială a securității juridice atât pentru furnizorii, cât și pentru utilizatorii de sisteme de IA cu privire la modul în care normele existente și cele noi se vor aplica acestor sisteme în Uniune. Având în vedere circulația largă a produselor și serviciilor la nivel transfrontalier, aceste două probleme pot fi rezolvate cel mai bine prin intermediul legislației UE de armonizare.

Într-adevăr, propunerea definește cerințe obligatorii comune aplicabile proiectării și dezvoltării anumitor sisteme de IA înainte ca acestea să fie introduse pe piață, care vor fi operaționalizate în continuare prin standarde tehnice armonizate. Propunerea abordează, de asemenea, situația după introducerea pe piață a sistemelor de IA prin armonizarea modului în care sunt efectuate verificările *ex post*.

În plus, având în vedere că prezenta propunere conține anumite norme specifice privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal, în

---

18 Busola pentru dimensiunea digitală către 2030: o traiectorie europeană pentru deceniul digital.

19 Propunere de regulament privind guvernanța datelor la nivel european (Legea privind guvernanța datelor) COM/2020/767.

20 Directiva (UE) 2019/1024 a Parlamentului European și a Consiliului din 20 iunie 2019 privind datele deschise și reutilizarea informațiilor din sectorul public, PE/28/2019/REV/1, JO L 172, 26.6.2019, p. 56-83.

21 Comunicarea Comisiei intitulată „O strategie europeană privind datele”, COM(2020) 66 final.

special restricții privind utilizarea sistemelor de IA pentru identificarea biometrică la distanță „în timp real” în spațiile accesibile publicului în scopul asigurării respectării legii, este oportun ca prezentul regulament să se întemeieze, în ceea ce privește normele specifice respective, pe articolul 16 din TFUE.

2.2. Subsidiaritatea (în cazul competențelor neexclusive)

Natura IA, care se bazează adesea pe seturi mari și variate de date și care pot fi încorporate în orice produs sau serviciu care circulă liber pe piața internă, implică faptul că obiectivele prezentei propuneri nu pot fi realizate în mod eficace de către statele membre la nivel individual. În plus, un mozaic emergent de norme naționale potențial divergente va împiedica circulația fără sincope a produselor și a serviciilor legate de sistemele de IA în UE și va fi ineficient în asigurarea siguranței și a protecției drepturilor fundamentale și a valorilor Uniunii în diferitele state membre. Abordările naționale privind tratarea problemelor vor crea doar insecuritate juridică și bariere suplimentare și vor încetini asimilarea IA pe piață.

Obiectivele prezentei propuneri pot fi realizate mai bine la nivelul Uniunii pentru a evita o fragmentare suplimentară a pieței unice în cadre naționale potențial contradictorii care împiedică libera circulație a bunurilor și a serviciilor ce integrează IA. Un cadru european solid de reglementare pentru o IA de încredere va asigura, de asemenea, condiții de concurență echitabile și îi va proteja pe toți cetățenii, consolidând, în același timp, competitivitatea și baza industrială a Europei în domeniul IA. Numai o acțiune comună la nivelul Uniunii poate să protejeze suveranitatea digitală a Uniunii și să mobilizeze instrumentele și competențele sale de reglementare pentru a modela normele și standardele globale.

2.3. Proporționalitatea

Propunerea se bazează pe cadrele juridice existente și este proporțională și necesară pentru atingerea obiectivelor sale, deoarece urmează o abordare bazată pe riscuri și impune sarcini de reglementare numai atunci când un sistem de IA este susceptibil să prezinte un grad ridicat de risc pentru drepturile fundamentale și pentru siguranță. Pentru alte sisteme de IA, care nu prezintă un risc ridicat, sunt impuse doar obligații foarte limitate în materie de transparență, de exemplu în ceea ce privește furnizarea de informații pentru a semnala utilizarea unui sistem de IA atunci când interacționează cu oamenii. Pentru sistemele de IA cu grad ridicat de risc, cerințele privind calitatea ridicată a datelor, documentația și trasabilitatea, transparența, supravegherea umană, acuratețea și robustețea sunt strict necesare pentru a atenua riscurile la adresa drepturilor fundamentale și a siguranței pe care le prezintă IA și care nu sunt acoperite de alte cadre juridice existente. Existența unor norme armonizate și a unor orientări de sprijin și instrumente de asigurare a conformității îi va ajuta pe furnizori și pe utilizatori să respecte cerințele prevăzute în propunere și va reduce la minimum costurile acestora. Costurile suportate de operatori sunt proporționale cu obiectivele atinse și cu beneficiile economice și în materie de reputație pe care operatorii le pot aștepta de la prezenta propunere.

2.4. Alegerea instrumentului

Alegerea unui regulament ca instrument juridic este justificată de necesitatea unei aplicări uniforme a noilor norme, cum ar fi definiția IA, interzicerea anumitor practici dăunătoare bazate pe IA și clasificarea anumitor sisteme de IA. Aplicabilitatea directă a unui regulament, în conformitate cu articolul 288 din TFUE, va reduce fragmentarea juridică și va facilita dezvoltarea unei piețe unice pentru sisteme de IA legale, sigure și de încredere. Acest lucru se va realiza, în special, prin introducerea unui set armonizat de cerințe de bază în ceea ce privește sistemele de IA clasificate ca fiind cu risc ridicat și obligațiile furnizorilor și

utilizatorilor acestor sisteme, prin îmbunătățirea protecției drepturilor fundamentale și prin asigurarea securității juridice atât pentru operatori, cât și pentru consumatori.

În același timp, dispozițiile regulamentului nu sunt excesiv de normative și lasă loc pentru diferite niveluri de acțiune din partea statelor membre pentru elemente care nu subminează obiectivele inițiativei, în special organizarea internă a sistemului de supraveghere a pieței și adoptarea de măsuri de stimulare a inovării.

3. REZULTATE ALE EVALUĂRILOR *EX POST*, CONSULTĂRILOR PĂRȚILOR INTERESATE ȘI EVALUĂRII IMPACTULUI

3.1. Consultările părților interesate

Prezenta propunere este rezultatul unei ample consultări cu toate părțile interesate importante, în cadrul căreia au fost aplicate principiile generale și standardele minime pentru consultarea părților interesate de către Comisie.

La 19 februarie 2020, împreună cu publicarea Cărții albe privind inteligența artificială, a fost lansată o **consultare publică online**, care s-a desfășurat până la 14 iunie 2020. Obiectivul acestei consultări a fost de a colecta păreri și opinii cu privire la cartea albă. Aceasta a vizat toate părțile interesate din sectorul public și privat, inclusiv guvernele, autoritățile locale, organizațiile comerciale și necomerciale, partenerii sociali, experții, mediul academic și cetățenii. După analizarea tuturor răspunsurilor primite, Comisia a publicat un rezumat al rezultatelor și răspunsurile individuale pe site-ul său web[22].

În total, s-au primit 1 215 contribuții, dintre care 352 de la întreprinderi sau organizații/asociații de întreprinderi, 406 de la persoane fizice (92 % persoane din UE), 152 în numele unor instituții academice/de cercetare și 73 de la autorități publice. Vocile societății civile au fost reprezentate de 160 de respondenți (printre care 9 organizații ale consumatorilor, 129 de organizații neguvernamentale și 22 de sindicate), iar 72 de respondenți au contribuit fiind incluși în categoria „alții”. Dintre cei 352 de reprezentanți ai mediului de afaceri și ai industriei, 222 au fost reprezentanți ai întreprinderilor și ai mediului de afaceri, dintre care 41,5 % microîntreprinderi și întreprinderi mici și mijlocii. Restul au fost asociații de întreprinderi. În total, 84 % dintre răspunsurile oferite de întreprinderi și industrie au provenit din UE-27. În funcție de întrebare, între 81 și 598 de respondenți au utilizat opțiunea de text liber pentru a introduce observații. Peste 450 de documente de poziție au fost transmise prin intermediul site-ului EU Survey, fie în plus față de răspunsurile la chestionar (peste 400), fie sub formă de contribuții individuale (peste 50).

Per ansamblu, există un acord general între părțile interesate cu privire la necesitatea de a acționa. Marea majoritate a părților interesate sunt de acord că există lacune legislative sau că este nevoie de o nouă legislație. Cu toate acestea, mai multe părți interesate avertizează Comisia cu privire la evitarea suprapunerilor, a obligațiilor contradictorii și a suprareglementării. Au existat numeroase observații care au subliniat importanța unui cadru de reglementare proporțional și neutru din punct de vedere tehnologic.

Părțile interesate au solicitat, în cea mai mare parte, o definiție restrânsă, clară și precisă a IA. Acestea au subliniat, de asemenea, că, pe lângă clarificarea noțiunii de IA, este important să se definească noțiunile de „risc”, „risc ridicat”, „risc scăzut”, „identificare biometrică la distanță” și „prejudiciu”.

[22] A se vedea toate rezultatele consultării aici.

Majoritatea respondenților sunt în mod explicit în favoarea abordării bazate pe riscuri. Utilizarea unui cadru bazat pe riscuri a fost considerată o opțiune mai bună decât reglementarea generală a tuturor sistemelor de IA. Tipurile de riscuri și amenințări ar trebui să se bazeze pe o abordare sectorială și de la caz la caz. Riscurile ar trebui, de asemenea, calculate ținând seama de impactul asupra drepturilor și asupra siguranței.

Spațiile de testare în materie de reglementare ar putea fi foarte utile pentru promovarea IA și sunt salutate de anumite părți interesate, în special de asociațiile de întreprinderi.

Dintre cei care și-au formulat opinia cu privire la modelele de asigurare a respectării legislației, peste 50 %, în special din rândul asociațiilor de întreprinderi, au fost în favoarea unei combinații între o autoevaluare *ex ante* a riscurilor și o aplicare *ex post* pentru sistemele de IA cu grad ridicat de risc.

3.2. Obținerea și utilizarea expertizei

Propunerea se bazează pe doi ani de analiză și pe implicarea strânsă a părților interesate, inclusiv a cadrelor universitare, a întreprinderilor, a partenerilor sociali, a organizațiilor neguvernamentale, a statelor membre și a cetățenilor. Lucrările pregătitoare au început în 2018 prin înființarea **Grupului de experți la nivel înalt privind inteligența artificială (*High-Level Expert Group on AI* – HLEG)**, care a avut o componență amplă și care reflectă principiul incluziunii, fiind format din 52 de experți bine-cunoscuți, însărcinați să consilieze Comisia cu privire la punerea în aplicare a Strategiei Comisiei privind inteligența artificială. În aprilie 2019, Comisia a sprijinit[23] cerințele-cheie prevăzute în Orientările în materie de etică ale Grupului de experți la nivel înalt pentru o IA de încredere[24], care au fost revizuite pentru a lua în considerare peste 500 de contribuții din partea părților interesate. Cerințele-cheie reflectă o abordare larg răspândită și comună, după cum reiese din multitudinea de coduri și principii etice elaborate de numeroase organizații publice și private din Europa și din afara acesteia, potrivit cărora dezvoltarea și utilizarea IA ar trebui să se ghideze după anumite principii esențiale orientate spre valori. Lista de evaluare pentru o inteligență artificială de încredere (*List for Trustworthy Artificial Intelligence* – ALTAI)[25] a făcut ca aceste cerințe să devină operaționale în cadrul unui proces-pilot care a implicat peste 350 de organizații.

În plus, a fost creată **Alianța europeană în domeniul inteligenței artificiale**[26], cu scopul de a oferi o platformă pentru aproximativ 4 000 de părți interesate în vederea organizării unor dezbateri privind implicațiile tehnologice și societale ale IA, care să culmineze cu o adunare anuală privind IA.

Cartea albă privind IA a dezvoltat în continuare această abordare favorabilă incluziunii, având ca rezultat transmiterea de observații de către peste 1 250 de părți interesate, inclusiv peste 450 de documente de poziție suplimentare. Prin urmare, Comisia a publicat o evaluare inițială a impactului, care, la rândul său, a atras peste 130 de observații[27]. Au fost organizate, de asemenea, **ateliere și evenimente suplimentare cu părțile interesate**, ale căror rezultate sprijină analiza din evaluarea impactului și alegerile de politică făcute în prezenta

---

23 Comisia Europeană, *Cum construim încrederea cetățenilor într-o inteligență artificială centrată pe factorul uman*, COM(2019) 168.

24 HLEG, *Orientări în materie de etică pentru o inteligență artificială (IA) fiabilă*, 2019.

25 HLEG, *Lista de evaluare pentru o inteligență artificială de încredere (ALTAI)*, 2020.

26 Alianța europeană în domeniul inteligenței artificiale este un forum multipartit lansat în iunie 2018, Alianța europeană în domeniul inteligenței artificiale https://ec.europa.eu/digital-single-market/en/european-ai-alliance.

27 Comisia Europeană, *Evaluarea inițială a impactului unei propuneri de act legislativ al Parlamentul European și al Consiliului în care sunt prevăzute cerințele privind inteligența artificială.*

propunere[28]. De asemenea, a fost comandat un **studiu extern**, pentru a contribui la evaluarea impactului.

3.3. Evaluarea impactului

În conformitate cu politica sa privind o mai bună legiferare, Comisia a efectuat o evaluare a impactului pentru prezenta propunere, examinată de Comitetul de control normativ al Comisiei. La 16 decembrie 2020 a avut loc o reuniune cu Comitetul de control normativ, urmată de un aviz negativ. După o revizuire substanțială a evaluării impactului pentru a răspunde observațiilor și o retransmitere a evaluării impactului, Comitetul de control normativ a emis un aviz pozitiv la 21 martie 2021. Avizele Comitetului de control normativ, recomandările și o explicație a modului în care acestea au fost luate în considerare sunt prezentate în anexa 1 la evaluarea impactului.

Comisia a examinat diferite opțiuni de politică pentru atingerea obiectivului general al propunerii, și anume de **a asigura buna funcționare a pieței unice** prin crearea condițiilor pentru dezvoltarea și utilizarea unei IA de încredere în Uniune.

Au fost evaluate patru opțiuni de politică cu grade diferite de intervenție normativă:

- **opțiunea 1**: un instrument legislativ al UE care să instituie un sistem voluntar de etichetare;
- **opțiunea 2**: o abordare sectorială „ad-hoc”;
- **opțiunea 3**: un instrument legislativ orizontal al UE care să urmeze o abordare proporțională bazată pe riscuri;
- **opțiunea 3+**: un instrument legislativ orizontal al UE care să urmeze o abordare proporțională bazată pe riscuri + coduri de conduită pentru sistemele de IA care nu prezintă un grad ridicat de risc;
- **opțiunea 4**: un instrument legislativ orizontal al UE care să stabilească cerințe obligatorii pentru toate sistemele de IA, indiferent de riscul pe care îl prezintă.

În conformitate cu metodologia stabilită de Comisie, fiecare opțiune de politică a fost evaluată în funcție de impactul economic și societal, cu un accent deosebit pe impactul asupra drepturilor fundamentale. Opțiunea preferată este opțiunea 3+, un cadru de reglementare numai pentru sistemele de IA cu grad ridicat de risc, cu posibilitatea ca toți furnizorii de sisteme de IA care nu prezintă un risc ridicat să urmeze un cod de conduită. Cerințele vor viza datele, documentația și trasabilitatea, furnizarea de informații și transparența, supravegherea umană, robustețea și acuratețea și ar urma să fie obligatorii pentru sistemele de IA cu grad ridicat de risc. Întreprinderile care au introdus coduri de conduită pentru alte sisteme de IA ar urma să facă acest lucru în mod voluntar.

Opțiunea preferată a fost considerată adecvată pentru a aborda în modul cel mai eficace obiectivele prezentei propuneri. Prin impunerea unui set limitat, dar eficace, de acțiuni din partea dezvoltatorilor și a utilizatorilor de IA, opțiunea preferată limitează riscurile de încălcare a drepturilor fundamentale și a siguranței persoanelor și încurajează supravegherea și aplicarea eficace a legii, direcționând cerințele doar către sistemele în cazul cărora există un risc ridicat ca astfel de încălcări să aibă loc. Drept urmare, această opțiune menține costurile de asigurare a conformității la un nivel minim, evitând astfel o încetinire inutilă a gradului de asimilare din cauza prețurilor mai mari și a costurilor de asigurare a conformității. Pentru a

[28] Pentru detalii privind toate consultările care au avut loc, a se vedea anexa 2 la evaluarea impactului.

compensa eventualele dezavantaje pentru IMM-uri, această opțiune include mai multe dispoziții de sprijinire a conformității acestora și de reducere a costurilor acestora, inclusiv crearea unor spații de testare în materie de reglementare și obligația de a lua în considerare interesele IMM-urilor atunci când se stabilesc taxele legate de evaluarea conformității.

Opțiunea preferată va spori încrederea cetățenilor în IA, întreprinderile vor dobândi securitatea juridică, iar statele membre nu vor vedea niciun motiv pentru a lua măsuri unilaterale care ar putea fragmenta piața unică. Ca urmare a creșterii cererii datorită încrederii sporite, a numărului mai mare de oferte disponibile datorită securității juridice și a absenței obstacolelor în calea circulației transfrontaliere a sistemelor de IA, piața unică a IA va prospera cel mai probabil. Uniunea Europeană va continua să dezvolte un ecosistem IA cu creștere rapidă pentru servicii și produse inovatoare care integrează tehnologia IA sau sisteme de IA autonome, ceea ce va duce la o autonomie digitală sporită.

Întreprinderile sau autoritățile publice care dezvoltă sau utilizează aplicații de IA cu grad ridicat de risc pentru siguranța sau drepturile fundamentale ale cetățenilor ar trebui să respecte cerințe și obligații specifice. Respectarea acestor cerințelor ar implica costuri de aproximativ 6 000-7 000 EUR pentru furnizarea unui sistem de IA cu grad mediu ridicat de risc de aproximativ 170 000 EUR până în 2025. Pentru utilizatorii de IA, ar exista, de asemenea, costul anual al timpului dedicat asigurării supravegherii umane, atunci când este cazul, în funcție de cazul de utilizare. Acesta a fost estimat la aproximativ 5 000-8 000 EUR pe an. Costurile de verificare s-ar putea ridica la încă 3 000-7 500 EUR pentru furnizorii de sisteme de IA cu grad ridicat de risc. Întreprinderile sau autoritățile publice care dezvoltă sau utilizează aplicații de IA care nu sunt clasificate ca prezentând un grad ridicat de risc ar avea doar obligații minime de informare. Cu toate acestea, ele ar putea alege să se alăture celorlalte părți și să adopte împreună un cod de conduită pentru a respecta cerințele adecvate și pentru a se asigura că sistemele lor de IA sunt de încredere. Într-un astfel de caz, costurile ar fi cel mult la fel de ridicate ca cele pentru sistemele de IA cu grad ridicat de risc, dar, cel mai probabil, vor fi mai reduse.

Impactul opțiunilor de politică asupra diferitelor categorii de părți interesate (operatori economici/întreprinderi; organisme de evaluare a conformității, organisme de standardizare și alte organisme publice; persoane fizice/cetățeni; cercetători) este explicat în detaliu în anexa 3 la evaluarea impactului care sprijină prezenta propunere.

3.4. Adecvarea reglementărilor și simplificarea

Prezenta propunere stabilește obligația care se va aplica furnizorilor și utilizatorilor de sisteme de IA cu grad ridicat de risc. Pentru furnizorii care dezvoltă și introduc astfel de sisteme pe piața Uniunii, aceasta va crea securitate juridică și va garanta că nu va apărea niciun obstacol în calea furnizării transfrontaliere de servicii și produse legate de IA. Pentru întreprinderile care utilizează IA, aceasta va promova încrederea în rândul clienților lor. Pentru administrațiile publice naționale, aceasta va promova încrederea publicului în utilizarea IA și va consolida mecanismele de asigurare a respectării legii (prin introducerea unui mecanism european de coordonare, asigurarea capacităților adecvate și facilitarea auditurilor sistemelor de IA prin instituirea de noi cerințe în materie de documentare, trasabilitate și transparență). În plus, cadrul va avea în vedere măsuri specifice de sprijinire a inovării, inclusiv spații de testare în materie de reglementare și măsuri specifice de sprijinire a micilor utilizatori și a furnizorilor de sisteme de IA cu grad ridicat de risc în vederea respectării noilor norme.

Propunerea vizează, de asemenea, în mod specific, consolidarea competitivității și a bazei industriale a Europei în domeniul IA. Se asigură coerența deplină cu legislația sectorială existentă a Uniunii aplicabilă sistemelor de IA (de exemplu, în ceea ce privește produsele și

serviciile), ceea ce va aduce mai multă claritate și va simplifica punerea în aplicare a noilor norme.

3.5. Drepturile fundamentale

Utilizarea IA cu caracteristicile sale specifice (de exemplu, opacitatea, complexitatea, dependența de date, comportamentul autonom) poate afecta în mod negativ o serie de drepturi fundamentale consacrate în Carta drepturilor fundamentale a UE („Carta"). Prezenta propunere urmărește să asigure un nivel ridicat de protecție a acestor drepturi fundamentale și să abordeze diverse surse de riscuri printr-o abordare bazată pe riscuri clar definită. Incluzând un set de cerințe pentru o IA de încredere și obligații proporționale pentru toți participanții la lanțul valoric, propunerea va consolida și va promova protecția drepturilor protejate prin Cartă: dreptul la demnitate umană (articolul 1), respectarea vieții private și protecția datelor cu caracter personal (articolele 7 și 8), nediscriminarea (articolul 21) și egalitatea între femei și bărbați (articolul 23). Scopul său este de a preveni un efect descurajator în ceea ce privește dreptul la libertatea de exprimare (articolul 11) și la libertatea de întrunire (articolul 12), de a asigura protecția dreptului la o cale de atac eficientă și la un proces echitabil, a dreptului la apărare și a prezumției de nevinovăție (articolele 47 și 48), precum și a principiului general al bunei administrări. În plus, după caz, în anumite domenii, propunerea va afecta în mod pozitiv drepturile mai multor grupuri speciale, cum ar fi drepturile lucrătorilor la condiții de muncă echitabile și corecte (articolul 31), un nivel ridicat de protecție a consumatorilor (articolul 28), drepturile copilului (articolul 24) și integrarea persoanelor cu handicap (articolul 26). Dreptul la un nivel ridicat de protecție a mediului și la îmbunătățirea calității acestuia (articolul 37) este, de asemenea, relevant, inclusiv în ceea ce privește sănătatea și siguranța persoanelor. Obligațiile privind testarea *ex ante,* gestionarea riscurilor și supravegherea umană vor facilita, de asemenea, respectarea altor drepturi fundamentale prin reducerea la minimum a riscului unor decizii eronate sau subiective sprijinite de IA în domenii critice precum educația și formarea, ocuparea forței de muncă, serviciile importante, asigurarea respectării legii și sistemul judiciar. În cazul în care se produc totuși încălcări ale drepturilor fundamentale, vor fi posibile măsuri reparatorii eficace pentru persoanele afectate, prin asigurarea transparenței și a trasabilității sistemelor de IA, împreună cu verificări *ex post* solide.

Prezenta propunere impune anumite restricții asupra libertății de a desfășura o activitate comercială (articolul 16) și asupra libertății artelor și științelor (articolul 13), pentru a asigura respectarea unor motive imperative de interes public major, cum ar fi sănătatea, siguranța, protecția consumatorilor și protecția altor drepturi fundamentale („inovare responsabilă") atunci când se dezvoltă și se utilizează tehnologii IA cu grad ridicat de risc. Restricțiile respective sunt proporționale și limitate la nivelul minim necesar pentru a preveni și a atenua riscurile semnificative în materie de siguranță și posibilele încălcări ale drepturilor fundamentale.

De asemenea, obligațiile sporite în materie de transparență nu vor afecta în mod disproporționat dreptul la protecția proprietății intelectuale [articolul 17 alineatul (2)], deoarece acestea se vor limita doar la informațiile minime necesare pentru ca persoanele fizice să își poată exercita dreptul la o cale de atac eficientă și la transparența necesară față de autoritățile de supraveghere și de aplicare a legii, în conformitate cu mandatele acestora. Orice divulgare de informații se va efectua în conformitate cu legislația relevantă în domeniu, inclusiv cu Directiva 2016/943 privind protecția know-how-ului și a informațiilor de afaceri nedivulgate (secrete comerciale) împotriva dobândirii, utilizării și divulgării ilegale. Atunci când autorităților publice și organismelor notificate trebuie să li se acorde acces la informații confidențiale sau la codul sursă pentru a examina respectarea obligațiilor substanțiale, acestea sunt supuse unor obligații de confidențialitate obligatorii.

4. IMPLICAȚII BUGETARE

Statele membre vor trebui să desemneze autorități de supraveghere responsabile cu punerea în aplicare a cerințelor legislative. Funcția lor de supraveghere s-ar putea baza pe mecanismele existente, de exemplu în ceea ce privește organismele de evaluare a conformității sau supravegherea pieței, dar ar necesita expertiză tehnică și resurse umane și financiare suficiente. În funcție de structura preexistentă în fiecare stat membru, ar putea fi necesare între 1 și 25 de echivalente normă întreagă pentru fiecare stat membru.

O prezentare detaliată a costurilor implicate este inclusă în „fișa financiară” aferentă prezentei propuneri.

5. ELEMENTE DIVERSE

5.1. Planurile de implementare și mecanismele de monitorizare, evaluare și raportare

Este esențial să se prevadă un mecanism solid de monitorizare și evaluare pentru a se asigura că propunerea va fi eficace în ceea ce privește atingerea obiectivelor sale specifice. Comisia va fi responsabilă de monitorizarea efectelor propunerii. Aceasta va institui un sistem de înregistrare a aplicațiilor de IA autonome cu grad ridicat de risc într-o bază de date publică la nivelul UE. Această înregistrare va permite, de asemenea, autorităților competente, utilizatorilor și altor persoane interesate să verifice dacă sistemul de IA cu grad ridicat de risc respectă cerințele prevăzute în propunere și să exercite o supraveghere mai strictă asupra acelor sisteme de IA care prezintă riscuri ridicate pentru drepturile fundamentale. Pentru a alimenta această bază de date, furnizorii de IA vor fi obligați să furnizeze informații pertinente cu privire la sistemele lor și la evaluarea conformității efectuate în cadrul sistemelor respective.

În plus, furnizorii de IA vor fi obligați să informeze autoritățile naționale competente cu privire la incidentele grave sau la disfuncționalitățile care constituie o încălcare a obligațiilor privind drepturile fundamentale de îndată ce iau cunoștință de acestea, precum și cu privire la orice rechemare sau retragere de pe piață a sistemelor de IA. Ulterior, autoritățile naționale competente vor investiga incidentele/disfuncționalitățile, vor colecta toate informațiile necesare și le vor transmite periodic Comisiei, cu metadate adecvate. Comisia va completa aceste informații privind incidentele printr-o analiză cuprinzătoare a pieței globale a IA.

Comisia va publica un raport de evaluare și revizuire a cadrului privind IA propus la cinci ani de la data la care acesta devine aplicabil.

5.2. Explicații detaliate cu privire la prevederile specifice ale propunerii

5.2.1. DOMENIU DE APLICARE ȘI DEFINIȚII (TITLUL I)

Titlul I definește obiectul regulamentului și domeniul de aplicare al noilor norme care reglementează introducerea pe piață, punerea în funcțiune și utilizarea sistemelor de IA. Acesta stabilește, de asemenea, definițiile utilizate în cadrul instrumentului. Definiția sistemului de IA în cadrul juridic urmărește să fie cât mai neutră din punct de vedere tehnologic și cât mai adaptată exigențelor viitorului, ținând seama de evoluțiile rapide tehnologice și ale pieței în legătură cu IA. Pentru a asigura securitatea juridică necesară, titlul I este completat de anexa I, care conține o listă detaliată a abordărilor și tehnicilor de dezvoltare a IA care urmează să fie adaptate de către Comisie în funcție de noile evoluții tehnologice. Sunt, de asemenea, definiți în mod clar principalii participanți din întregul lanț valoric al IA, cum ar fi furnizorii și utilizatorii de sisteme de IA care acoperă atât operatorii publici, cât și pe cei privați, pentru a asigura condiții de concurență echitabile.

5.2.2. PRACTICI INTERZISE ÎN DOMENIUL INTELIGENȚEI ARTIFICIALE (TITLUL II)

Titlul II stabilește o listă a practicilor IA interzise. Regulamentul urmează o abordare bazată pe riscuri, făcând distincție între utilizările IA care creează (i) un risc inacceptabil, (ii) un risc ridicat și (iii) un risc scăzut sau minim. Lista practicilor interzise din titlul II cuprinde toate sistemele de IA a căror utilizare este considerată inacceptabilă întrucât contravin valorilor Uniunii, de exemplu prin încălcarea drepturilor fundamentale. Interdicțiile se referă la practicile care au un potențial semnificativ de manipulare a persoanelor prin tehnici subliminale dincolo de conștiința acestora sau de exploatare a vulnerabilităților unor categorii vulnerabile specifice, cum ar fi copiii sau persoanele cu handicap, pentru a le denatura în mod semnificativ comportamentul într-un mod care poate aduce prejudicii psihologice sau fizice acestora sau altor persoane. Alte practici de manipulare sau de exploatare care îi afectează pe adulți și care ar putea fi facilitate de sistemele de IA ar putea fi acoperite de legislația existentă privind protecția datelor, protecția consumatorilor și serviciile digitale, care garantează că persoanele fizice sunt informate în mod corespunzător și că au libertatea de a alege să nu facă obiectul creării de profiluri sau al altor practici care le-ar putea afecta comportamentul. Propunerea interzice, de asemenea, evaluarea comportamentului social prin intermediul sistemelor de IA în scopuri generale de către autoritățile publice. În fine, utilizarea sistemelor de identificare biometrică la distanță „în timp real" în spațiile accesibile publicului în scopul asigurării respectării legii este, de asemenea, interzisă, cu excepția cazului în care se aplică anumite excepții limitate.

5.2.3. SISTEME DE IA CU GRAD RIDICAT DE RISC (TITLUL III)

Titlul III conține norme specifice pentru sistemele de IA care creează un risc ridicat pentru sănătatea și siguranța persoanelor fizice sau pentru drepturile fundamentale ale acestora. În conformitate cu o abordare bazată pe riscuri, aceste sisteme de IA cu grad ridicat de risc sunt permise pe piața europeană sub rezerva respectării anumitor cerințe obligatorii și a unei evaluări *ex ante* a conformității. Clasificarea unui sistem de IA ca prezentând un risc ridicat se bazează pe scopul preconizat al sistemului de IA, în conformitate cu legislația existentă privind siguranța produselor. Prin urmare, clasificarea drept sistem care prezintă un risc ridicat nu depinde numai de funcția îndeplinită de sistemul de IA, ci și de scopul și modalitățile specifice pentru care este utilizat sistemul respectiv.

Capitolul 1 din titlul III stabilește normele de clasificare și identifică două categorii principale de sisteme de IA cu grad ridicat de risc:

- sisteme de IA destinate a fi utilizate drept componente de siguranță ale produselor care fac obiectul unei evaluări *ex ante* a conformității de către terți;
- alte sisteme de IA autonome, cu implicații în principal asupra drepturilor fundamentale, care sunt enumerate în mod explicit în anexa III.

Această listă de sisteme de IA cu grad ridicat de risc din anexa III conține un număr limitat de sisteme de IA ale căror riscuri s-au materializat deja sau sunt susceptibile să se materializeze în viitorul apropiat. Pentru a se asigura că regulamentul poate fi adaptat la noile utilizări și aplicații ale IA, Comisia poate extinde lista sistemelor de IA cu grad ridicat de risc utilizate în anumite domenii predefinite, prin aplicarea unui set de criterii și a unei metodologii de evaluare a riscurilor.

Capitolul 2 stabilește cerințele juridice pentru sistemele de IA cu grad ridicat de risc în ceea ce privește datele, precum și guvernanța datelor, documentația și evidența, transparența și furnizarea de informații către utilizatori, supravegherea umană, robustețea, acuratețea și securitatea. Cerințele minime propuse sunt deja de ultimă generație pentru mulți operatori diligenți și rezultatul a doi ani de activitate pregătitoare, fiind derivate din Orientările în

materie de etică ale HLEG[29], aplicate în proiecte-pilot desfășurate de peste 350 de organizații[30]. Acestea sunt, de asemenea, în mare măsură în concordanță cu alte recomandări și principii internaționale, ceea ce asigură compatibilitatea cadrului propus privind IA cu cele adoptate de partenerii comerciali internaționali ai UE. Soluțiile tehnice precise pentru asigurarea conformității cu cerințele respective pot fi furnizate de standarde sau de alte specificații tehnice sau pot fi dezvoltate în alt mod în conformitate cu cunoștințele tehnice sau științifice generale, la latitudinea furnizorului sistemului de IA. Această flexibilitate este deosebit de importantă, deoarece permite furnizorilor de sisteme de IA să aleagă modalitatea de îndeplinire a cerințelor lor, ținând seama de progresele tehnologice și științifice de ultimă generație din acest domeniu.

Capitolul 3 stabilește un set clar de obligații orizontale pentru furnizorii de sisteme de IA cu grad ridicat de risc. Utilizatorilor și altor participanți din lanțul valoric al IA (de exemplu, importatori, distribuitori, reprezentanți autorizați) li se impun obligații proporționale.

Capitolul 4 stabilește cadrul în care organismele notificate trebuie să fie implicate ca părți terțe independente în procedurile de evaluare a conformității, în timp ce capitolul 5 explică în detaliu procedurile de evaluare a conformității care trebuie urmate pentru fiecare tip de sistem de IA cu grad ridicat de risc. Abordarea privind evaluarea conformității urmărește să reducă la minimum sarcina pentru operatorii economici, precum și pentru organismele notificate, a căror capacitate trebuie să fie extinsă treptat în timp. Sistemele de IA destinate utilizării drept componente de siguranță ale produselor care sunt reglementate în temeiul noului cadru legislativ (de exemplu, echipamente tehnice, jucării, dispozitive medicale etc.) vor face obiectul acelorași mecanisme *ex ante* și *ex post* de asigurare a conformității și de punere în aplicare ale produselor din care fac parte. Principala diferență este că mecanismele *ex ante* și *ex post* vor asigura conformitatea nu numai cu cerințele stabilite de legislația sectorială, ci și cu cerințele stabilite de prezentul regulament.

În ceea ce privește sistemele de IA autonome cu grad ridicat de risc menționate în anexa III, se va institui un nou sistem de asigurare a conformității și de asigurare a respectării legislației. Acesta urmează modelul legislației privind noul cadru legislativ pus în aplicare prin controale interne de către furnizori, cu excepția sistemelor de identificare biometrică la distanță care ar face obiectul evaluării conformității de către terți. O evaluare *ex ante* cuprinzătoare a conformității prin controale interne, combinată cu o aplicare *ex post* solidă, ar putea fi o soluție eficace și rezonabilă pentru sistemele respective, având în vedere faza incipientă a intervenției în materie de reglementare și faptul că sectorul IA este foarte inovator, iar expertiza în materie de audit se acumulează abia acum. O evaluare prin controale interne a sistemelor de IA „autonome” cu risc ridicat ar necesita o conformitate *ex ante* deplină, eficace și documentată corespunzător cu toate cerințele regulamentului, precum și conformitatea cu sisteme solide de gestionare a calității și a riscurilor și o monitorizare ulterioară introducerii pe piață. După ce furnizorul a efectuat evaluarea conformității relevantă, acesta ar trebui să înregistreze sistemele independente de IA cu grad ridicat de risc într-o bază de date a UE care va fi gestionată de Comisie pentru a spori transparența și supravegherea publică și pentru a consolida supravegherea *ex post* de către autoritățile competente. În schimb, din motive de coerență cu legislația existentă privind siguranța produselor, evaluările conformității sistemelor de IA care sunt componente de siguranță ale produselor vor urma un sistem cu proceduri de evaluare a conformității de către terți, deja stabilite în temeiul legislației

[29] Grupul de experți la nivel înalt privind inteligența artificială, *Orientări în materie de etică pentru o inteligență artificială (IA) fiabilă*, 2019.

[30] Acestea au fost, de asemenea, aprobate de Comisie în comunicarea sa din 2019 privind abordarea centrată pe factorul uman a IA.

sectoriale relevante privind siguranța produselor. Vor fi necesare noi reevaluări *ex ante* ale conformității în cazul unor modificări substanțiale ale sistemelor de IA (în special modificări care depășesc ceea ce este stabilit în prealabil de către furnizor în documentația sa tehnică și verificat la momentul evaluării *ex ante* a conformității).

5.2.4. OBLIGAȚII DE TRANSPARENȚĂ PENTRU ANUMITE SISTEME DE IA (TITLUL IV)

Titlul IV vizează anumite sisteme de IA pentru a ține seama de riscurile specifice de manipulare pe care le prezintă acestea. Obligațiile de transparență se vor aplica sistemelor care (i) interacționează cu oamenii, (ii) sunt utilizate pentru a detecta emoțiile sau pentru a determina asocierea cu categorii (sociale) bazate pe date biometrice sau (iii) generează sau manipulează conținut („deepfake-uri”). Atunci când persoanele interacționează cu un sistem de IA sau emoțiile sau caracteristicile lor sunt recunoscute prin mijloace automatizate, persoanele trebuie să fie informate cu privire la circumstanțele respective. În cazul în care un sistem de IA este utilizat pentru a genera sau a manipula imagini, conținuturi audio sau video care seamănă în mod semnificativ cu conținutul autentic, ar trebui să existe obligația de a divulga faptul că respectivul conținut este generat prin mijloace automatizate, sub rezerva unor excepții în scopuri legitime (asigurarea aplicării legislației, libertatea de exprimare). Acest lucru le permite persoanelor să facă alegeri în cunoștință de cauză sau să facă un pas înapoi dintr-o anumită situație.

5.2.5. MĂSURI ÎN SPRIJINUL INOVĂRII (TITLUL V)

Titlul V contribuie la obiectivul de a crea un cadru juridic care să fie favorabil inovării, adaptat exigențelor viitorului și rezistent la perturbări. În acest scop, încurajează autoritățile naționale competente să creeze spații de testare în materie de reglementare și stabilește un cadru de bază în ceea ce privește guvernanța, supravegherea și răspunderea. Spațiile de testare în materie de reglementare a IA creează un mediu controlat pentru testarea tehnologiilor inovatoare pentru o perioadă limitată de timp, pe baza unui plan de testare convenit cu autoritățile competente. Titlul V conține, de asemenea, măsuri de reducere a sarcinii de reglementare ce revine IMM-urilor și întreprinderilor nou-înființate.

5.2.6. GUVERNANȚĂ ȘI PUNERE ÎN APLICARE (TITLURILE VI, VII ȘI VIII)

Titlul VI stabilește sistemele de guvernanță la nivelul Uniunii și la nivel național. La nivelul Uniunii, propunerea instituie un Comitet european pentru inteligența artificială (denumit în continuare „comitetul”), alcătuit din reprezentanți ai statelor membre și ai Comisiei. Comitetul va facilita o punere în aplicare fără probleme, eficace și armonizată a prezentului regulament, contribuind la cooperarea eficace dintre autoritățile naționale de supraveghere și Comisie și furnizând consultanță și expertiză Comisiei. De asemenea, va colecta și va face schimb de bune practici între statele membre.

La nivel național, statele membre vor trebui să desemneze una sau mai multe autorități naționale competente și, printre acestea, autoritatea națională de supraveghere, în scopul supravegherii aplicării și punerii în aplicare a regulamentului. Autoritatea Europeană pentru Protecția Datelor va acționa în calitate de autoritate competentă pentru supravegherea instituțiilor, a agențiilor și a organelor Uniunii atunci când acestea intră în domeniul de aplicare al prezentului regulament.

Titlul VII urmărește să faciliteze activitatea de monitorizare desfășurată de Comisie și de autoritățile naționale prin crearea unei baze de date la nivelul UE pentru sistemele de IA autonome cu grad ridicat de risc, cu implicații în principal asupra drepturilor fundamentale. Baza de date va fi gestionată de Comisie și va fi alimentată cu date de către furnizorii de

sisteme de IA, care vor trebui să își înregistreze sistemele înainte de a le introduce pe piață sau de a le pune în funcțiune în alt mod.

Titlul VIII stabilește obligațiile de monitorizare și raportare pentru furnizorii de sisteme de IA în ceea ce privește monitorizarea și raportarea ulterioară introducerii pe piață, precum și investigarea incidentelor și a disfuncționalităților legate de IA. De asemenea, autoritățile de supraveghere a pieței ar urma să controleze piața și să investigheze respectarea obligațiilor și a cerințelor pentru toate sistemele de IA cu grad ridicat de risc deja introduse pe piață. Autoritățile de supraveghere a pieței ar urma să aibă toate competențele în temeiul Regulamentului (UE) 2019/1020 privind supravegherea pieței. Aplicarea *ex post* ar trebui să garanteze că, odată ce sistemul de IA a fost introdus pe piață, autoritățile publice au competențele și resursele necesare să intervină în cazul în care sistemele de IA generează riscuri neprevăzute care justifică o acțiune rapidă. Acestea vor monitoriza, de asemenea, respectarea de către operatori a obligațiilor care le revin în temeiul regulamentului. Propunerea nu prevede crearea automată a unor organisme sau autorități suplimentare la nivelul statelor membre. Prin urmare, statele membre pot numi autorități sectoriale existente (putând utiliza expertiza acestora), cărora li s-ar încredința, de asemenea, competența de a monitoriza și de a asigura respectarea dispozițiilor regulamentului.

Toate acestea nu aduc atingere sistemului existent și repartizării competențelor de aplicare *ex post* a obligațiilor privind drepturile fundamentale în statele membre. Atunci când acest lucru este necesar pentru îndeplinirea mandatului lor, autoritățile de supraveghere și de asigurare a conformității existente vor avea, de asemenea, competența de a solicita și de a accesa orice documentație păstrată în conformitate cu prezentul regulament și, dacă este necesar, de a solicita autorităților de supraveghere a pieței să organizeze testarea sistemului de IA cu grad ridicat de risc prin mijloace tehnice.

5.2.7. CODURI DE CONDUITĂ (TITLUL IX)

Titlul IX instituie un cadru pentru crearea de coduri de conduită, al căror scop este de a încuraja furnizorii de sisteme de IA care nu prezintă un grad ridicat de risc să aplice în mod voluntar cerințele obligatorii pentru sistemele de IA cu grad ridicat de risc (astfel cum se prevede în titlul III). Furnizorii de sisteme IA care nu prezintă un grad ridicat de risc pot crea și pune ei înșiși în aplicare codurile de conduită. Aceste coduri pot include, de asemenea, angajamente voluntare legate, de exemplu, de durabilitatea mediului, accesibilitatea pentru persoanele cu handicap, participarea părților interesate la proiectarea și dezvoltarea sistemelor de IA și diversitatea echipelor de dezvoltare.

5.2.8. DISPOZIȚII FINALE (TITLURILE X, XI ȘI XII)

Titlul X subliniază obligația tuturor părților de a respecta confidențialitatea informațiilor și a datelor și stabilește norme pentru schimbul de informații obținute în cursul punerii în aplicare a regulamentului. Titlul X include, de asemenea, măsuri de asigurare a punerii în aplicare cu eficacitate a regulamentului prin sancțiuni eficace, proporționale și disuasive pentru încălcarea dispozițiilor.

Titlul XI stabilește norme pentru exercitarea competențelor delegate și de executare. Propunerea împuternicește Comisia să adopte, după caz, acte de punere în aplicare pentru a asigura aplicarea uniformă a regulamentului sau acte delegate pentru actualizarea sau completarea listelor din anexele I-VII.

Titlul XII prevede obligația Comisiei de a evalua periodic necesitatea unei actualizări a anexei III și de a întocmi rapoarte periodice privind evaluarea și revizuirea regulamentului. Acesta prevede, de asemenea, dispoziții finale, inclusiv o perioadă de tranziție diferențiată

pentru data inițială de aplicabilitate a regulamentului, pentru a facilita punerea în aplicare fără probleme pentru toate părțile implicate.

2021/0106 (COD)

Propunere de

REGULAMENT AL PARLAMENTULUI EUROPEAN ȘI AL CONSILIULUI

DE STABILIRE A UNOR NORME ARMONIZATE PRIVIND INTELIGENȚA ARTIFICIALĂ (LEGEA PRIVIND INTELIGENȚA ARTIFICIALĂ) ȘI DE MODIFICARE A ANUMITOR ACTE LEGISLATIVE ALE UNIUNII

PARLAMENTUL EUROPEAN ȘI CONSILIUL UNIUNII EUROPENE,

având în vedere Tratatul privind funcționarea Uniunii Europene, în special articolele 16 și 114,

având în vedere propunerea Comisiei Europene,

după transmiterea proiectului de act legislativ parlamentelor naționale,

având în vedere avizul Comitetului Economic și Social European[31],

având în vedere avizul Comitetului Regiunilor[32],

hotărând în conformitate cu procedura legislativă ordinară,

întrucât:

(1) Scopul prezentului regulament este de a îmbunătăți funcționarea pieței interne prin stabilirea unui cadru juridic uniform, în special pentru dezvoltarea, comercializarea și utilizarea inteligenței artificiale, în conformitate cu valorile Uniunii. Prezentul regulament urmărește o serie de motive imperative de interes public major, cum ar fi un nivel ridicat de protecție a sănătății, a siguranței și a drepturilor fundamentale, și asigură libera circulație transfrontalieră a bunurilor și serviciilor bazate pe IA, împiedicând astfel statele membre să impună restricții privind dezvoltarea, comercializarea și utilizarea sistemelor de IA, cu excepția cazului în care acest lucru este autorizat în mod explicit de prezentul regulament.

(2) Sistemele de inteligență artificială (sistemele de IA) pot fi implementate cu ușurință în mai multe sectoare ale economiei și societății, inclusiv la nivel transfrontalier, și pot circula în întreaga Uniune. Anumite state membre au explorat deja adoptarea unor norme naționale pentru a se asigura că inteligența artificială este sigură și că este dezvoltată și utilizată în conformitate cu obligațiile în materie de drepturi fundamentale. Normele naționale diferite pot duce la fragmentarea pieței interne și pot reduce gradul de securitate juridică pentru operatorii care dezvoltă sau utilizează sisteme de IA. Prin urmare, ar trebui să se asigure un nivel ridicat și consecvent de protecție în întreaga Uniune, iar divergențele care împiedică libera circulație a sistemelor de IA și a produselor și serviciilor conexe în cadrul pieței interne ar trebui prevenite, prin stabilirea unor obligații uniforme pentru operatori și prin garantarea protecției uniforme a motivelor imperative de interes public major și a drepturilor persoanelor în întreaga piață internă, în temeiul articolului 114 din Tratatul privind

[31] JO C […], […], p. […].
[32] JO C […], […], p. […].

funcționarea Uniunii Europene (TFUE). În măsura în care prezentul regulament conține norme specifice privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal referitoare la restricțiile de utilizare a sistemelor de IA pentru identificarea biometrică la distanță „în timp real” în spațiile accesibile publicului în scopul asigurării respectării legii, este oportun ca prezentul regulament să se întemeieze, în ceea ce privește normele specifice respective, pe articolul 16 din TFUE. Având în vedere aceste norme specifice și recurgerea la articolul 16 din TFUE, este oportun să se consulte Comitetul european pentru protecția datelor.

(3) Inteligența artificială este o familie de tehnologii cu evoluție rapidă, care poate genera o gamă largă de beneficii economice și societale în întregul spectru de industrii și activități sociale. Prin îmbunătățirea previziunilor, optimizarea operațiunilor și a alocării resurselor, precum și prin personalizarea soluțiilor digitale disponibile pentru persoane și organizații, utilizarea inteligenței artificiale poate oferi avantaje concurențiale esențiale întreprinderilor și poate sprijini obținerea de rezultate benefice din punct de vedere social și ecologic, de exemplu în domeniul asistenței medicale, al agriculturii, al educației și formării, al gestionării infrastructurii, al energiei, al transporturilor și logisticii, al serviciilor publice, al securității, justiției, eficienței resurselor și energiei, precum și al atenuării schimbărilor climatice și al adaptării la acestea.

(4) În același timp, în funcție de circumstanțele legate de aplicarea și utilizarea sa specifică, inteligența artificială poate genera riscuri și poate aduce prejudicii intereselor publice și drepturilor care sunt protejate de dreptul Uniunii. Un astfel de prejudiciu ar putea fi material sau moral.

(5) Prin urmare, este necesar un cadru juridic al Uniunii care să stabilească norme armonizate privind inteligența artificială pentru a încuraja dezvoltarea, utilizarea și adoptarea inteligenței artificiale pe piața internă și care să asigure, în același timp, un nivel ridicat de protecție a intereselor publice, cum ar fi sănătatea, siguranța și protecția drepturilor fundamentale, astfel cum sunt recunoscute și protejate de dreptul Uniunii. Pentru atingerea acestui obiectiv, ar trebui stabilite norme care să reglementeze introducerea pe piață și punerea în funcțiune a anumitor sisteme de IA, asigurând astfel buna funcționare a pieței interne și permițând acestor sisteme să beneficieze de principiul liberei circulații a bunurilor și serviciilor. Prin stabilirea acestor norme, prezentul regulament sprijină obiectivul Uniunii de a se poziționa ca lider mondial în dezvoltarea unei inteligențe artificiale sigure, de încredere și etice, astfel cum a afirmat Consiliul European[33], și asigură protecția principiilor etice, astfel cum a solicitat în mod expres Parlamentul European[34].

(6) Noțiunea de sistem de IA ar trebui definită în mod clar pentru a asigura securitatea juridică, oferind, în același timp, flexibilitatea necesară pentru a ține seama de evoluțiile tehnologice viitoare. Definiția ar trebui să se bazeze pe caracteristicile funcționale esențiale ale software-ului, în special pe capacitatea, pentru un anumit set de obiective definite de om, de a genera rezultate cum ar fi conținutul, previziunile, recomandările sau deciziile care influențează mediul cu care interacționează sistemul,

---

33 Consiliul European, Reuniunea extraordinară a Consiliului European (1-2 octombrie 2020) – Concluzii, EUCO 13/20, 2020, p. 6.

34 Rezoluția Parlamentului European din 20 octombrie 2020 conținând recomandări adresate Comisiei privind cadrul de aspecte etice asociate cu inteligența artificială, robotica și tehnologiile conexe, 2020/2012 (INL).

fie că este vorba de o dimensiune fizică, fie de una digitală. Sistemele de IA pot fi proiectate pentru a funcționa cu diferite niveluri de autonomie și pot fi utilizate în mod independent sau ca o componentă a unui produs, indiferent dacă sistemul este integrat fizic în produs (încorporat) sau dacă servește funcționalității produsului fără a fi integrat în acesta (neîncorporat). Definiția sistemului de IA ar trebui să fie completată de o listă de tehnici și abordări specifice utilizate pentru dezvoltarea sa, care ar trebui să fie actualizată în lumina evoluțiilor tehnologice și ale pieței prin adoptarea de acte delegate de către Comisie pentru modificarea listei respective.

(7) Noțiunea de date biometrice utilizată în prezentul regulament este în concordanță cu noțiunea de date biometrice astfel cum este definită la articolul 4 alineatul (14) din Regulamentul (UE) 2016/679 al Parlamentului European și al Consiliului[35], la articolul 3 alineatul (18) din Regulamentul (UE) 2018/1725 al Parlamentului European și al Consiliului[36] și la articolul 3 alineatul (13) din Directiva (UE) 2016/680 a Parlamentului European și a Consiliului[37] și ar trebui interpretată în concordanță cu aceasta.

(8) Noțiunea de sistem de identificare biometrică la distanță, astfel cum este utilizată în prezentul regulament, ar trebui definită din punct de vedere funcțional ca fiind un sistem de IA destinat identificării persoanelor fizice la distanță prin compararea datelor biometrice ale unei persoane cu datele biometrice conținute într-o bază de date de referință și fără a se cunoaște în prealabil dacă persoana vizată va fi prezentă și dacă poate fi identificată, indiferent de tehnologia, procesele sau tipurile specifice de date biometrice utilizate. Având în vedere diferitele caracteristici și moduri în care sunt utilizate, precum și diferitele riscuri implicate, ar trebui să se facă o distincție între sistemele de identificare biometrică la distanță „în timp real” și „ulterior”. În cazul sistemelor „în timp real”, captarea datelor biometrice, compararea și identificarea se efectuează instantaneu, aproape instantaneu sau, în orice caz, fără întârzieri semnificative. În acest sens, nu ar trebui să existe posibilități de eludare a normelor prezentului regulament privind utilizarea „în timp real” a sistemelor de IA în cauză prin prevederea unor întârzieri minore. Sistemele „în timp real” implică utilizarea de materiale „în direct” sau „aproape în direct”, cum ar fi înregistrări video, generate de o cameră video sau de un alt dispozitiv cu funcționalitate similară. În schimb, în cazul sistemelor de identificare „ulterioară”, datele biometrice au fost deja captate, iar compararea și identificarea au loc numai după o întârziere semnificativă. Este vorba despre materiale, cum ar fi imagini sau înregistrări video generate de camere de televiziune cu circuit închis sau de dispozitive private, care au fost generate înainte de utilizarea sistemului în legătură cu persoanele fizice în cauză.

---

35 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).

36 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).

37 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 (Directiva privind protecția datelor în materie de asigurare a respectării legii) (JO L 119, 4.5.2016, p. 89).

(9) În sensul prezentului regulament, noțiunea de spațiu accesibil publicului ar trebui înțeleasă ca referindu-se la orice loc fizic accesibil publicului, indiferent dacă locul în cauză este proprietate privată sau publică. Prin urmare, noțiunea nu acoperă locurile care sunt private în esență și care, în mod normal, nu sunt accesibile în mod liber terților, inclusiv autorităților de aplicare a legii, cu excepția cazului în care părțile respective au fost invitate sau autorizate în mod specific, cum ar fi locuințele, cluburile private, birourile, depozitele și fabricile. Spațiile online nu sunt nici ele acoperite, deoarece nu sunt spații fizice. Cu toate acestea, simplul fapt că se pot aplica anumite condiții pentru accesarea unui anumit spațiu, cum ar fi biletele de intrare sau restricțiile de vârstă, nu înseamnă că spațiul nu este accesibil publicului în sensul prezentului regulament. Prin urmare, pe lângă spațiile publice, cum ar fi străzile, părțile relevante ale clădirilor guvernamentale și cea mai mare parte a infrastructurii de transport, spațiile precum cinematografele, teatrele, magazinele și centrele comerciale sunt, de asemenea, accesibile publicului în mod normal. Cu toate acestea, ar trebui să se stabilească de la caz la caz dacă un anumit spațiu este accesibil publicului, având în vedere particularitățile situației individuale în cauză.

(10) Pentru a asigura condiții de concurență echitabile și o protecție eficace a drepturilor și libertăților persoanelor fizice în întreaga Uniune, normele stabilite prin prezentul regulament ar trebui să se aplice în mod nediscriminatoriu furnizorilor de sisteme de IA, indiferent dacă sunt stabiliți în Uniune sau într-o țară terță, precum și utilizatorilor de sisteme de IA stabiliți în Uniune.

(11) Având în vedere natura lor digitală, anumite sisteme de IA ar trebui să intre în domeniul de aplicare al prezentului regulament chiar și atunci când nu sunt introduse pe piață, nu sunt puse în funcțiune și nu sunt utilizate în Uniune. Acesta este cazul, de exemplu, al unui operator stabilit în Uniune care contractează anumite servicii unui operator stabilit în afara Uniunii în legătură cu o activitate care urmează să fie desfășurată de un sistem de IA care s-ar califica drept sistem cu risc ridicat și ale cărei efecte ar avea un impact asupra persoanelor fizice situate în Uniune. În aceste circumstanțe, sistemul de IA utilizat de operatorul din afara Uniunii ar putea prelucra datele colectate în mod legal în Uniune și transferate din Uniune și ar putea furniza operatorului contractant din Uniune rezultatele produse de sistemul de IA respectiv ca urmare a prelucrării respective, fără ca respectivul sistem de IA să fie introdus pe piață, pus în funcțiune sau utilizat în Uniune. Pentru a preveni eludarea prezentului regulament și pentru a asigura o protecție eficace a persoanelor fizice situate în Uniune, prezentul regulament ar trebui să se aplice, de asemenea, furnizorilor și utilizatorilor de sisteme de IA care sunt stabiliți într-o țară terță, în măsura în care producția realizată de sistemele respective este utilizată în Uniune. Cu toate acestea, pentru a ține seama de acordurile existente și de nevoile speciale de cooperare cu partenerii străini cu care se fac schimburi de informații și probe, prezentul regulament nu ar trebui să se aplice autorităților publice ale unei țări terțe și organizațiilor internaționale atunci când acționează în cadrul acordurilor internaționale încheiate la nivel național sau european pentru asigurarea respectării legii și în contextul cooperării judiciare cu Uniunea sau cu statele sale membre. Astfel de acorduri au fost încheiate bilateral între statele membre și țările terțe sau între Uniunea Europeană, Europol și alte agenții ale UE și țări terțe și organizații internaționale.

(12) Prezentul regulament ar trebui să se aplice, de asemenea, instituțiilor, oficiilor, organelor și agențiilor Uniunii atunci când acționează în calitate de furnizor sau utilizator al unui sistem de IA. Sistemele de IA dezvoltate sau utilizate exclusiv în scopuri militare ar trebui excluse din domeniul de aplicare al prezentului regulament în

cazul în care utilizarea respectivă intră în sfera de competență exclusivă a politicii externe și de securitate comune, reglementată în temeiul titlului V din Tratatul privind Uniunea Europeană (TUE). Prezentul regulament nu ar trebui să aducă atingere dispozițiilor privind răspunderea furnizorilor de servicii intermediari prevăzute în Directiva 2000/31/CE a Parlamentului European și a Consiliului [astfel cum a fost modificată prin Actul legislativ privind serviciile digitale].

(13) Pentru a asigura un nivel consecvent și ridicat de protecție a intereselor publice în ceea ce privește sănătatea, siguranța și drepturile fundamentale, ar trebui stabilite standarde normative comune pentru toate sistemele de IA cu grad ridicat de risc. Aceste standarde ar trebui să fie în concordanță cu Carta drepturilor fundamentale a Uniunii Europene („Carta") și ar trebui să fie nediscriminatorii și în conformitate cu angajamentele comerciale internaționale ale Uniunii.

(14) Pentru a introduce un set proporțional și eficace de norme obligatorii pentru sistemele de IA, ar trebui urmată o abordare bazată pe riscuri clar definită. Această abordare ar trebui să adapteze tipul și conținutul unor astfel de norme la intensitatea și amploarea riscurilor pe care le pot genera sistemele de IA. Prin urmare, este necesar să se interzică anumite practici în domeniul inteligenței artificiale, să se stabilească cerințe pentru sistemele de IA cu grad ridicat de risc și obligații pentru operatorii relevanți și să se stabilească obligații în materie de transparență pentru anumite sisteme de IA.

(15) Pe lângă numeroasele utilizări benefice ale inteligenței artificiale, această tehnologie poate fi utilizată în mod abuziv și poate oferi instrumente noi și puternice pentru practici de manipulare, exploatare și control social. Astfel de practici sunt deosebit de nocive și ar trebui interzise deoarece contravin valorilor Uniunii privind respectarea demnității umane, a libertății, a egalității, a democrației și a statului de drept, precum și a drepturilor fundamentale ale Uniunii, inclusiv a dreptului la nediscriminare, a protecției datelor și a vieții private, precum și a drepturilor copilului.

(16) Ar trebui interzisă introducerea pe piață, punerea în funcțiune sau utilizarea anumitor sisteme de IA destinate să denatureze comportamentul uman, în cazul cărora este probabil să se aducă prejudicii fizice sau psihice. Astfel de sisteme de IA implementează componente subliminale pe care persoanele nu le pot percepe sau exploatează vulnerabilitățile copiilor și ale oamenilor ca urmare a vârstei și incapacității fizice sau mentale a acestora. Ele fac acest lucru cu intenția de a denatura în mod semnificativ comportamentul unei persoane și într-un mod care cauzează sau ar putea cauza prejudicii persoanei respective sau unei alte persoane. Intenția nu poate fi prezumată în cazul în care denaturarea comportamentului uman rezultă din factori externi sistemului de IA, care se află în afara controlului furnizorului sau al utilizatorului. Cercetarea în scopuri legitime în legătură cu astfel de sisteme de IA nu ar trebui să fie împiedicată de interdicție, în cazul în care o astfel de cercetare nu echivalează cu utilizarea sistemului de IA în relațiile om-mașină, provocând prejudicii persoanelor fizice, iar o astfel de cercetare se desfășoară în conformitate cu standardele etice recunoscute pentru cercetarea științifică.

(17) Sistemele de IA care oferă o evaluare a comportamentului social al persoanelor fizice în scopuri generale de către autoritățile publice sau în numele acestora pot genera rezultate discriminatorii și excluderea anumitor grupuri. Acestea pot încălca dreptul la demnitate și nediscriminare, precum și valorile egalității și justiției. Astfel de sisteme de IA evaluează sau clasifică credibilitatea persoanelor fizice pe baza comportamentului lor social în contexte multiple sau a unor caracteristici personale sau de personalitate cunoscute sau preconizate. Punctajul privind comportamentul

social obținut din astfel de sisteme de IA poate duce la un tratament negativ sau nefavorabil al persoanelor fizice sau al unor grupuri întregi de astfel de persoane în contexte sociale care nu au legătură cu contextul în care datele au fost inițial generate sau colectate sau la un tratament defavorabil care este disproporționat sau nejustificat în raport cu gravitatea comportamentului lor social. Prin urmare, astfel de sisteme de IA ar trebui interzise.

(18) Utilizarea sistemelor de IA pentru identificarea biometrică „în timp real" a persoanelor fizice în spațiile accesibile publicului în scopul asigurării respectării legii este considerată deosebit de intruzivă pentru drepturile și libertățile persoanelor în cauză, în măsura în care poate afecta viața privată a unei părți mari a populației, evocă un sentiment de supraveghere constantă și descurajează indirect exercitarea libertății de întrunire și a altor drepturi fundamentale. În plus, caracterul imediat al impactului și posibilitățile limitate de a efectua verificări sau corecții suplimentare în ceea ce privește utilizarea unor astfel de sisteme care funcționează în timp real implică riscuri sporite pentru drepturile și libertățile persoanelor vizate de activitățile de asigurare a respectării legii.

(19) Prin urmare, utilizarea acestor sisteme în scopul asigurării respectării legii ar trebui interzisă, cu excepția a trei situații enumerate în mod exhaustiv și definite în mod strict, în care utilizarea este strict necesară pentru un interes public substanțial, importanța acestei utilizări fiind mai mare decât riscurile. Aceste situații implică căutarea potențialelor victime ale criminalității, inclusiv a copiilor dispăruți, anumite amenințări la adresa vieții sau a siguranței fizice a persoanelor fizice sau privind un atac terorist și detectarea, localizarea, identificarea sau urmărirea penală a autorilor unor infracțiuni sau a persoanelor suspectate menționate în Decizia-cadru 2002/584/JAI a Consiliului[38], în cazul în care infracțiunile respective se pedepsesc în statul membru în cauză cu o pedeapsă sau o măsură de siguranță privativă de libertate pentru o perioadă maximă de cel puțin trei ani și conform definiției din dreptul statului membru respectiv. Un astfel de prag pentru pedeapsa sau măsura de siguranță privativă de libertate în conformitate cu dreptul intern contribuie la asigurarea faptului că infracțiunea ar trebui să fie suficient de gravă pentru a justifica eventual utilizarea sistemelor de identificare biometrică la distanță „în timp real". În plus, dintre cele 32 de infracțiuni enumerate în Decizia-cadru 2002/584/JAI a Consiliului, unele sunt, în practică, susceptibile să fie mai relevante decât altele, în sensul că recurgerea la identificarea biometrică la distanță „în timp real" va fi, în mod previzibil, necesară și proporțională în grade foarte diferite pentru urmărirea practică a detectării, localizării, identificării sau urmăririi penale a unui autor al unei infracțiuni sau a unei persoane suspectate că ar fi comis diferitele infracțiuni enumerate și având în vedere diferențele probabile în ceea ce privește gravitatea, probabilitatea și amploarea prejudiciului sau posibilele consecințe negative.

(20) Pentru a se asigura că aceste sisteme sunt utilizate în mod responsabil și proporțional, este de asemenea important să se stabilească faptul că, în fiecare dintre aceste trei situații enumerate în mod exhaustiv și strict definite, ar trebui luate în considerare anumite elemente, în special în ceea ce privește natura situației care a stat la baza cererii și consecințele utilizării asupra drepturilor și libertăților tuturor persoanelor vizate, precum și garanțiile și condițiile prevăzute pentru utilizare. În plus, utilizarea sistemelor de identificare biometrică la distanță „în timp real" în spațiile accesibile

[38] Decizia-cadru 2002/584/JAI a Consiliului din 13 iunie 2002 privind mandatul european de arestare și procedurile de predare între statele membre (JO L 190, 18.7.2002, p. 1).

publicului în scopul asigurării respectării legii ar trebui să facă obiectul unor limite de timp și spațiu adecvate, având în vedere, în special, dovezile sau indicațiile privind amenințările, victimele sau autorul infracțiunii. Baza de date de referință a persoanelor ar trebui să fie adecvată pentru fiecare caz de utilizare în fiecare dintre cele trei situații menționate mai sus.

(21) Fiecare utilizare a unui sistem de identificare biometrică la distanță „în timp real" în spațiile accesibile publicului în scopul asigurării respectării legii ar trebui să facă obiectul unei autorizări exprese și specifice de către o autoritate judiciară sau o autoritate administrativă independentă a unui stat membru. O astfel de autorizație ar trebui, în principiu, să fie obținută înainte de utilizare, cu excepția situațiilor de urgență justificate în mod corespunzător, și anume situațiile în care necesitatea de a utiliza sistemele în cauză este de așa natură încât obținerea unei autorizații înainte de începerea utilizării este imposibilă din punctul de vedere al eficacității și în mod obiectiv. În astfel de situații de urgență, utilizarea ar trebui să fie limitată la ceea ce este minim și absolut necesar și să facă obiectul unor garanții și condiții adecvate, astfel cum sunt stabilite în dreptul intern și specificate în contextul fiecărui caz individual de utilizare urgentă de către însăși autoritatea de aplicare a legii. În plus, în astfel de situații, autoritatea de aplicare a legii ar trebui să încerce să obțină o autorizație cât mai curând posibil, indicând motivele pentru care nu a fost în măsură să o solicite mai devreme.

(22) În plus, este oportun să se prevadă, în cadrul exhaustiv stabilit de prezentul regulament, că o astfel de utilizare pe teritoriul unui stat membru în conformitate cu prezentul regulament ar trebui să fie posibilă numai în cazul și în măsura în care statul membru în cauză a decis să prevadă în mod expres posibilitatea de a autoriza o astfel de utilizare în normele sale detaliate de drept intern. În consecință, în temeiul prezentului regulament, statele membre au în continuare libertatea de a nu prevedea o astfel de posibilitate sau de a prevedea o astfel de posibilitate numai în ceea ce privește unele dintre obiectivele care pot justifica utilizarea autorizată identificate în prezentul regulament.

(23) Utilizarea sistemelor de IA pentru identificarea biometrică „în timp real" a persoanelor fizice în spațiile accesibile publicului în scopul asigurării respectării legii implică în mod necesar prelucrarea datelor biometrice. Normele din prezentul regulament care interzic, sub rezerva anumitor excepții, o astfel de utilizare, care se bazează pe articolul 16 din TFUE, ar trebui să se aplice ca *lex specialis* în ceea ce privește normele privind prelucrarea datelor biometrice prevăzute la articolul 10 din Directiva (UE) 2016/680, reglementând astfel în mod exhaustiv această utilizare și prelucrarea datelor biometrice implicate. Prin urmare, o astfel de utilizare și prelucrare ar trebui să fie posibilă numai în măsura în care este compatibilă cu cadrul stabilit de prezentul regulament, fără a exista, în afara cadrului respectiv, posibilitatea ca autoritățile competente, atunci când acționează în scopul asigurării respectării legii, să utilizeze astfel de sisteme și să prelucreze astfel de date în legătură cu acestea din motivele enumerate la articolul 10 din Directiva (UE) 2016/680. În acest context, prezentul regulament nu este menit să ofere temeiul juridic pentru prelucrarea datelor cu caracter personal în baza articolului 8 din Directiva 2016/680. Cu toate acestea, utilizarea sistemelor de identificare biometrică la distanță „în timp real" în spații accesibile publicului în alte scopuri decât cele de asigurare a respectării legii, inclusiv de către autoritățile competente, nu ar trebui să facă obiectul cadrului specific privind o astfel de utilizare în scopul asigurării respectării legii stabilit de prezentul regulament. Prin urmare, o astfel de utilizare în alte scopuri decât asigurarea

respectării legii nu ar trebui să facă obiectul cerinței unei autorizații în temeiul prezentului regulament și al normelor detaliate aplicabile din dreptul intern care o pot pune în aplicare.

(24) Orice prelucrare a datelor biometrice și a altor date cu caracter personal implicate în utilizarea sistemelor de IA pentru identificarea biometrică, alta decât în legătură cu utilizarea sistemelor de identificare biometrică la distanță „în timp real" în spații accesibile publicului în scopul asigurării respectării legii, astfel cum este reglementat de prezentul regulament, inclusiv în cazul în care aceste sisteme sunt utilizate de autoritățile competente în spații accesibile publicului în alte scopuri decât asigurarea respectării legii, ar trebui să respecte în continuare toate cerințele care decurg din articolul 9 alineatul (1) din Regulamentul (UE) 2016/679, articolul 10 alineatul (1) din Regulamentul (UE) 2018/1725 și articolul 10 din Directiva (UE) 2016/680, după caz.

(25) În conformitate cu articolul 6a din Protocolul nr. 21 privind poziția Regatului Unit și a Irlandei în ceea ce privește spațiul de libertate, securitate și justiție, anexat la TUE și la TFUE, Irlandei nu îi revin obligații în temeiul normelor prevăzute la articolul 5 alineatul (1) litera (d) și la articolul 5 alineatele (2) și (3) din prezentul regulament, adoptate în temeiul articolului 16 din TFUE referitoare la prelucrarea datelor cu caracter personal de către statele membre în exercitarea activităților care intră în domeniul de aplicare al părții a treia titlul V capitolul 4 sau 5 din TFUE, atât timp cât Irlandei nu îi revin obligații în temeiul normelor privind formele de cooperare judiciară în materie penală sau de cooperare polițienească care necesită respectarea dispozițiilor stabilite în temeiul articolului 16 din TFUE.

(26) În conformitate cu articolele 2 și 2a din Protocolul nr. 22 privind poziția Danemarcei, anexat la TUE și la TFUE, Danemarcei nu îi revin obligații în temeiul normelor prevăzute la articolul 5 alineatul (1) litera (d) și la articolul 5 alineatele (2) și (3) din prezentul regulament, adoptate în temeiul articolului 16 din TFUE, și nici nu face obiectul aplicării acestora în ceea ce privește prelucrarea datelor cu caracter personal de către statele membre în exercitarea activităților care intră sub incidența părții a treia titlul V capitolul 4 sau 5 din TFUE.

(27) Sistemele de IA cu grad ridicat de risc ar trebui introduse pe piața Uniunii sau puse în funcțiune numai dacă respectă anumite cerințe obligatorii. Aceste cerințe ar trebui să asigure faptul că sistemele de IA cu grad ridicat de risc disponibile în Uniune sau ale căror rezultate sunt utilizate în alt mod în Uniune nu prezintă riscuri inacceptabile pentru interesele publice importante ale Uniunii, astfel cum sunt recunoscute și protejate de dreptul Uniunii. Sistemele de IA identificate ca prezentând un grad ridicat de risc ar trebui să se limiteze la cele care au un impact negativ semnificativ asupra sănătății, siguranței și drepturilor fundamentale ale persoanelor din Uniune, iar o astfel de limitare reduce la minimum orice eventuală restricționare a comerțului internațional, dacă este cazul.

(28) Sistemele de IA ar putea avea efecte adverse asupra sănătății și siguranței persoanelor, în special atunci când ele funcționează drept componente ale produselor. În concordanță cu obiectivele legislației de armonizare a Uniunii de a facilita libera circulație a produselor pe piața internă și de a asigura că numai produsele sigure și conforme în toate privințele își găsesc drumul pe piață, este important ca riscurile în materie de siguranță care pot fi generate de un produs în ansamblu din cauza componentelor sale digitale, inclusiv a sistemelor de IA, să fie prevenite și atenuate în mod corespunzător. De exemplu, roboții din ce în ce mai autonomi, fie în contextul producției, fie în contextul asistenței și îngrijirii personale, ar trebui să fie în măsură să

își desfășoare activitatea în condiții de siguranță și să își îndeplinească funcțiile în medii complexe. În mod similar, în sectorul sănătății, unde mizele privind viața și sănătatea sunt deosebit de ridicate, sistemele de diagnosticare din ce în ce mai sofisticate și sistemele care sprijină deciziile umane ar trebui să fie fiabile și exacte. Amploarea impactului negativ al sistemului de IA asupra drepturilor fundamentale protejate de Cartă este deosebit de relevantă atunci când un sistem de IA este clasificat ca prezentând un risc ridicat. Printre aceste drepturi se numără dreptul la demnitate umană, respectarea vieții private și de familie, protecția datelor cu caracter personal, libertatea de exprimare și de informare, libertatea de întrunire și de asociere, precum și nediscriminarea, protecția consumatorilor, drepturile lucrătorilor, drepturile persoanelor cu handicap, dreptul la o cale de atac eficientă și la un proces echitabil, dreptul la apărare și prezumția de nevinovăție, dreptul la o bună administrare. Pe lângă aceste drepturi, este important să se sublinieze că, în ceea ce privește copiii, aceștia au drepturi specifice, astfel cum sunt consacrate la articolul 24 din Carta UE și în Convenția Organizației Națiunilor Unite cu privire la drepturile copilului (dezvoltată în continuare în Comentariul general nr. 25 al CDC privind mediul digital), ambele necesitând luarea în considerare a vulnerabilităților copiilor și asigurarea protecției și îngrijirii necesare pentru bunăstarea lor. Dreptul fundamental la un nivel ridicat de protecție a mediului consacrat în Cartă și pus în aplicare în politicile Uniunii ar trebui, de asemenea, luat în considerare atunci când se evaluează gravitatea prejudiciului pe care un sistem de IA îl poate cauza, inclusiv în ceea ce privește sănătatea și siguranța persoanelor.

(29) În ceea ce privește sistemele de IA cu grad ridicat de risc care sunt componente de siguranță ale produselor sau sistemelor sau care sunt ele însele produse sau sisteme care intră în domeniul de aplicare al Regulamentului (CE) nr. 300/2008 al Parlamentului European și al Consiliului[39], al Regulamentului (UE) nr. 167/2013 al Parlamentului European și al Consiliului[40], al Regulamentului (UE) nr. 168/2013 al Parlamentului European și al Consiliului[41], al Directivei (UE) 2014/90/UE a Parlamentului European și a Consiliului[42], al Directivei (UE) 2016/797 a Parlamentului European și a Consiliului[43], al Regulamentului (UE) 2018/858 al Parlamentului European și al Consiliului[44], al Regulamentului (UE) 2018/1139 al

[39] Regulamentul (CE) nr. 300/2008 al Parlamentului European și al Consiliului din 11 martie 2008 privind norme comune în domeniul securității aviației civile și de abrogare a Regulamentului (CE) nr. 2320/2002 (JO L 97, 9.4.2008, p. 72).

[40] Regulamentul (UE) nr. 167/2013 al Parlamentului European și al Consiliului din 5 februarie 2013 privind omologarea și supravegherea pieței pentru vehiculele agricole și forestiere (JO L 60, 2.3.2013, p. 1).

[41] Regulamentul (UE) nr. 168/2013 al Parlamentului European și al Consiliului din 15 ianuarie 2013 privind omologarea și supravegherea pieței pentru vehiculele cu două sau trei roți și pentru cvadricicluri (JO L 60, 2.3.2013, p. 52).

[42] Directiva 2014/90/UE a Parlamentului European și a Consiliului din 23 iulie 2014 privind echipamentele maritime și de abrogare a Directivei 96/98/CE a Consiliului (JO L 257, 28.8.2014, p. 146).

[43] Directiva (UE) 2016/797 a Parlamentului European și a Consiliului din 11 mai 2016 privind interoperabilitatea sistemului feroviar în Uniunea Europeană (JO L 138, 26.5.2016, p. 44).

[44] Regulamentul (UE) 2018/858 al Parlamentului European și al Consiliului din 30 mai 2018 privind omologarea și supravegherea pieței autovehiculelor și remorcilor acestora, precum și ale sistemelor, componentelor și unităților tehnice separate destinate vehiculelor respective, de modificare a Regulamentelor (CE) nr. 715/2007 și (CE) nr. 595/2009 și de abrogare a Directivei 2007/46/CE (JO L 151, 14.6.2018, p. 1).

Parlamentului European și al Consiliului[45] și al Regulamentului (UE) 2019/2144 al Parlamentului European și al Consiliului[46], este oportun să se modifice aceste acte legislative pentru a se asigura că Comisia ia în considerare, pe baza specificităților tehnice și de reglementare ale fiecărui sector, și fără a afecta mecanismele existente de guvernanță, de evaluare a conformității și de aplicare și autoritățile stabilite în acestea, cerințele obligatorii pentru sistemele de IA cu risc ridicat stabilite în prezentul regulament atunci când adoptă orice act relevant viitor delegat sau de punere în aplicare pe baza acestor acte legislative.

(30) În ceea ce privește sistemele de IA care sunt componente de siguranță ale produselor care intră în domeniul de aplicare al anumitor acte legislative de armonizare ale Uniunii, sau care sunt ele însele astfel de produse, este oportun ca acestea să fie clasificate ca având un grad ridicat de risc în temeiul prezentului regulament, în cazul în care produsul în cauză este supus procedurii de evaluare a conformității efectuate de un organism terț de evaluare a conformității în temeiul legislației de armonizare relevante a Uniunii. În special, astfel de produse sunt echipamentele tehnice, jucăriile, ascensoarele, echipamentele și sistemele de protecție destinate utilizării în atmosfere potențial explozive, echipamentele radio, echipamentele sub presiune, echipamentele pentru ambarcațiuni de agrement, instalațiile pe cablu, aparatele consumatoare de combustibili gazoși, dispozitivele medicale și dispozitivele medicale pentru diagnostic in vitro.

(31) Clasificarea unui sistem de IA ca prezentând un risc ridicat în temeiul prezentului regulament nu ar trebui să însemne neapărat că produsul a cărui componentă de siguranță este sistemul de IA sau că sistemul de IA în sine ca produs este considerat „cu risc ridicat” în conformitate cu criteriile stabilite în legislația relevantă de armonizare a Uniunii care se aplică produsului. Acest lucru este valabil în special în cazul Regulamentului (UE) 2017/745 al Parlamentului European și al Consiliului[47] și al Regulamentului (UE) 2017/746 al Parlamentului European și al Consiliului[48], care

---

45 Regulamentul (UE) 2018/1139 al Parlamentului European și al Consiliului din 4 iulie 2018 privind normele comune în domeniul aviației civile și de înființare a Agenției Uniunii Europene pentru Siguranța Aviației, de modificare a Regulamentelor (CE) nr. 2111/2005, (CE) nr. 1008/2008, (UE) nr. 996/2010, (UE) nr. 376/2014 și a Directivelor 2014/30/UE și 2014/53/UE ale Parlamentului European și ale Consiliului, precum și de abrogare a Regulamentelor (CE) nr. 552/2004 și (CE) nr. 216/2008 ale Parlamentului European și ale Consiliului și a Regulamentului (CEE) nr. 3922/91 al Consiliului (JO L 212, 22.8.2018, p. 1).

46 Regulamentul (UE) 2019/2144 al Parlamentului European și al Consiliului din 27 noiembrie 2019 privind cerințele pentru omologarea de tip a autovehiculelor și remorcilor acestora, precum și a sistemelor, componentelor și unităților tehnice separate destinate unor astfel de vehicule, în ceea ce privește siguranța generală a acestora și protecția ocupanților vehiculului și a utilizatorilor vulnerabili ai drumurilor, de modificare a Regulamentului (UE) 2018/858 al Parlamentului European și al Consiliului și de abrogare a Regulamentelor (CE) nr. 78/2009, (CE) nr. 79/2009 și (CE) nr. 661/2009 ale Parlamentului European și ale Consiliului și a Regulamentelor (CE) nr. 631/2009, (UE) nr. 406/2010, (UE) nr. 672/2010, (UE) nr. 1003/2010, (UE) nr. 1005/2010, (UE) nr. 1008/2010, (UE) nr. 1009/2010, (UE) nr. 19/2011, (UE) nr. 109/2011, (UE) nr. 458/2011, (UE) nr. 65/2012, (UE) nr. 130/2012, (UE) nr. 347/2012, (UE) nr. 351/2012, (UE) nr. 1230/2012 și (UE) 2015/166 ale Comisie (JO L 325, 16.12.2019, p. 1).

47 Regulamentul (UE) 2017/745 al Parlamentului European și al Consiliului din 5 aprilie 2017 privind dispozitivele medicale, de modificare a Directivei 2001/83/CE, a Regulamentului (CE) nr. 178/2002 și a Regulamentului (CE) nr. 1223/2009 și de abrogare a Directivelor 90/385/CEE și 93/42/CEE ale Consiliului (JO L 117, 5.5.2017, p. 1).

48 Regulamentul (UE) 2017/746 al Parlamentului European și al Consiliului din 5 aprilie 2017 privind dispozitivele medicale pentru diagnostic in vitro și de abrogare a Directivei 98/79/CE și a Deciziei 2010/227/UE a Comisiei (JO L 117, 5.5.2017, p. 176).

prevăd o evaluare a conformității de către o parte terță pentru produsele cu risc mediu și cu risc ridicat.

(32) În ceea ce privește sistemele de IA autonome, adică alte sisteme de IA cu grad ridicat de risc decât cele care sunt componente de siguranță ale produselor sau care sunt ele însele produse, este oportun ca acestea să fie clasificate ca fiind cu risc ridicat dacă, având în vedere scopul preconizat, prezintă un risc ridicat de a aduce prejudicii sănătății și siguranței sau drepturilor fundamentale ale persoanelor, ținând seama atât de gravitatea posibilelor prejudicii, cât și de probabilitatea producerii acestora, și dacă sunt utilizate într-o serie de domenii predefinite în mod specific în regulament. Identificarea acestor sisteme se bazează pe aceeași metodologie și pe aceleași criterii avute în vedere și pentru orice modificare viitoare a listei de sisteme de IA cu grad ridicat de risc.

(33) Inexactitățile tehnice ale sistemelor de IA destinate identificării biometrice la distanță a persoanelor fizice pot conduce la rezultate subiective și pot avea efecte discriminatorii. Acest lucru este deosebit de relevant în ceea ce privește vârsta, etnia, sexul sau handicapul. Prin urmare, sistemele de identificare biometrică la distanță „în timp real” și „ulterior” ar trebui clasificate ca având un grad ridicat de risc. Având în vedere riscurile pe care le prezintă, ambele tipuri de sisteme de identificare biometrică la distanță ar trebui să facă obiectul unor cerințe specifice privind capacitățile de jurnalizare și supravegherea umană.

(34) În ceea ce privește gestionarea și exploatarea infrastructurii critice, este oportun să se clasifice ca fiind cu risc ridicat sistemele de IA destinate utilizării ca elemente de siguranță în gestionarea și exploatarea traficului rutier și în aprovizionarea cu apă, gaz, încălzire și energie electrică, deoarece defectarea sau funcționarea defectuoasă a acestora poate pune în pericol viața și sănătatea persoanelor la scară largă și poate conduce la perturbări semnificative ale desfășurării obișnuite a activităților sociale și economice.

(35) Sistemele de IA utilizate în educație sau în formarea profesională, în special pentru determinarea accesului sau desemnarea persoanelor în instituțiile de învățământ și formare profesională sau pentru evaluarea persoanelor care participă la teste ca parte a educației lor sau ca o condiție prealabilă pentru aceasta, ar trebui considerate ca având un grad ridicat de risc, deoarece pot determina parcursul educațional și profesional al vieții unei persoane și, prin urmare, pot afecta capacitatea acesteia de a-și asigura mijloacele de subzistență. Atunci când sunt concepute și utilizate în mod necorespunzător, astfel de sisteme pot încălca dreptul la educație și formare, precum și dreptul de a nu fi discriminat, și pot perpetua tiparele istorice de discriminare.

(36) Sistemele de IA utilizate în domeniul ocupării forței de muncă, al gestionării lucrătorilor și al accesului la activități independente, în special pentru recrutarea și selectarea persoanelor, pentru luarea deciziilor privind promovarea și încetarea activității, precum și pentru alocarea sarcinilor, monitorizarea sau evaluarea persoanelor aflate în raporturi contractuale legate de muncă, ar trebui, de asemenea, clasificate ca având un grad ridicat de risc, deoarece aceste sisteme pot avea un impact semnificativ asupra viitoarelor perspective de carieră și asupra mijloacelor de subzistență ale acestor persoane. Relațiile contractuale relevante legate de muncă ar trebui să implice angajații și persoanele care prestează servicii prin intermediul platformelor, astfel cum se menționează în Programul de lucru al Comisiei pentru 2021. Aceste persoane nu ar trebui, în principiu, să fie considerate utilizatori în sensul prezentului regulament. Pe tot parcursul procesului de recrutare, precum și în

evaluarea, promovarea sau menținerea persoanelor în relații contractuale legate de muncă, astfel de sisteme pot perpetua tiparele istorice de discriminare, de exemplu împotriva femeilor, a anumitor grupe de vârstă, a persoanelor cu handicap sau a persoanelor de anumite origini rasiale sau etnice sau cu o anumită orientare sexuală. Sistemele de IA utilizate pentru a monitoriza performanța și comportamentul acestor persoane pot avea, de asemenea, un impact asupra drepturilor lor la protecția datelor și la viața privată.

(37) Un alt domeniu în care utilizarea sistemelor de IA merită o atenție deosebită este accesul și posibilitatea de a beneficia de anumite servicii și beneficii publice și private esențiale, necesare pentru ca oamenii să participe pe deplin în societate sau să își îmbunătățească nivelul de trai. În special, sistemele de IA utilizate pentru a evalua punctajul de credit sau bonitatea persoanelor fizice ar trebui clasificate ca sisteme de IA cu grad ridicat de risc, întrucât acestea determină accesul persoanelor respective la resurse financiare sau la servicii esențiale, cum ar fi locuințe, electricitate și servicii de telecomunicații. Sistemele de IA utilizate în acest scop pot duce la discriminarea persoanelor sau a grupurilor și perpetuează modelele istorice de discriminare, de exemplu pe criterii de origine rasială sau etnică, handicap, vârstă, orientare sexuală, sau pot crea noi forme de impact discriminatoriu. Având în vedere amploarea foarte limitată a impactului și alternativele disponibile pe piață, este oportun să se excepteze sistemele de IA în scopul evaluării bonității și al evaluării creditelor atunci când sunt puse în funcțiune de către micii furnizori pentru uzul propriu. Persoanele fizice care solicită sau primesc prestații și servicii de asistență publică din partea autorităților publice depind, în general, de aceste prestații și servicii și se află într-o poziție vulnerabilă în raport cu autoritățile responsabile. În cazul în care sistemele de IA sunt utilizate pentru a stabili dacă astfel de prestații și servicii ar trebui refuzate, reduse, revocate sau recuperate de autorități, acestea pot avea un impact semnificativ asupra mijloacelor de subzistență ale persoanelor și le pot încălca drepturile fundamentale, cum ar fi dreptul la protecție socială, la nediscriminare, la demnitatea umană sau la o cale de atac eficientă. Prin urmare, aceste sisteme ar trebui clasificate ca prezentând un grad ridicat de risc. Cu toate acestea, prezentul regulament nu ar trebui să împiedice dezvoltarea și utilizarea unor abordări inovatoare în administrația publică, care ar putea beneficia de o utilizare mai largă a sistemelor de IA conforme și sigure, cu condiția ca aceste sisteme să nu implice un risc ridicat pentru persoanele fizice și juridice. În cele din urmă, sistemele de IA utilizate pentru dispecerizarea sau stabilirea priorității în dispecerizarea serviciilor de primă intervenție de urgență ar trebui, de asemenea, clasificate ca având un grad ridicat de risc, deoarece iau decizii în situații foarte critice pentru viața și sănătatea persoanelor și a bunurilor acestora.

(38) Acțiunile întreprinse de autoritățile de aplicare a legii care implică anumite utilizări ale sistemelor de IA sunt caracterizate de un grad semnificativ de dezechilibru de putere și pot duce la supravegherea, arestarea sau privarea de libertate a unei persoane fizice, precum și la alte efecte negative asupra drepturilor fundamentale garantate în Cartă. În special, în cazul în care în sistemul de IA nu se introduc date de înaltă calitate, în cazul în care acesta nu îndeplinește cerințele adecvate în ceea ce privește precizia sau robustețea sau nu este proiectat și testat în mod corespunzător înainte de a fi introdus pe piață sau pus în funcțiune în alt mod, acesta poate selecta persoanele într-un mod discriminatoriu sau incorect sau injust. În plus, exercitarea unor drepturi procedurale fundamentale importante, cum ar fi dreptul la o cale de atac eficientă și la un proces echitabil, precum și dreptul la apărare și prezumția de nevinovăție, ar putea fi împiedicată, în special, în cazul în care astfel de sisteme de IA nu sunt suficient de transparente, explicabile și documentate. Prin urmare, este oportun să se clasifice ca

având un grad ridicat de risc o serie de sisteme de IA destinate a fi utilizate în contextul asigurării respectării legii, în care acuratețea, fiabilitatea și transparența sunt deosebit de importante pentru a evita efectele negative, pentru a păstra încrederea publicului și pentru a asigura asumarea răspunderii și căi de atac eficace. Având în vedere natura activităților în cauză și riscurile aferente, aceste sisteme de IA cu grad ridicat de risc ar trebui să includă, în special, sistemele de IA destinate a fi utilizate de autoritățile de aplicare a legii pentru evaluări individuale ale riscurilor, pentru poligrafe și instrumente similare, sau pentru detectarea stării emoționale a persoanelor fizice, pentru a detecta „deepfake-urile", pentru a evalua fiabilitatea probelor în cadrul procedurilor penale, pentru a anticipa apariția sau repetarea unei infracțiuni reale sau potențiale pe baza stabilirii profilului criminalistic al persoanelor fizice sau pentru a evalua trăsăturile și caracteristicile de personalitate sau comportamentul infracțional anterior al unor persoane fizice sau al unor grupuri, pentru stabilirea de profiluri criminalistice în cursul depistării, al investigării sau al urmăririi penale a infracțiunilor, precum și pentru analiza infracționalității în ceea ce privește persoanele fizice. Sistemele de IA destinate în mod special utilizării în proceduri administrative de către autoritățile fiscale și vamale nu ar trebui să fie considerate sisteme de IA cu grad ridicat de risc utilizate de autoritățile de aplicare a legii în scopul prevenirii, depistării, investigării și urmăririi penale a infracțiunilor.

(39) Sistemele de IA utilizate în gestionarea migrației, a azilului și a controlului la frontieră afectează persoane care se află adesea într-o poziție deosebit de vulnerabilă și care depind de rezultatul acțiunilor autorităților publice competente. Acuratețea, caracterul nediscriminatoriu și transparența sistemelor de IA utilizate în aceste contexte sunt, prin urmare, deosebit de importante pentru a garanta respectarea drepturilor fundamentale ale persoanelor afectate, în special a drepturilor acestora la liberă circulație, nediscriminare, protecția vieții private și a datelor cu caracter personal, protecția internațională și buna administrare. Prin urmare, este oportun să fie clasificate cu grad ridicat de risc sistemele de IA destinate a fi utilizate de autoritățile publice competente care au atribuții în domeniile migrației, azilului și gestionării controlului la frontiere ca poligrafe și instrumente similare sau pentru a detecta starea emoțională a unei persoane fizice, pentru a evalua anumite riscuri prezentate de persoanele fizice care intră pe teritoriul unui stat membru sau care solicită viză sau azil, pentru a verifica autenticitatea documentelor relevante ale persoanelor fizice și pentru a acorda asistență autorităților publice competente în ceea ce privește examinarea cererilor de azil, de vize și de permise de ședere și a plângerilor aferente cu privire la obiectivul de stabilire a eligibilității persoanelor fizice care solicită un statut. Sistemele de IA din domeniul migrației, azilului și gestionării controlului la frontiere reglementate de prezentul regulament ar trebui să respecte cerințele procedurale relevante stabilite de Directiva 2013/32/UE a Parlamentului European și a Consiliului[49], de Regulamentul (CE) nr. 810/2009 al Parlamentului European și al Consiliului[50] și de alte acte legislative relevante.

(40) Anumite sisteme de IA destinate administrării justiției și proceselor democratice ar trebui clasificate ca având un grad ridicat de risc, având în vedere impactul potențial

[49] Directiva 2013/32/UE a Parlamentului European și a Consiliului din 26 iunie 2013 privind procedurile comune de acordare și retragere a protecției internaționale (JO L 180, 29.6.2013, p. 60).

[50] Regulamentul (CE) nr. 810/2009 al Parlamentului European și al Consiliului din 13 iulie 2009 privind instituirea unui Cod comunitar de vize (Codul de vize) (JO L 243, 15.9.2009, p. 1).

semnificativ al acestora asupra democrației, statului de drept și libertăților individuale, precum și asupra dreptului la o cale de atac eficientă și la un proces echitabil. În special, pentru a aborda potențialele riscuri de părtinire, erori și opacitate, este oportun să fie calificate drept sisteme cu grad ridicat de risc sistemele de IA menite să ajute autoritățile judiciare să cerceteze și să interpreteze faptele și legea și să aplice legea unui set concret de fapte. Cu toate acestea, o astfel de calificare nu ar trebui să se extindă la sistemele de IA destinate unor activități administrative pur auxiliare care nu afectează administrarea efectivă a justiției în cazuri individuale, cum ar fi anonimizarea sau pseudonimizarea hotărârilor judecătorești, a documentelor sau a datelor, comunicarea între membrii personalului, sarcinile administrative sau alocarea resurselor.

(41) Faptul că un sistem de IA este clasificat ca prezentând un risc ridicat în temeiul prezentului regulament nu ar trebui interpretat ca indicând faptul că utilizarea sistemului este neapărat legală în temeiul altor acte ale dreptului Uniunii sau al dreptului intern compatibil cu dreptul Uniunii, cum ar fi în ceea ce privește protecția datelor cu caracter personal, utilizarea poligrafelor și a instrumentelor similare sau a altor sisteme pentru a detecta starea emoțională a persoanelor fizice. Orice astfel de utilizare ar trebui să continue să aibă loc numai în conformitate cu cerințele aplicabile care decurg din Cartă, precum și din legislația secundară a Uniunii și din dreptul intern aplicabil. Prezentul regulament nu ar trebui înțeles ca oferind temeiul juridic pentru prelucrarea datelor cu caracter personal, inclusiv a categoriilor speciale de date cu caracter personal, după caz.

(42) Pentru atenuarea riscurilor generate de sistemele de IA cu grad ridicat de risc introduse sau puse în funcțiune în alt mod pe piața Uniunii pentru utilizatori și persoanele afectate, ar trebui să se aplice anumite cerințe obligatorii, ținând seama de scopul preconizat al utilizării sistemului și în conformitate cu sistemul de gestionare a riscurilor care urmează să fie instituit de furnizor.

(43) Cerințele ar trebui să se aplice sistemelor de IA cu grad ridicat de risc în ceea ce privește calitatea seturilor de date utilizate, documentația tehnică și păstrarea evidențelor, transparența și furnizarea de informații către utilizatori, supravegherea umană, robustețea, acuratețea și securitatea cibernetică. Aceste cerințe sunt necesare pentru a atenua în mod eficace riscurile pentru sănătate, siguranță și drepturile fundamentale, după caz, în funcție de scopul preconizat al sistemului, și nefiind disponibile în mod rezonabil alte măsuri mai puțin restrictive privind comerțul, se evită astfel restricțiile nejustificate în calea comerțului.

(44) Calitatea ridicată a datelor este esențială pentru performanța multor sisteme de IA, în special atunci când se utilizează tehnici care implică formarea de modele, pentru a se asigura că sistemul de IA cu grad ridicat de risc funcționează astfel cum s-a prevăzut și în condiții de siguranță și nu devine sursa discriminării, interzisă de dreptul Uniunii. Seturile de date de înaltă calitate de antrenament, de validare și de testare necesită punerea în aplicare a unor practici adecvate de guvernanță și gestionare a datelor. Seturile de date de antrenament, de validare și de testare ar trebui să fie suficient de relevante, reprezentative și lipsite de erori și complete având în vedere scopul preconizat al sistemului. Acestea ar trebui să aibă, de asemenea, proprietățile statistice adecvate, inclusiv în ceea ce privește persoanele sau grupurile de persoane în legătură cu care se intenționează să fie utilizat sistemul de IA cu grad ridicat de risc. În special, seturile de date de antrenament, de validare și de testare ar trebui să țină seama, în măsura în care acest lucru este necesar având în vedere scopul preconizat, de particularitățile, caracteristicile sau elementele care sunt specifice cadrului sau

contextului geografic, comportamental sau funcțional specific în care este destinat să fie utilizat sistemul de IA. Pentru a proteja dreptul altora împotriva discriminării care ar putea rezulta din părtinirea generată de sistemele de IA, furnizorii ar trebui să aibă posibilitatea de a prelucra și categorii speciale de date cu caracter personal, ca o chestiune de interes public major, pentru a asigura monitorizarea, detectarea și corectarea părtinirii în ceea ce privește sistemele de IA cu grad ridicat de risc.

(45) Pentru dezvoltarea sistemelor de IA cu grad ridicat de risc, anumiți actori, cum ar fi furnizorii, organismele notificate și alte entități relevante, cum ar fi centrele de inovare digitală, instalațiile de testare experimentate și cercetătorii, ar trebui să poată accesa și utiliza seturi de date de înaltă calitate în domeniile lor de activitate respective care sunt legate de prezentul regulament. Spațiile europene comune ale datelor instituite de Comisie și facilitarea schimbului de date între întreprinderi și cu administrațiile publice în interes public vor fi esențiale pentru a oferi un acces de încredere, responsabil și nediscriminatoriu la date de înaltă calitate pentru antrenarea, validarea și testarea sistemelor de IA. De exemplu, în domeniul sănătății, spațiul european al datelor medicale va facilita accesul nediscriminatoriu la datele medicale și antrenarea algoritmilor inteligenței artificiale cu privire la aceste seturi de date, într-un mod care protejează viața privată, sigur, prompt, transparent și fiabil și cu o guvernanță instituțională adecvată. Autoritățile competente relevante, inclusiv cele sectoriale, care furnizează sau sprijină accesul la date pot sprijini, de asemenea, furnizarea de date de înaltă calitate pentru antrenarea, validarea și testarea sistemelor de IA.

(46) Deținerea de informații cu privire la modul în care au fost dezvoltate sistemele de IA cu grad ridicat de risc și la modul în care acestea funcționează pe parcursul întregului lor ciclu de viață este esențială pentru verificarea conformității cu cerințele prevăzute în prezentul regulament. Acest lucru presupune păstrarea evidențelor și disponibilitatea unei documentații tehnice care să conțină informațiile necesare pentru a evalua conformitatea sistemului de IA cu cerințele relevante. Aceste informații ar trebui să includă caracteristicile generale, capacitățile și limitările sistemului, algoritmii, datele, procesele de antrenare, testare și validare utilizate, precum și documentația privind sistemul relevant de gestionare a riscurilor. Documentația tehnică ar trebui actualizată permanent.

(47) Pentru a aborda opacitatea care poate determina anumite sisteme de IA să fie imposibil de înțeles sau prea complexe pentru persoanele fizice, ar trebui să fie impus un anumit grad de transparență pentru sistemele de IA cu grad ridicat de risc. Utilizatorii ar trebui să poată interpreta rezultatele sistemului și să le poată utiliza în mod corespunzător. Prin urmare, sistemele de IA cu grad ridicat de risc ar trebui să fie însoțite de documentația relevantă și de instrucțiuni de utilizare și să includă informații concise și clare, inclusiv în ceea ce privește posibilele riscuri la adresa drepturilor fundamentale și în ceea ce privește discriminarea, după caz.

(48) Sistemele de IA cu grad ridicat de risc ar trebui să fie concepute și dezvoltate astfel încât persoanele fizice să poată supraveghea funcționarea lor. În acest scop, furnizorul sistemului ar trebui să identifice măsuri adecvate de supraveghere umană înainte de introducerea sa pe piață sau de punerea sa în funcțiune. În special, după caz, astfel de măsuri ar trebui să garanteze că sistemul este supus unor constrângeri operaționale integrate care nu pot fi dezactivate de sistem și care sunt receptive la operatorul uman și că persoanele fizice cărora le-a fost încredințată supravegherea umană au competența, pregătirea și autoritatea necesare pentru îndeplinirea acestui rol.

(49) Sistemele de IA cu grad ridicat de risc ar trebui să funcționeze în mod consecvent pe parcursul întregului lor ciclu de viață și să atingă un nivel adecvat de acuratețe, robustețe și securitate cibernetică, în conformitate cu stadiul actual al tehnologiei general recunoscut. Nivelul de acuratețe și de precizie ar trebui comunicat utilizatorilor.

(50) Robustețea tehnică este o cerință esențială pentru sistemele de IA cu grad ridicat de risc. Acestea ar trebui să fie rezistente la riscurile legate de limitările sistemului (de exemplu, erori, defecțiuni, inconsecvențe, situații neprevăzute), precum și la acțiunile răuvoitoare care pot compromite securitatea sistemului de IA și pot avea ca rezultat un comportament dăunător sau nedorit în alt mod. Incapacitatea de a asigura protecția împotriva acestor riscuri ar putea avea un impact asupra siguranței sau ar putea afecta în mod negativ drepturile fundamentale, de exemplu din cauza unor decizii eronate sau a unor rezultate greșite sau subiective generate de sistemul de IA.

(51) Securitatea cibernetică joacă un rol esențial în asigurarea rezilienței sistemelor de IA împotriva încercărilor de modificare a utilizării, a comportamentului, a performanței sau de compromitere a proprietăților lor de securitate de către părți terțe răuvoitoare care exploatează vulnerabilitățile sistemului. Atacurile cibernetice împotriva sistemelor de IA pot mobiliza active specifice de IA, cum ar fi seturi de date de antrenament (de exemplu, „data poisoning”) sau modele antrenate (de exemplu, atacuri contradictorii), sau pot exploata vulnerabilitățile activelor digitale ale sistemului de IA sau ale infrastructurii TIC subiacente. Pentru a asigura un nivel de securitate cibernetică adecvat riscurilor, furnizorii de sisteme de IA cu grad ridicat de risc ar trebui, prin urmare, să ia măsuri adecvate, ținând seama, de asemenea, după caz, de infrastructura TIC subiacentă.

(52) Ca parte a legislației de armonizare a Uniunii, normele aplicabile introducerii pe piață, punerii în funcțiune și utilizării sistemelor de IA cu grad ridicat de risc ar trebui să fie stabilite în conformitate cu Regulamentul (CE) nr. 765/2008 al Parlamentului European și al Consiliului[51] de stabilire a cerințelor de acreditare și de supraveghere a pieței în ceea ce privește comercializarea produselor, cu Decizia nr. 768/2008/CE a Parlamentului European și a Consiliului[52] privind un cadru comun pentru comercializarea produselor și cu Regulamentul (UE) 2019/1020 al Parlamentului European și al Consiliului[53] privind supravegherea pieței și conformitatea produselor („Noul cadru legislativ pentru comercializarea produselor”).

(53) Este oportun ca o anumită persoană fizică sau juridică, definită drept furnizor, să își asume responsabilitatea pentru introducerea pe piață sau punerea în funcțiune a unui sistem de IA cu grad ridicat de risc, indiferent dacă persoana fizică sau juridică respectivă este persoana care a proiectat sau a dezvoltat sistemul.

---

51 Regulamentul (CE) nr. 765/2008 al Parlamentului European și al Consiliului din 9 iulie 2008 de stabilire a cerințelor de acreditare și de supraveghere a pieței în ceea ce privește comercializarea produselor și de abrogare a Regulamentului (CEE) nr. 339/93 (JO L 218, 13.8.2008, p. 30).

52 Decizia nr. 768/2008/CE a Parlamentului European și a Consiliului din 9 iulie 2008 privind un cadru comun pentru comercializarea produselor și de abrogare a Deciziei 93/465/CEE a Consiliului (JO L 218, 13.8.2008, p. 82).

53 Regulamentul (UE) 2019/1020 al Parlamentului European și al Consiliului din 20 iunie 2019 privind supravegherea pieței și conformitatea produselor și de modificare a Directivei 2004/42/CE și a Regulamentelor (CE) nr. 765/2008 și (UE) nr. 305/2011 (Text cu relevanță pentru SEE) (JO L 169, 25.6.2019, p. 1-44).

(54) Furnizorul ar trebui să instituie un sistem solid de management al calității, să asigure realizarea procedurii necesare de evaluare a conformității, să întocmească documentația relevantă și să instituie un sistem solid de monitorizare după introducerea pe piață. Autoritățile publice care pun în funcțiune sisteme de IA cu grad ridicat de risc pentru uzul propriu pot adopta și pune în aplicare norme privind sistemul de management al calității ca parte a sistemului de management al calității adoptat la nivel național sau regional, după caz, ținând seama de particularitățile sectorului și de competențele și organizarea autorității publice în cauză.

(55) În cazul în care un sistem de IA cu grad ridicat de risc care este o componentă de siguranță a unui produs care face obiectul unei noi legislații sectoriale relevante nu este introdus pe piață sau pus în funcțiune independent de produs, producătorul produsului final, astfel cum este definit în legislația relevantă privind noul cadru legislativ, ar trebui să respecte obligațiile furnizorului stabilite în prezentul regulament și, în special, să se asigure că sistemul de IA încorporat în produsul final respectă cerințele prezentului regulament.

(56) Pentru a permite asigurarea respectării prezentului regulament și a crea condiții de concurență echitabile pentru operatori și ținând seama de diferitele forme de punere la dispoziție a produselor digitale, este important să se asigure că, în toate circumstanțele, o persoană stabilită în Uniune poate furniza autorităților toate informațiile necesare cu privire la conformitatea unui sistem de IA. Prin urmare, înainte de a-și pune la dispoziție sistemele de IA în Uniune, în cazul în care un importator nu poate fi identificat, furnizorii stabiliți în afara Uniunii desemnează, prin mandat scris, un reprezentant autorizat stabilit în Uniune.

(57) În conformitate cu principiile noului cadru legislativ, ar trebui stabilite obligații specifice pentru operatorii economici relevanți, cum ar fi importatorii și distribuitorii, pentru a asigura securitatea juridică și a facilita respectarea reglementărilor de către operatorii relevanți respectivi.

(58) Având în vedere natura sistemelor de IA și riscurile la adresa siguranței și a drepturilor fundamentale care pot fi asociate cu utilizarea lor, inclusiv în ceea ce privește necesitatea de a asigura o monitorizare adecvată a performanței unui sistem de IA într-un context real, este oportun să se stabilească responsabilități specifice pentru utilizatori. Utilizatorii ar trebui, în special, să utilizeze sisteme de IA cu grad ridicat de risc în conformitate cu instrucțiunile de utilizare și ar trebui prevăzute alte obligații în ceea ce privește monitorizarea funcționării sistemelor de IA și păstrarea evidențelor, după caz.

(59) Este oportun să se aibă în vedere faptul că utilizatorul sistemului de IA ar trebui să fie persoana fizică sau juridică, autoritatea publică, agenția sau alt organism sub a cărui autoritate funcționează sistemul de IA, cu excepția cazului în care utilizarea se face în cursul unei activități personale neprofesionale.

(60) Având în vedere complexitatea lanțului valoric al inteligenței artificiale, părțile terțe relevante, în special cele implicate în vânzarea și furnizarea de software, instrumente și componente software, modele și date pre-antrenate sau furnizorii de servicii de rețea ar trebui să coopereze, după caz, cu furnizorii și utilizatorii pentru a permite respectarea de către aceștia a obligațiilor care le revin în temeiul prezentului regulament și cu autoritățile competente instituite în temeiul prezentului regulament.

(61) Standardizarea ar trebui să joace un rol esențial în furnizarea de soluții tehnice furnizorilor pentru a asigura conformitatea cu prezentul regulament. Conformitatea cu

normele armonizate, astfel cum se prevede în Regulamentul (UE) nr. 1025/2012 al Parlamentului European și al Consiliului[54], ar trebui să fie un mijloc prin care furnizorii să demonstreze conformitatea cu cerințele prezentului regulament. Cu toate acestea, Comisia ar putea adopta specificații tehnice comune în domenii în care nu există norme armonizate sau în care acestea sunt insuficiente.

(62) Pentru a asigura un nivel ridicat de fiabilitate a sistemelor de IA cu grad ridicat de risc, aceste sisteme ar trebui să facă obiectul unei evaluări a conformității înainte de introducerea lor pe piață sau de punerea lor în funcțiune.

(63) Este oportun ca, pentru a reduce la minimum sarcina operatorilor și pentru a evita eventualele suprapuneri, pentru sistemele de IA cu grad ridicat de risc legate de produse care fac obiectul legislației de armonizare existente a Uniunii în conformitate cu abordarea bazată pe noul cadru legislativ, conformitatea acestor sisteme de IA cu cerințele prezentului regulament ar trebui să fie evaluată ca parte a evaluării conformității prevăzute deja în temeiul legislației respective. Aplicabilitatea cerințelor prezentului regulament nu ar trebui, prin urmare, să afecteze logica specifică, metodologia sau structura generală a evaluării conformității în temeiul legislației relevante din noul cadru legislativ. Această abordare se reflectă pe deplin în interacțiunea dintre prezentul regulament și [Regulamentul privind echipamentele tehnice]. În timp ce riscurile în materie de siguranță ale sistemelor de IA care asigură funcții de siguranță în echipamente tehnice sunt abordate de cerințele prezentului regulament, anumite cerințe specifice din [Regulamentul privind echipamentele tehnice] vor asigura integrarea în siguranță a sistemului de IA în întregul echipament tehnic, astfel încât să nu compromită siguranța echipamentului în ansamblu. [Regulamentul privind echipamentele tehnice] aplică aceeași definiție a sistemului de IA ca și prezentul regulament.

(64) Având în vedere experiența mai extinsă a organismelor profesionale de certificare înainte de introducerea pe piață în domeniul siguranței produselor și natura diferită a riscurilor implicate, este oportun să se limiteze, cel puțin într-o fază inițială de aplicare a prezentului regulament, domeniul de aplicare al evaluării conformității de către terți pentru sistemele de IA cu grad ridicat de risc, altele decât cele legate de produse. Prin urmare, evaluarea conformității unor astfel de sisteme ar trebui să fie efectuată, ca regulă generală, de către furnizor, pe propria răspundere, cu singura excepție a sistemelor de IA destinate a fi utilizate pentru identificarea biometrică la distanță a persoanelor, pentru care ar trebui prevăzută implicarea unui organism notificat în evaluarea conformității, în măsura în care acestea nu sunt interzise.

(65) Pentru a efectua evaluarea conformității de către terți a sistemelor de IA destinate utilizării pentru identificarea biometrică la distanță a persoanelor, autoritățile naționale competente ar trebui să desemneze organismele notificate în temeiul prezentului regulament, cu condiția ca acestea să respecte un set de cerințe, în special în ceea ce privește independența, competența și absența conflictelor de interese.

---

[54] Regulamentul (UE) nr. 1025/2012 al Parlamentului European și al Consiliului din 25 octombrie 2012 privind standardizarea europeană, de modificare a Directivelor 89/686/CEE și 93/15/CEE ale Consiliului și a Directivelor 94/9/CE, 94/25/CE, 95/16/CE, 97/23/CE, 98/34/CE, 2004/22/CE, 2007/23/CE, 2009/23/CE și 2009/105/CE ale Parlamentului European și ale Consiliului și de abrogare a Deciziei 87/95/CEE a Consiliului și a Deciziei nr. 1673/2006/CE a Parlamentului European și a Consiliului (JO L 316, 14.11.2012, p. 12).

(66) În conformitate cu noțiunea stabilită de comun acord a modificării substanțiale pentru produsele reglementate de legislația de armonizare a Uniunii, este oportun ca un sistem de IA să fie supus unei noi evaluări a conformității ori de câte ori apare o modificare care ar putea afecta conformitatea sistemului cu prezentul regulament sau atunci când scopul preconizat al sistemului se modifică. În plus, în ceea ce privește sistemele de IA care continuă să „învețe” după ce au fost introduse pe piață sau puse în funcțiune (adică adaptează automat modul în care sunt îndeplinite funcțiile), este necesar să se prevadă norme care să stabilească faptul că modificările algoritmului și ale performanței sale care au fost predeterminate de furnizor și evaluate la momentul evaluării conformității nu ar trebui să constituie o modificare substanțială.

(67) Sistemele de IA cu grad ridicat de risc ar trebui să poarte marcajul CE pentru a indica conformitatea lor cu prezentul regulament, astfel încât să poată circula liber în cadrul pieței interne. Statele membre ar trebui să nu genereze obstacole nejustificate în calea introducerii pe piață sau a punerii în funcțiune a sistemelor de IA cu risc ridicat care sunt conforme cu cerințele prevăzute de prezentul regulament și care poartă marcajul CE.

(68) În anumite condiții, disponibilitatea rapidă a tehnologiilor inovatoare poate fi esențială pentru sănătatea și siguranța persoanelor și pentru societate în ansamblu. Prin urmare, este oportun ca, din motive excepționale de siguranță publică sau de protecție a vieții și a sănătății persoanelor fizice și de protecție a proprietății industriale și comerciale, statele membre să poată autoriza introducerea pe piață sau punerea în funcțiune a sistemelor de IA care nu au fost supuse unei evaluări a conformității.

(69) Pentru a facilita activitatea Comisiei și a statelor membre în domeniul inteligenței artificiale, precum și pentru a spori transparența față de public, furnizorii de sisteme de IA cu grad ridicat de risc, altele decât cele legate de produse care intră în domeniul de aplicare al legislației de armonizare relevante existente a Uniunii, ar trebui să aibă obligația de a-și înregistra propriul sistem de IA cu grad ridicat de risc într-o bază de date a UE, care urmează să fie creată și gestionată de Comisie. Comisia ar trebui să fie operatorul bazei de date respective, în conformitate cu Regulamentul (UE) 2018/1725 al Parlamentului European și al Consiliului[55]. Pentru a asigura funcționalitatea deplină a bazei de date, atunci când aceasta este implementată, procedura de stabilire a bazei de date ar trebui să includă elaborarea de specificații funcționale de către Comisie și un raport de audit independent.

(70) Anumite sisteme de IA destinate să interacționeze cu persoane fizice sau să genereze conținut pot prezenta riscuri specifice de uzurpare a identității sau de înșelăciune, indiferent dacă acestea se califică drept sisteme cu risc ridicat sau nu. Prin urmare, în anumite circumstanțe, utilizarea acestor sisteme ar trebui să facă obiectul unor obligații specifice în materie de transparență, fără a aduce atingere cerințelor și obligațiilor pentru sistemele de IA cu grad ridicat de risc. În special, persoanele fizice ar trebui să fie informate că interacționează cu un sistem de IA, cu excepția cazului în care acest lucru este evident din circumstanțele și din contextul utilizării. În plus, persoanele fizice ar trebui notificate atunci când sunt expuse unui sistem de recunoaștere a emoțiilor sau unui sistem biometric de clasificare. Astfel de informații

[55] 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).

și notificări ar trebui să fie furnizate în formate accesibile pentru persoanele cu handicap. În plus, utilizatorii care utilizează un sistem de IA pentru a genera sau a manipula conținuturi de imagine, audio sau video care se aseamănă în mod apreciabil cu persoane, locuri sau evenimente existente și care par a fi autentice în mod fals, ar trebui să dezvăluie faptul că respectivul conținut a fost creat sau manipulat în mod artificial, prin etichetarea în consecință a rezultatului inteligenței artificiale și divulgarea originii sale artificiale.

(71) Inteligența artificială este o familie de tehnologii care se dezvoltă rapid și care necesită forme noi de supraveghere normativă și un spațiu sigur pentru experimentare, asigurând, în același timp, inovarea responsabilă și integrarea unor garanții adecvate și a unor măsuri de atenuare a riscurilor. Pentru a asigura un cadru juridic favorabil inovării, adaptat exigențelor viitorului și rezistent la perturbări, autoritățile naționale competente din unul sau mai multe state membre ar trebui încurajate să instituie spații de testare în materie de reglementare în domeniul inteligenței artificiale pentru a facilita dezvoltarea și testarea sistemelor de IA inovatoare aflate sub supraveghere normativă strictă înainte ca aceste sisteme să fie introduse pe piață sau puse în funcțiune în alt mod.

(72) Obiectivele spațiilor de testare în materie de reglementare ar trebui să fie promovarea inovării în domeniul IA prin instituirea unui mediu de experimentare și testare controlat în faza de dezvoltare și de precomercializare, cu scopul de a asigura conformitatea sistemelor de IA inovatoare cu prezentul regulament și cu alte acte legislative relevante ale Uniunii și ale statelor membre, sporirea securității juridice pentru inovatori și supravegherea și înțelegerea de către autoritățile competente a oportunităților, a riscurilor emergente și a impactului utilizării IA, precum și accelerarea accesului la piețe, inclusiv prin eliminarea barierelor din calea întreprinderilor mici și mijlocii (IMM-uri) și a întreprinderilor nou-înființate. Pentru a asigura o punere în aplicare uniformă în întreaga Uniune și economii de scară, este oportun să se stabilească norme comune pentru punerea în aplicare a spațiilor de testare în materie de reglementare și un cadru de cooperare între autoritățile relevante implicate în supravegherea spațiilor de testare. Prezentul regulament ar trebui să ofere temeiul juridic pentru utilizarea datelor cu caracter personal colectate în alte scopuri pentru dezvoltarea anumitor sisteme de IA în interes public în cadrul spațiului de testare în materie de reglementare privind IA, în conformitate cu articolul 6 alineatul (4) din Regulamentul (UE) 2016/679 și cu articolul 6 din Regulamentul (UE) 2018/1725 și fără a aduce atingere articolului 4 alineatul (2) din Directiva (UE) 2016/680. Participanții la spațiile de testare ar trebui să asigure garanții adecvate și să coopereze cu autoritățile competente, inclusiv urmând orientările acestora și acționând cu promptitudine și cu bună-credință pentru a atenua orice risc ridicat la adresa siguranței și a drepturilor fundamentale care ar putea apărea în timpul dezvoltării și experimentării în spațiul de testare. Comportamentul participanților la spațiile de testare ar trebui luat în considerare atunci când autoritățile competente decid dacă să impună sau nu o amendă administrativă în temeiul articolului 83 alineatul (2) din Regulamentul 2016/679 și al articolului 57 din Directiva 2016/680.

(73) Pentru a promova și proteja inovarea, este important ca interesele micilor furnizori și utilizatori de sisteme de IA să fie luate în considerare în mod deosebit. În acest scop, statele membre ar trebui să elaboreze inițiative care să vizeze operatorii respectivi, inclusiv în ceea ce privește sensibilizarea și comunicarea informațiilor. În plus, interesele și nevoile specifice ale micilor furnizorilor sunt luate în considerare atunci când organismele notificate stabilesc taxe de evaluare a conformității. Costurile de

traducere legate de documentația obligatorie și de comunicarea cu autoritățile pot constitui un cost semnificativ pentru furnizori și alți operatori, în special pentru cei de dimensiuni mai mici. Statele membre ar trebui, eventual, să se asigure că una dintre limbile stabilite și acceptate pentru documentația furnizorilor relevanți și pentru comunicarea cu operatorii este una înțeleasă pe larg de un număr cât mai mare de utilizatori transfrontalieri.

(74) Pentru a reduce la minimum riscurile la adresa punerii în aplicare care decurg din lipsa de cunoștințe și de expertiză de pe piață, precum și pentru a facilita respectarea de către furnizori și organismele notificate a obligațiilor care le revin în temeiul prezentului regulament, platforma de IA la cerere, centrele europene de inovare digitală și instalațiile de testare și experimentare instituite de Comisie și de statele membre la nivel național sau la nivelul UE ar trebui, eventual, să contribuie la punerea în aplicare a prezentului regulament. În cadrul misiunii și domeniilor lor de competență respective, aceștia pot oferi, în special, sprijin tehnic și științific furnizorilor și organismelor notificate.

(75) Este oportun ca, în măsura posibilului, Comisia să faciliteze accesul la instalațiile de testare și experimentare pentru organismele, grupurile sau laboratoarele înființate sau acreditate în temeiul oricărei legislații de armonizare relevante a Uniunii și care îndeplinesc sarcini în contextul evaluării conformității produselor sau dispozitivelor reglementate de respectiva legislație de armonizare a Uniunii. Acest lucru este valabil în special pentru grupurile de experți, laboratoarele de expertiză și laboratoarele de referință în domeniul dispozitivelor medicale în temeiul Regulamentului (UE) 2017/745 și al Regulamentului (UE) 2017/746.

(76) Pentru a facilita o punere în aplicare armonioasă, eficace și armonizată a prezentului regulament, ar trebui instituit un Comitet european pentru inteligența artificială. Comitetul ar trebui să fie responsabil pentru o serie de sarcini consultative, inclusiv emiterea de avize, recomandări, consiliere sau orientări cu privire la aspecte legate de punerea în aplicare a prezentului regulament, inclusiv cu privire la specificațiile tehnice sau standardele existente referitoare la cerințele stabilite în prezentul regulament, precum și furnizarea de consiliere și asistență Comisiei cu privire la chestiuni specifice legate de inteligența artificială.

(77) Statele membre joacă un rol esențial în aplicarea și asigurarea respectării prezentului regulament. În acest sens, fiecare stat membru ar trebui să desemneze una sau mai multe autorități naționale competente în scopul supravegherii aplicării și punerii în aplicare a prezentului regulament. Pentru a spori eficiența organizațională din partea statelor membre și pentru a stabili un punct oficial de contact cu publicul și cu alți omologi la nivelul statelor membre și al Uniunii, în fiecare stat membru, o autoritate națională ar trebui desemnată drept autoritate națională de supraveghere.

(78) Pentru a se asigura că furnizorii de sisteme de IA cu grad ridicat de risc pot ține seama de experiența privind utilizarea sistemelor de IA cu grad ridicat de risc pentru îmbunătățirea sistemelor lor și a procesului de proiectare și dezvoltare sau că pot lua orice măsură corectivă posibilă în timp util, toți furnizorii ar trebui să dispună de un sistem de monitorizare ulterioară introducerii pe piață. Acest sistem este, de asemenea, esențial pentru a se asigura că posibilele riscuri care decurg din sistemele de IA care continuă să „învețe” după ce au fost introduse pe piață sau puse în funcțiune pot fi abordate într-un mod mai eficient și la timp. În acest context, furnizorii ar trebui, de asemenea, să aibă obligația de a dispune de un sistem pentru a raporta autorităților

relevante orice incident grav sau orice încălcare a legislației naționale și a Uniunii care protejează drepturile fundamentale, ca urmare a utilizării sistemelor lor de IA.

(79) Pentru a asigura o aplicare adecvată și eficace a cerințelor și a obligațiilor prevăzute în prezentul regulament, și anume în legislația de armonizare a Uniunii, sistemul de supraveghere a pieței și de conformitate a produselor instituit prin Regulamentul (UE) 2019/1020 ar trebui să se aplice în întregime. În cazul în care acest lucru este necesar pentru îndeplinirea mandatului lor, autoritățile sau organismele publice naționale care supraveghează aplicarea dreptului Uniunii care protejează drepturile fundamentale, inclusiv organismele de promovare a egalității, ar trebui să aibă, de asemenea, acces la orice documentație creată în temeiul prezentului regulament.

(80) Legislația Uniunii privind serviciile financiare include norme și cerințe privind guvernanța internă și gestionarea riscurilor care sunt aplicabile instituțiilor financiare reglementate în cursul furnizării acestor servicii, inclusiv atunci când acestea utilizează sisteme de IA. Pentru a asigura aplicarea și asigurarea respectării coerente a obligațiilor prevăzute în prezentul regulament și a normelor și cerințelor relevante ale legislației Uniunii în domeniul serviciilor financiare, autoritățile responsabile cu supravegherea și asigurarea respectării legislației privind serviciile financiare, inclusiv, după caz, Banca Centrală Europeană, ar trebui desemnate drept autorități competente în scopul supravegherii punerii în aplicare a prezentului regulament, inclusiv pentru activitățile de supraveghere a pieței, în ceea ce privește sistemele de IA furnizate sau utilizate de instituțiile financiare reglementate și supravegheate. Pentru a spori și mai mult coerența dintre prezentul regulament și normele aplicabile instituțiilor de credit reglementate în temeiul Directivei 2013/36/UE a Parlamentului European și a Consiliului[56], este, de asemenea, oportun să se integreze procedura de evaluare a conformității și unele dintre obligațiile procedurale ale furnizorilor în ceea ce privește gestionarea riscurilor, monitorizarea ulterioară introducerii pe piață și documentația în obligațiile și procedurile existente în temeiul Directivei 2013/36/UE. Pentru a evita suprapunerile, ar trebui avute în vedere derogări limitate și în ceea ce privește sistemul de management al calității furnizorilor și obligația de monitorizare impusă utilizatorilor de sisteme de IA cu grad ridicat de risc, în măsura în care acestea se aplică instituțiilor de credit reglementate de Directiva 2013/36/UE.

(81) Dezvoltarea altor sisteme de IA decât cele cu grad ridicat de risc în conformitate cu cerințele prezentului regulament poate duce la o utilizare pe scară mai largă a inteligenței artificiale de încredere în Uniune. Furnizorii de sisteme de IA care nu prezintă un grad ridicat de risc ar trebui încurajați să creeze coduri de conduită menite să promoveze aplicarea voluntară a cerințelor obligatorii aplicabile sistemelor de IA cu grad ridicat de risc. Furnizorii ar trebui, de asemenea, încurajați să aplice în mod voluntar cerințe suplimentare legate, de exemplu, de durabilitatea mediului, de accesibilitatea pentru persoanele cu handicap, de participarea părților interesate la proiectarea și dezvoltarea sistemelor de IA și de diversitatea echipelor de dezvoltare. Comisia poate elabora inițiative, inclusiv de natură sectorială, pentru a facilita reducerea barierelor tehnice care împiedică schimbul transfrontalier de date pentru dezvoltarea IA, inclusiv în ceea ce privește infrastructura de acces la date, interoperabilitatea semantică și tehnică a diferitelor tipuri de date.

---

[56] Directiva 2013/36/UE a Parlamentului European și a Consiliului din 26 iunie 2013 cu privire la accesul la activitatea instituțiilor de credit și supravegherea prudențială a instituțiilor de credit și a firmelor de investiții, de modificare a Directivei 2002/87/CE și de abrogare a Directivelor 2006/48/CE și 2006/49/CE (JO L 176, 27.6.2013, p. 338).

(82) Este important ca sistemele de IA legate de produse care nu prezintă un risc ridicat în conformitate cu prezentul regulament și care, prin urmare, nu sunt obligate să respecte cerințele prevăzute în prezentul regulament să fie totuși sigure atunci când sunt introduse pe piață sau puse în funcțiune. Pentru a contribui la acest obiectiv, Directiva 2001/95/CE a Parlamentului European și a Consiliului[57] ar fi aplicată ca o „plasă de siguranță”.

(83) Pentru a asigura o cooperare de încredere și constructivă a autorităților competente la nivelul Uniunii și la nivel național, toate părțile implicate în aplicarea prezentului regulament ar trebui să respecte confidențialitatea informațiilor și a datelor obținute în cursul îndeplinirii sarcinilor lor.

(84) Statele membre ar trebui să ia toate măsurile necesare pentru a se asigura că dispozițiile prezentului regulament sunt puse în aplicare, inclusiv prin stabilirea unor sancțiuni eficace, proporționale și disuasive în cazul încălcării acestora. Pentru anumite încălcări specifice, statele membre ar trebui să țină seama de marjele și de criteriile stabilite în prezentul regulament. Autoritatea Europeană pentru Protecția Datelor ar trebui să aibă competența de a impune amenzi instituțiilor, agențiilor și organelor Uniunii care intră în domeniul de aplicare al prezentului regulament.

(85) Pentru a se asigura posibilitatea de adaptare a cadrului de reglementare atunci când este necesar, competența de a adopta acte în conformitate cu articolul 290 din TFUE ar trebui delegată Comisiei pentru a modifica tehnicile și abordările menționate în anexa I pentru definirea sistemelor de IA, legislația de armonizare a Uniunii enumerată în anexa II, sistemele de IA cu grad ridicat de risc enumerate în anexa III, dispozițiile privind documentația tehnică enumerate în anexa IV, conținutul declarației de conformitate UE din anexa V, dispozițiile privind procedurile de evaluare a conformității din anexele VI și VII și dispozițiile de stabilire a sistemelor de IA cu grad ridicat de risc cărora ar trebui să li se aplice procedura de evaluare a conformității bazată pe evaluarea sistemului de management al calității și evaluarea documentației tehnice. Este deosebit de important ca, în cursul lucrărilor sale pregătitoare, Comisia să organizeze consultări corespunzătoare, inclusiv la nivel de experți, și ca respectivele consultări să se desfășoare în conformitate cu principiile stabilite în Acordul interinstituțional privind o mai bună legiferare[58], adoptat la 13 aprilie 2016. În special, pentru a asigura participarea egală la pregătirea actelor delegate, Parlamentul European și Consiliul primesc toate documentele în același timp cu experții din statele membre, iar experții acestor instituții au acces sistematic la reuniunile grupurilor de experți ale Comisiei însărcinate cu pregătirea actelor delegate.

(86) În vederea asigurării unor condiții uniforme pentru punerea în aplicare a prezentului regulament, ar trebui conferite competențe de executare Comisiei. Respectivele competențe ar trebui exercitate în conformitate cu Regulamentul (UE) nr. 182/2011 al Parlamentului European și al Consiliului[59].

(87) Deoarece obiectivele prezentului regulament nu pot fi realizate în mod satisfăcător de către statele membre dar, având în vedere amploarea și efectele acțiunii, pot fi realizate

---

57 Directiva 2001/95/CE a Parlamentului European și a Consiliului din 3 decembrie 2001 privind siguranța generală a produselor (JO L 11, 15.1.2002, p. 4).

58 JO L 123, 12.5.2016, p. 1.

59 Regulamentul (UE) nr. 182/2011 al Parlamentului European și al Consiliului din 16 februarie 2011 de stabilire a normelor și principiilor generale privind mecanismele de control de către statele membre al exercitării competențelor de executare de către Comisie (JO L 55, 28.2.2011, p. 13).

mai bine la nivelul Uniunii, aceasta poate adopta măsuri în conformitate cu principiul subsidiarității astfel cum este definit la articolul 5 din TUE. În conformitate cu principiul proporționalității, astfel cum este definit la articolul respectiv, prezentul regulament nu depășește ceea ce este necesar pentru realizarea obiectivului menționat.

(88) Prezentul regulament ar trebui să se aplice de la... [*OP – de introdus data stabilită la articolul 85*]. Cu toate acestea, infrastructura legată de guvernanță și de sistemul de evaluare a conformității ar trebui să fie operațională înainte de data respectivă; prin urmare, dispozițiile privind organismele notificate și structura de guvernanță ar trebui să se aplice de la ... [*OP – de introdus data – trei luni de la intrarea în vigoare a prezentului regulament*]. În plus, statele membre ar trebui să stabilească și să notifice Comisiei normele privind sancțiunile, inclusiv amenzile administrative, și să se asigure că acestea sunt puse în aplicare în mod corespunzător și cu eficacitate până la data aplicării prezentului regulament. Prin urmare, dispozițiile privind sancțiunile ar trebui să se aplice de la [*OP – de introdus data – douăsprezece luni de la intrarea în vigoare a prezentului regulament*].

(89) Autoritatea Europeană pentru Protecția Datelor și Comitetul european pentru protecția datelor au fost consultate în conformitate cu articolul 42 alineatul (2) din Regulamentul (UE) 2018/1725 și au emis un aviz la [...]”,

ADOPTĂ PREZENTUL REGULAMENT:

TITLUL I

DISPOZIȚII GENERALE

Articolul 1

Obiectul

Prezentul regulament stabilește:

(a) norme armonizate pentru introducerea pe piață, punerea în funcțiune și utilizarea sistemelor de inteligență artificială („sisteme de IA”) în Uniune;

(a) interzicerea anumitor practici în domeniul inteligenței artificiale;

(b) cerințe specifice pentru sistemele de IA cu grad ridicat de risc și obligații pentru operatorii unor astfel de sisteme;

(c) norme armonizate de transparență pentru sistemele de IA destinate să interacționeze cu persoane fizice, pentru sistemele de recunoaștere a emoțiilor, pentru sistemele biometrice de clasificare și pentru sistemele de IA utilizate pentru a genera sau a manipula imagini, conținuturi audio sau video;

(d) norme privind monitorizarea și supravegherea pieței.

Articolul 2

Domeniul de aplicare

1. Prezentul regulament se aplică pentru:

(a) furnizorii care introduc pe piață sau pun în funcțiune sisteme de IA în Uniune, indiferent dacă furnizorii respectivi sunt stabiliți în Uniune sau într-o țară terță;

(b) utilizatorii sistemelor de IA situați pe teritoriul Uniunii;

(c) furnizorii și utilizatorii de sisteme de IA care sunt situați într-o țară terță, în cazul în care rezultatele produse de sistem sunt utilizate în Uniune.

2. În cazul sistemelor de IA cu grad ridicat de risc care sunt componente de siguranță ale unor produse sau sisteme sau care sunt ele însele produse sau sisteme, care intră în domeniul de aplicare al următoarelor acte legislative, se aplică numai articolul 84 din prezentul regulament:

(a) Regulamentul (CE) 300/2008;

(b) Regulamentul (UE) nr. 167/2013;

(c) Regulamentul (UE) nr. 168/2013;

(d) Directiva 2014/90/UE;

(e) Directiva (UE) 2016/797;

(f) Regulamentul (UE) 2018/858;

(g) Regulamentul (UE) 2018/1139;

(h) Regulamentul (UE) 2019/2144.

3. Prezentul regulament nu se aplică sistemelor de IA dezvoltate sau utilizate exclusiv în scopuri militare.

4. Prezentul regulament nu se aplică autorităților publice dintr-o țară terță și nici organizațiilor internaționale care intră în domeniul de aplicare al prezentului regulament în temeiul alineatului (1), în cazul în care respectivele autorități sau organizații utilizează sisteme de IA în cadrul acordurilor internaționale pentru asigurarea respectării legii și pentru cooperarea judiciară cu Uniunea sau cu unul sau mai multe state membre.

5. Prezentul regulament nu aduce atingere aplicării dispozițiilor privind răspunderea furnizorilor de servicii intermediari prevăzute în capitolul II secțiunea IV din Directiva 2000/31/CE a Parlamentului European și a Consiliului[60] [*astfel cum urmează să fie înlocuite cu dispozițiile corespunzătoare din Actul legislativ privind serviciile digitale*].

Articolul 3

Definiții

În sensul prezentului regulament, se aplică următoarele definiții:

(1) „sistem de inteligență artificială” (sistem de IA) înseamnă un software care este dezvoltat prin una sau mai multe dintre tehnicile și abordările enumerate în anexa I și care, pentru un anumit set de obiective definite de om, poate genera rezultate precum conținuturi, previziuni, recomandări sau decizii care influențează mediile cu care interacționează;

[60] Directiva 2000/31/CE a Parlamentului European și a Consiliului din 8 iunie 2000 privind anumite aspecte juridice ale serviciilor societății informaționale, în special ale comerțului electronic, pe piața internă („Directiva privind comerțul electronic”) (JO L 178, 17.7.2000, p. 1).

(2) „furnizor” înseamnă o persoană fizică sau juridică, o autoritate publică, o agenție sau un alt organism care dezvoltă un sistem de IA sau care dispune de un sistem de IA dezvoltat în vederea introducerii sale pe piață sau a punerii sale în funcțiune sub propriul nume sau propria marcă comercială, contra cost sau gratuit;

(3) „mic furnizor” înseamnă un furnizor care este o microîntreprindere sau o întreprindere mică în sensul Recomandării 2003/361/CE a Comisiei[61];

(4) „utilizator” înseamnă orice persoană fizică sau juridică, autoritate publică, agenție sau alt organism care utilizează un sistem de IA aflat sub autoritatea sa, cu excepția cazului în care sistemul de IA este utilizat în cursul unei activități neprofesionale, personale;

(5) „reprezentant autorizat” înseamnă orice persoană fizică sau juridică stabilită în Uniune care a primit un mandat scris din partea unui furnizor de sistem de IA pentru a exercita și, respectiv, a îndeplini, în numele său, obligațiile și procedurile stabilite prin prezentul regulament;

(6) „importator” înseamnă orice persoană fizică sau juridică stabilită în Uniune care introduce pe piață sau pune în funcțiune un sistem de IA care poartă numele sau marca unei persoane fizice sau juridice stabilite în afara Uniunii;

(7) „distribuitor” înseamnă orice persoană fizică sau juridică din lanțul de aprovizionare, alta decât furnizorul sau importatorul, care pune la dispoziție un sistem de IA pe piața Uniunii fără a-i afecta proprietățile;

(8) „operator” înseamnă furnizorul, utilizatorul, reprezentantul autorizat, importatorul și distribuitorul;

(9) „introducere pe piață” înseamnă prima punere la dispoziție a unui sistem de IA pe piața Uniunii;

(10) „punere la dispoziție pe piață” înseamnă furnizarea unui sistem de IA pentru distribuție sau uz pe piața Uniunii în cursul unei activități comerciale, contra cost sau gratuit;

(11) „punere în funcțiune” înseamnă furnizarea unui sistem de IA pentru prima utilizare direct utilizatorului sau pentru uz propriu pe piața Uniunii, în scopul pentru care a fost conceput;

(12) „scop preconizat” înseamnă utilizarea preconizată de către furnizor a unui sistem de IA, inclusiv contextul specific și condițiile de utilizare, astfel cum se specifică în informațiile oferite de furnizor în instrucțiunile de utilizare, în materialele promoționale sau de vânzare și în declarații, precum și în documentația tehnică;

(13) „utilizare necorespunzătoare previzibilă în mod rezonabil” înseamnă utilizarea unui sistem de IA într-un mod care nu este în conformitate cu scopul său preconizat, dar care poate rezulta din comportamentul uman sau din interacțiunea previzibilă în mod rezonabil cu alte sisteme;

(14) „componentă de siguranță a unui produs sau sistem” înseamnă o componentă a unui produs sau a unui sistem care îndeplinește o funcție de siguranță pentru produsul sau sistemul respectiv sau a cărei defectare sau funcționare defectuoasă pune în pericol sănătatea și siguranța persoanelor sau a bunurilor;

---

[61] Recomandarea Comisiei din 6 mai 2003 privind definirea microîntreprinderilor și a întreprinderilor mici și mijlocii, (JO L 124, 20.5.2003, p. 36).

(15) „instrucțiuni de utilizare” înseamnă informațiile oferite de furnizor pentru a informa utilizatorul, în special cu privire la scopul preconizat și utilizarea corespunzătoare a unui sistem de IA, inclusiv cu privire la mediul geografic, comportamental sau funcțional specific în care urmează să fie utilizat sistemul de IA cu grad ridicat de risc;

(16) „rechemare a unui sistem de IA” înseamnă orice măsură care are drept scop returnarea către furnizor a unui sistem de IA deja pus la dispoziția utilizatorilor;

(17) „retragere a unui sistem de IA” înseamnă orice măsură care are drept scop prevenirea distribuției, a expunerii și a oferirii unui sistem de IA;

(18) „performanță a unui sistem de IA” înseamnă capacitatea unui sistem de IA de a-și atinge scopul preconizat;

(19) „autoritate de notificare” înseamnă autoritatea națională responsabilă cu instituirea și îndeplinirea procedurilor necesare pentru evaluarea, desemnarea și notificarea organismelor de evaluare a conformității și pentru monitorizarea acestora;

(20) „evaluare a conformității” înseamnă procesul prin care se verifică dacă au fost îndeplinite cerințele prevăzute în titlul III capitolul 2 din prezentul regulament referitoare la un sistem de IA;

(21) „organism de evaluare a conformității” înseamnă un organism care efectuează activități de evaluare a conformității ca parte terță, incluzând testarea, certificarea și inspecția;

(22) „organism notificat” înseamnă un organism de evaluare a conformității desemnat în conformitate cu prezentul regulament și cu alte acte legislative relevante de armonizare ale Uniunii;

(23) „modificare substanțială” înseamnă o modificare a sistemului de IA ca urmare a introducerii sale pe piață sau a punerii sale în funcțiune, care afectează conformitatea sistemului de IA cu cerințele prevăzute în titlul III capitolul 2 din prezentul regulament sau care conduce la o modificare a scopului preconizat pentru care a fost evaluat sistemul de IA;

(24) „marcaj CE de conformitate” (marcaj CE) înseamnă un marcaj prin care un furnizor indică faptul că un sistem de IA este în conformitate cu cerințele prevăzute în titlul III capitolul 2 din prezentul regulament și în alte acte legislative aplicabile ale Uniunii care armonizează condițiile de comercializare a produselor („legislația de armonizare a Uniunii”), care prevede aplicarea acestuia;

(25) „monitorizare ulterioară introducerii pe piață” înseamnă toate activitățile desfășurate de furnizorii de sisteme de IA pentru a colecta și a revizui în mod proactiv experiența dobândită în urma utilizării sistemelor de IA pe care le introduc pe piață sau le pun în funcțiune, în scopul identificării oricărei nevoi de a aplica imediat orice măsură corectivă sau preventivă necesară;

(26) „autoritate de supraveghere a pieței” înseamnă autoritatea națională care desfășoară activități și ia măsuri în temeiul Regulamentului (UE) 2019/1020;

(27) „normă armonizată” înseamnă un standard european conform definiției de la articolul 2 alineatul (1) litera (c) din Regulamentul (UE) nr. 1025/2012;

(28) „specificații comune” înseamnă un document, altul decât un standard, care conține soluții tehnice care oferă un mijloc pentru respectarea anumitor cerințe și obligații stabilite în temeiul prezentului regulament;

(29) „date de antrenament” înseamnă datele utilizate pentru antrenarea unui sistem de IA prin adaptarea parametrilor săi care pot fi învățați, inclusiv a ponderilor unei rețele neuronale;

(30) „date de verificare” înseamnă datele utilizate pentru a furniza o evaluare a sistemului de IA antrenat și pentru a-i ajusta parametrii care nu pot fi învățați și procesul său de învățare, printre altele, pentru a preveni supraadaptarea; în timp ce setul de date de verificare poate fi un set de date separat sau o parte a setului de date de antrenament, ca o divizare fixă sau variabilă;

(31) „date de testare” înseamnă datele utilizate pentru a furniza o evaluare independentă a sistemului de IA antrenat și validat, pentru a confirma performanța preconizată a sistemului respectiv înainte de introducerea sa pe piață sau de punerea sa în funcțiune;

(32) „date de intrare” înseamnă datele furnizate unui sistem de IA sau achiziționate direct de acesta, pe baza cărora sistemul produce un rezultat;

(33) „date biometrice” înseamnă datele cu caracter personal rezultate din aplicarea unor tehnici de prelucrare specifice referitoare la caracteristicile fizice, fiziologice sau comportamentale ale unei persoane fizice, care permit sau confirmă identificarea unică a respectivei persoane, cum ar fi imaginile faciale sau datele dactiloscopice;

(34) „sistem de recunoaștere a emoțiilor” înseamnă un sistem de IA al cărui scop este de a identifica sau a deduce emoțiile sau intențiile persoanelor fizice pe baza datelor lor biometrice;

(35) „sistem biometric de clasificare” înseamnă un sistem de IA al cărui scop este de a încadra persoanele fizice în categorii specifice, cum ar fi sexul, vârsta, culoarea părului, culoarea ochilor, tatuajele, originea etnică sau orientarea sexuală sau politică, pe baza datelor lor biometrice;

(36) „sistem de identificare biometrică la distanță” înseamnă un sistem de IA al cărui scop este de a identifica persoanele fizice la distanță prin compararea datelor biometrice ale unei persoane cu datele biometrice conținute într-o bază de date de referință și fără ca utilizatorul sistemului de IA să cunoască în prealabil dacă persoana va fi prezentă și dacă poate fi identificată;

(37) „sistem de identificare biometrică la distanță «în timp real»” înseamnă un sistem de identificare biometrică la distanță în care capturarea datelor biometrice și compararea și identificarea au loc toate fără întârzieri semnificative. Acesta include nu numai identificarea instantanee, ci și întârzieri scurte limitate pentru a se evita eludarea;

(38) „sistem de identificare biometrică la distanță «ulterioară»” înseamnă un sistem de identificare biometrică la distanță, altul decât un sistem de identificare biometrică la distanță „în timp real”;

(39) „spațiu accesibil publicului” înseamnă orice loc fizic accesibil publicului, indiferent daca se pot aplica anumite condiții de acces;

(40) „autoritate de aplicare a legii” înseamnă:

(a) orice autoritate publică competentă în materie de prevenire, investigare, depistare sau urmărire penală a infracțiunilor sau de executare a pedepselor, inclusiv în materie de protejare împotriva amenințărilor la adresa securității publice și de prevenire a acestora; sau

(b) orice alt organism sau entitate împuternicit(ă) de dreptul statului membru să exercite autoritate publică și competențe publice în scopul prevenirii, investigării, depistării sau urmăririi penale a infracțiunilor sau al executării pedepselor, inclusiv al protejării împotriva amenințărilor la adresa securității publice și al prevenirii acestora;

(41) „asigurare a respectării legii” înseamnă activitățile desfășurate de autoritățile de aplicare a legii pentru prevenirea, investigarea, depistarea sau urmărirea penală a infracțiunilor sau pentru executarea pedepselor, inclusiv în ceea ce privește protejarea împotriva amenințărilor la adresa securității publice și prevenirea acestora;

(42) „autoritate națională de supraveghere” înseamnă autoritatea căreia un stat membru îi atribuie responsabilitatea pentru punerea în aplicare a prezentului regulament, pentru coordonarea activităților încredințate statului membru respectiv, pentru îndeplinirea rolului de punct unic de contact pentru Comisie și pentru reprezentarea statului membru în cadrul Comitetului european pentru inteligența artificială;

(43) „autoritate națională competentă” înseamnă autoritatea națională de supraveghere, autoritatea de notificare și autoritatea de supraveghere a pieței;

(44) „incident grav” înseamnă orice incident care, direct sau indirect, determină, ar fi putut determina sau ar putea determina oricare dintre următoarele:

(a) decesul unei persoane sau afectarea gravă a sănătății unei persoane, a bunurilor sau a mediului;

(b) o perturbare gravă și ireversibilă a gestionării și funcționării infrastructurii critice.

Articolul 4

Modificarea anexei I

Comisia este împuternicită să adopte acte delegate în conformitate cu articolul 73 pentru a modifica lista tehnicilor și abordărilor enumerate în anexa I, în vederea actualizării listei respective în funcție de evoluțiile pieței și de cele tehnologice, pe baza caracteristicilor care sunt similare cu tehnicile și abordările enumerate în anexa respectivă.

TITLUL II

PRACTICI INTERZISE ÎN DOMENIUL INTELIGENȚEI ARTIFICIALE

Articolul 5

1. Sunt interzise următoarele practici în domeniul inteligenței artificiale:

(a) introducerea pe piață, punerea în funcțiune sau utilizarea unui sistem de IA care utilizează tehnici subliminale fără ca persoanele să fie conștiente de acest lucru, pentru a denatura în mod semnificativ comportamentul unei persoane într-un mod care aduce sau poate aduce prejudicii fizice sau psihologice persoanei respective sau altei persoane;

(b) introducerea pe piață, punerea în funcțiune sau utilizarea unui sistem de IA care exploatează oricare dintre vulnerabilitățile unui anumit grup de persoane din cauza vârstei, a unui handicap fizic sau mental, pentru a denatura în mod semnificativ comportamentul unei persoane care aparține grupului respectiv

într-un mod care aduce sau poate aduce prejudicii fizice sau psihologice persoanei respective sau altei persoane;

(c) introducerea pe piață, punerea în funcțiune sau utilizarea sistemelor de IA de către autoritățile publice sau în numele acestora pentru evaluarea sau clasificarea credibilității persoanelor fizice într-o anumită perioadă de timp, pe baza comportamentului lor social sau a caracteristicilor personale sau de personalitate cunoscute sau preconizate, cu un punctaj privind comportamentul social care conduce la una dintre următoarele situații sau la ambele:

(i) tratamentul prejudiciabil sau nefavorabil al anumitor persoane fizice sau al unor grupuri întregi de persoane în contexte sociale care nu au legătură cu contextele în care datele au fost generate sau colectate inițial;

(ii) tratamentul prejudiciabil sau nefavorabil al anumitor persoane fizice sau al unor grupuri întregi de persoane care este nejustificat sau disproporționat în raport cu comportamentul social al acestora sau cu gravitatea acestuia;

(d) utilizarea sistemelor de identificare biometrică la distanță „în timp real" în spații accesibile publicului în scopul asigurării respectării legii, cu excepția cazului și în măsura în care o astfel de utilizare este strict necesară pentru unul dintre următoarele obiective:

(i) căutarea specifică a potențialelor victime ale infracționalității, inclusiv a copiilor dispăruți;

(ii) prevenirea unei amenințări specifice, substanțiale și iminente la adresa vieții sau a siguranței fizice a persoanelor fizice sau a unui atac terorist;

(iii) detectarea, localizarea, identificarea sau urmărirea penală a autorului unei infracțiuni sau a unei persoane suspectate de o infracțiune menționată la articolul 2 alineatul (2) din Decizia-cadru 2002/584/JAI a Consiliului[62] și pedepsită în statul membru în cauză cu o pedeapsă sau o măsură de siguranță privativă de libertate pentru o perioadă maximă de cel puțin trei ani, astfel cum este stabilit de legislația statului membru respectiv.

2. Utilizarea sistemelor de identificare biometrică la distanță „în timp real" în spațiile accesibile publicului în scopul asigurării respectării legii pentru oricare dintre obiectivele menționate la alineatul (1) litera (d) ține seama de următoarele elemente:

(a) natura situației care determină posibila utilizare, în special gravitatea, probabilitatea și amploarea prejudiciului cauzat în absența utilizării sistemului;

(b) consecințele utilizării sistemului asupra drepturilor și libertăților tuturor persoanelor vizate, în special gravitatea, probabilitatea și amploarea acestor consecințe.

În plus, utilizarea sistemelor de identificare biometrică la distanță „în timp real" în spațiile accesibile publicului în scopul asigurării respectării legii pentru oricare dintre obiectivele menționate la alineatul (1) litera (d) respectă garanțiile și condițiile

[62] Decizia-cadru 2002/584/JAI a Consiliului din 13 iunie 2002 privind mandatul european de arestare și procedurile de predare între statele membre (JO L 190, 18.7.2002, p. 1).

necesare și proporționale în ceea ce privește utilizarea, în special în ceea ce privește limitările temporale, geografice și personale.

3. În ceea ce privește alineatul (1) litera (d) și alineatul (2), fiecare utilizare individuală în scopul asigurării respectării legii a unui sistem de identificare biometrică la distanță „în timp real” în spațiile accesibile publicului face obiectul unei autorizări prealabile acordate de o autoritate judiciară sau de o autoritate administrativă independentă a statului membru în care urmează să aibă loc utilizarea, emisă pe baza unei cereri motivate și în conformitate cu normele detaliate de drept intern menționate la alineatul (4). Cu toate acestea, într-o situație de urgență justificată în mod corespunzător, utilizarea sistemului poate începe fără autorizație, iar autorizația poate fi solicitată numai în timpul utilizării sau ulterior.

   Autoritatea judiciară sau administrativă competentă acordă autorizația numai dacă este convinsă, pe baza unor dovezi obiective sau a unor indicii clare care i-au fost prezentate, că utilizarea sistemului de identificare biometrică la distanță „în timp real” în cauză este necesară și proporțională pentru realizarea unuia dintre obiectivele menționate la alineatul (1) litera (d), astfel cum au fost identificate în cerere. Atunci când ia o decizie cu privire la cerere, autoritatea judiciară sau administrativă competentă ia în considerare elementele menționate la alineatul (2).

4. Un stat membru poate decide să prevadă posibilitatea de a autoriza, integral sau parțial, utilizarea sistemelor de identificare biometrică la distanță „în timp real” în spațiile accesibile publicului în scopul asigurării respectării legii, în limitele și condițiile enumerate la alineatul (1) litera (d) și la alineatele (2) și (3). Statul membru respectiv stabilește în dreptul său intern normele detaliate necesare pentru solicitarea, eliberarea și exercitarea, precum și pentru supravegherea autorizațiilor menționate la alineatul (3). Normele respective specifică, de asemenea, pentru care dintre obiectivele enumerate la alineatul (1) litera (d), inclusiv pentru care dintre infracțiunile menționate la punctul (iii) din alineatul respectiv, pot fi autorizate autoritățile competente să utilizeze respectivele sisteme în scopul asigurării respectării legii.

TITLUL III

SISTEME DE IA CU GRAD RIDICAT DE RISC

CAPITOLUL 1

CLASIFICAREA SISTEMELOR DE IA CA PREZENTÂND UN RISC RIDICAT

Articolul 6

Norme de clasificare pentru sistemele de IA cu grad ridicat de risc

1. Indiferent dacă un sistem de IA este introdus pe piață sau pus în funcțiune independent de produsele menționate la literele (a) și (b), respectivul sistem de IA este considerat ca prezentând risc ridicat în cazul în care sunt îndeplinite cumulativ următoarele două condiții:

(a) sistemul de IA este destinat a fi utilizat ca o componentă de siguranță a unui produs sau este el însuși un produs care face obiectul legislației de armonizare a Uniunii enumerate în anexa II;

(b) produsul a cărui componentă de siguranță este sistemul de IA sau sistemul de IA în sine ca produs trebuie să fie supus unei evaluări a conformității de către o terță parte în vederea introducerii pe piață sau a punerii în funcțiune a produsului respectiv în temeiul legislației de armonizare a Uniunii enumerate în anexa II.

2. Pe lângă sistemele de IA cu grad ridicat de risc menționate la alineatul (1), sistemele de IA menționate în anexa III sunt considerate, de asemenea, sisteme cu grad ridicat de risc.

Articolul 7

Modificări aduse anexei III

1. Comisia este împuternicită să adopte acte delegate în conformitate cu articolul 73 pentru a actualiza lista din anexa III prin adăugarea de sisteme de IA cu grad ridicat de risc în cazul în care sunt îndeplinite cumulativ următoarele două condiții:

(a) sistemele de IA sunt destinate a fi utilizate în oricare dintre domeniile enumerate la punctele 1-8 din anexa III;

(b) sistemele de IA prezintă riscul de a aduce prejudicii sănătății și siguranței sau un risc de impact negativ asupra drepturilor fundamentale, și anume, în ceea ce privește gravitatea și probabilitatea de apariție, echivalent cu sau mai mare decât riscul de a aduce prejudicii sau de a provoca un impact negativ prezentat de sistemele de IA cu grad ridicat de risc deja menționate în anexa III.

2. Atunci când evaluează, în sensul alineatului (1), dacă un sistem de IA prezintă un risc de a aduce prejudicii sănătății și siguranței sau un risc de impact negativ asupra drepturilor fundamentale care este echivalent sau mai mare decât riscul de a aduce prejudicii prezentat de sistemele de IA cu grad ridicat de risc deja menționate în anexa III, Comisia ia în considerare următoarele criterii:

(a) scopul preconizat al sistemului de IA;

(b) măsura în care a fost utilizat sau este probabil să fie utilizat un sistem de IA;

(c) măsura în care utilizarea unui sistem de IA a adus deja prejudicii sănătății și siguranței sau a avut un impact negativ asupra drepturilor fundamentale sau a generat motive de îngrijorare semnificative în ceea ce privește materializarea unor astfel de prejudicii sau a unui astfel de impact negativ, astfel cum o demonstrează rapoartele sau acuzațiile documentate prezentate autorităților naționale competente;

(d) amploarea potențială a unor astfel de prejudicii sau a unui astfel de impact negativ, în special în ceea ce privește intensitatea și capacitatea sa de a afecta un număr mare de persoane;

(e) măsura în care persoanele potențial prejudiciate sau afectate de un impact negativ depind de rezultatul produs cu ajutorul unui sistem de IA, în special deoarece, din motive practice sau juridice, nu este posibil în mod rezonabil să se renunțe la rezultatul respectiv;

(f) măsura în care persoanele potențial prejudiciate sau afectate de impactul negativ se află într-o poziție vulnerabilă în raport cu utilizatorul unui sistem de IA, în special din cauza unui dezechilibru de putere, de cunoștințe, de circumstanțe economice sau sociale sau de vârstă;

(g) măsura în care rezultatul produs cu ajutorul unui sistem de IA este ușor reversibil, iar rezultatele care au un impact asupra sănătății sau siguranței persoanelor nu sunt considerate ca fiind ușor reversibile;

(h) măsura în care legislația existentă a Uniunii prevede:

(i) măsuri reparatorii eficace în legătură cu riscurile prezentate de un sistem de IA, cu excepția cererilor de despăgubiri;

(ii) măsuri eficace de prevenire sau de reducere substanțială a acestor riscuri.

CAPITOLUL 2

CERINȚE PENTRU SISTEMELE DE AI CU GRAD RIDICAT DE RISC

Articolul 8

Respectarea cerințelor

1. Sistemele de IA cu grad ridicat de risc respectă cerințele stabilite în prezentul capitol.

2. Scopul preconizat al sistemului de IA cu grad ridicat de risc și al sistemului de gestionare a riscurilor menționate la articolul 9 este luat în considerare atunci când se asigură conformitatea cu cerințele respective.

Articolul 9

Sistemul de gestionare a riscurilor

1. Se instituie, se pune în aplicare, se documentează și se menține un sistem de gestionare a riscurilor în legătură cu sistemele de IA cu grad ridicat de risc.

2. Sistemul de gestionare a riscurilor constă într-un proces iterativ continuu desfășurat pe parcursul întregului ciclu de viață al unui sistem de IA cu grad ridicat de risc, necesitând o actualizare sistematică periodică. Acesta cuprinde următoarele etape:

(a) identificarea și analiza riscurilor cunoscute și previzibile asociate fiecărui sistem de IA cu grad ridicat de risc;

(b) estimarea și evaluarea riscurilor care pot apărea atunci când sistemul de IA cu grad ridicat de risc este utilizat în conformitate cu scopul preconizat și în condiții de utilizare necorespunzătoare previzibile în mod rezonabil;

(c) evaluarea altor riscuri care ar putea apărea pe baza analizei datelor colectate din sistemul de monitorizare ulterioară introducerii pe piață menționat la articolul 61;

(d) adoptarea unor măsuri adecvate de gestionare a riscurilor în conformitate cu dispozițiile alineatelor următoare.

3. Măsurile de gestionare a riscurilor menționate la alineatul (2) litera (d) țin seama în mod corespunzător de efectele și interacțiunile posibile care rezultă din aplicarea

combinată a cerințelor prevăzute în prezentul capitol 2. Acestea țin seama de stadiul actual al tehnologiei general recunoscut, inclusiv astfel cum se reflectă în normele armonizate sau în specificațiile comune relevante.

4. Măsurile de gestionare a riscurilor menționate la alineatul (2) litera (d) sunt de așa natură încât orice risc rezidual asociat fiecărui pericol, precum și riscul rezidual global al sistemelor de IA cu grad ridicat de risc să fie considerate acceptabile, cu condiția ca sistemul de IA cu grad ridicat de risc să fie utilizat în conformitate cu scopul preconizat sau în condiții de utilizare necorespunzătoare previzibile în mod rezonabil. Riscurile reziduale respective se comunică utilizatorului.

   La identificarea celor mai adecvate măsuri de gestionare a riscurilor se asigură următoarele:

   (a) eliminarea sau reducerea riscurilor pe cât posibil prin proiectare și dezvoltare adecvate;

   (b) după caz, punerea în aplicare a unor măsuri adecvate de atenuare și control în ceea ce privește riscurile care nu pot fi eliminate;

   (c) furnizarea de informații adecvate în temeiul articolului 13, în special în ceea ce privește riscurile menționate la alineatul (2) litera (b) din prezentul articol și, după caz, formarea utilizatorilor.

   La eliminarea sau reducerea riscurilor legate de utilizarea sistemului de IA cu grad ridicat de risc se acordă atenția cuvenită cunoștințelor tehnice, experienței, educației, formării pe care le preconizează utilizatorul și conforme cu mediul în care urmează să fie utilizat sistemul.

5. Sistemele de IA cu grad ridicat de risc sunt testate în scopul identificării celor mai adecvate măsuri de gestionare a riscurilor. Testarea asigură faptul că sistemele de IA cu grad ridicat de risc funcționează în mod consecvent în scopul preconizat și sunt conforme cu cerințele stabilite în prezentul capitol.

6. Procedurile de testare sunt adecvate pentru a atinge scopul preconizat al sistemului de IA și nu trebuie să depășească ceea ce este necesar pentru atingerea scopului respectiv.

7. Testarea sistemelor de IA cu grad ridicat de risc se efectuează, după caz, în orice moment pe parcursul procesului de dezvoltare și, în orice caz, înainte de introducerea pe piață sau de punerea în funcțiune. Testarea se efectuează pe baza unor indicatori și a unor praguri probabilistice definite în prealabil, care sunt adecvate scopului preconizat al sistemului de IA cu grad ridicat de risc.

8. La punerea în aplicare a sistemului de gestionare a riscurilor descris la alineatele (1) – (7), se acordă o atenție deosebită posibilității ca sistemul de IA cu grad ridicat de risc să fie accesat de copii sau să aibă un impact asupra acestora.

9. În cazul instituțiilor de credit reglementate de Directiva 2013/36/UE, aspectele descrise la alineatele (1) – (8) fac parte din procedurile de gestionare a riscurilor stabilite de instituțiile respective în temeiul articolului 74 din directiva respectivă.

Articolul 10

Datele și guvernanța datelor

1. Sistemele de IA cu grad ridicat de risc care utilizează tehnici ce implică antrenarea de modele cu date sunt dezvoltate pe baza unor seturi de date de antrenament, de validare și de testare care îndeplinesc criteriile de calitate menționate la alineatele (2) – (5).

2. Seturile de date de antrenament, de validare și de testare fac obiectul unor practici adecvate de guvernanță și gestionare a datelor. Practicile respective se referă în special la:

   (a) opțiunile de proiectare relevante;

   (b) colectarea datelor;

   (c) operațiunile relevante de prelucrare a datelor, cum ar fi adnotarea, etichetarea, curățarea, îmbogățirea și agregarea;

   (d) formularea unor ipoteze relevante, în special în ceea ce privește informațiile pe care datele ar trebui să le măsoare și să le reprezinte;

   (e) o evaluare prealabilă a disponibilității, a cantității și a adecvării seturilor de date necesare;

   (f) examinarea în vederea identificării unor posibile părtiniri;

   (g) identificarea eventualelor lacune sau deficiențe în materie de date și a modului în care acestea pot fi abordate.

3. Seturile de date de antrenament, de validare și de testare trebuie să fie relevante, reprezentative, fără erori și complete. Acestea au proprietățile statistice corespunzătoare, inclusiv, după caz, în ceea ce privește persoanele sau grupurile de persoane în legătură cu care se intenționează să fie utilizat sistemul de IA cu grad ridicat de risc. Aceste caracteristici ale seturilor de date pot fi îndeplinite la nivelul seturilor de date individuale sau al unei combinații a acestora.

4. Seturile de date de antrenament, de validare și de testare iau în considerare, în măsura impusă de scopul preconizat, caracteristicile sau elementele specifice cadrului geografic, comportamental sau funcțional specific în care este destinat să fie utilizat sistemul de IA cu grad ridicat de risc.

5. În măsura în care acest lucru este strict necesar pentru a asigura monitorizarea, detectarea și corectarea erorilor sistematice în legătură cu sistemele de IA cu grad ridicat de risc, furnizorii de astfel de sisteme pot prelucra categoriile speciale de date cu caracter personal_menționate la articolul 9 alineatul (1) din Regulamentul (UE) 2016/679, la articolul 10 din Directiva (UE) 2016/680 și la articolul 10 alineatul (1) din Regulamentul (UE) 2018/1725, sub rezerva unor garanții adecvate pentru drepturile și libertățile fundamentale ale persoanelor fizice, inclusiv pentru limitările tehnice privind reutilizarea și utilizarea măsurilor de securitate și de protejare a vieții private de ultimă generație, cum ar fi pseudonimizarea, sau criptarea în cazul în care anonimizarea poate afecta în mod semnificativ scopul urmărit.

6. Pentru dezvoltarea unor sisteme de IA cu grad ridicat de risc, altele decât cele care utilizează tehnici ce implică antrenarea de modele, se aplică practici adecvate de guvernanță și de gestionare a datelor, pentru a se asigura conformitatea acestor sisteme de IA cu grad ridicat de risc cu alineatul (2).

Articolul 11

Documentația tehnică

1. Documentația tehnică a unui sistem de IA cu grad ridicat de risc se întocmește înainte ca sistemul respectiv să fie introdus pe piață sau pus în funcțiune și se actualizează.

   Documentația tehnică se întocmește astfel încât să demonstreze că sistemul de IA cu grad ridicat de risc respectă cerințele prevăzute în prezentul capitol și să furnizeze autorităților naționale competente și organismelor notificate toate informațiile necesare pentru a evalua conformitatea sistemului de IA cu cerințele respective. Aceasta conține cel puțin elementele prevăzute în anexa IV.

2. În cazul în care un sistem de IA cu grad ridicat de risc legat de un produs, căruia i se aplică actele juridice enumerate în anexa II secțiunea A, este introdus pe piață sau pus în funcțiune, se întocmește o singură documentație tehnică ce conține toate informațiile prevăzute în anexa IV, precum și informațiile solicitate în temeiul respectivelor acte juridice.

3. Comisia este împuternicită să adopte acte delegate în conformitate cu articolul 73 pentru a modifica anexa IV atunci când este necesar, pentru a se asigura că, având în vedere progresul tehnic, documentația tehnică furnizează toate informațiile necesare pentru evaluarea conformității sistemului cu cerințele prevăzute în prezentul capitol.

Articolul 12

Păstrarea evidențelor

1. Sistemele de IA cu grad ridicat de risc sunt proiectate și dezvoltate cu capacități care permit înregistrarea automată a evenimentelor („fișiere de jurnalizare”) în timpul funcționării sistemelor de IA cu grad ridicat de risc. Aceste capacități de jurnalizare sunt conforme cu standardele recunoscute sau cu specificațiile comune.

2. Capacitățile de jurnalizare asigură un nivel de trasabilitate a funcționării sistemului de IA pe parcursul întregului său ciclu de viață, care este adecvat scopului preconizat al sistemului.

3. În special, capacitățile de jurnalizare permit monitorizarea funcționării sistemului de IA cu grad ridicat de risc în ceea ce privește apariția situațiilor care pot avea ca rezultat un sistem de IA care prezintă un risc în sensul articolului 65 alineatul (1) sau care pot conduce la o modificare substanțială, și facilitează monitorizarea ulterioară introducerii pe piață menționată la articolul 61.

4. În cazul sistemelor de IA cu grad ridicat de risc menționate în anexa III punctul1 litera (a), capacitățile de jurnalizare asigură cel puțin:

   (a) înregistrarea perioadei fiecărei utilizări a sistemului (data și ora de începere, precum și data și ora de încheiere a fiecărei utilizări);

   (b) baza de date de referință cu care au fost verificate de sistem datele de intrare;

   (c) datele de intrare pentru care căutarea a generat o concordanță;

   (d) identificarea persoanelor fizice implicate în verificarea rezultatelor, astfel cum se menționează la articolul 14 alineatul (5).

Articolul 13

Transparența și furnizarea de informații utilizatorilor

1. Sistemele de IA cu grad ridicat de risc sunt proiectate și dezvoltate astfel încât să se asigure că funcționarea lor este suficient de transparentă pentru a permite utilizatorilor să interpreteze rezultatele sistemului și să le utilizeze în mod corespunzător. Se asigură un tip și un grad adecvat de transparență, în vederea respectării obligațiilor relevante ale utilizatorului și ale furnizorului prevăzute în capitolul 3 din prezentul titlu.

2. Sistemele de IA cu grad ridicat de risc sunt însoțite de instrucțiuni de utilizare într-un format digital adecvat sau în alte moduri, care includ informații concise, complete, corecte și clare care sunt relevante, accesibile și ușor de înțeles pentru utilizatori.

3. Informațiile menționate la alineatul (2) precizează:

   (a) identitatea și datele de contact ale furnizorului și, după caz, ale reprezentantului său autorizat;

   (b) caracteristicile, capacitățile și limitările performanței sistemului de IA cu grad ridicat de risc, inclusiv:

      (i) scopul său preconizat;

      (ii) nivelul de acuratețe, robustețe și securitate cibernetică menționat la articolul 15 în raport cu care sistemul de IA cu grad ridicat de risc a fost testat și validat și care poate fi preconizat, precum și orice circumstanță cunoscută și previzibilă care ar putea avea un impact asupra nivelului preconizat de acuratețe, robustețe și securitate cibernetică;

      (iii) orice circumstanță cunoscută sau previzibilă legată de utilizarea sistemului de IA cu grad ridicat de risc în conformitate cu scopul preconizat sau în condiții de utilizare necorespunzătoare previzibile în mod rezonabil, care poate conduce la riscuri pentru sănătate și siguranță sau pentru drepturile fundamentale;

      (iv) performanța sa în ceea ce privește persoanele sau grupurile de persoane în legătură cu care urmează să fie utilizat sistemul;

      (v) după caz, specificațiile pentru datele de intrare sau orice altă informație relevantă în ceea ce privește seturile de date de antrenament, de validare și de testare utilizate, ținând seama de scopul preconizat al sistemului de IA.

   (c) modificările aduse sistemului de IA cu grad ridicat de risc și performanței acestuia care au fost predeterminate de către furnizor la momentul evaluării inițiale a conformității, dacă este cazul;

   (d) măsurile de supraveghere umană menționate la articolul 14, inclusiv măsurile tehnice instituite pentru a facilita interpretarea rezultatelor sistemelor de IA de către utilizatori;

   (e) durata de viață preconizată a sistemului de IA cu grad ridicat de risc și orice măsură de întreținere și de îngrijire necesară pentru a asigura funcționarea corespunzătoare a sistemului de IA respectiv, inclusiv în ceea ce privește actualizările software-ului.

Articolul 14

Supravegherea umană

1. Sistemele de IA cu grad ridicat de risc sunt proiectate și dezvoltate astfel încât, inclusiv cu instrumente adecvate de interfață om-mașină, să poată fi supravegheate în mod eficace de către persoanele fizice în perioada în care este utilizat sistemul de IA.

2. Supravegherea umană are ca scop prevenirea sau reducerea la minimum a riscurilor pentru sănătate, siguranță sau pentru drepturile fundamentale, care pot apărea atunci când un sistem de IA cu grad ridicat de risc este utilizat în conformitate cu scopul său preconizat sau în condiții de utilizare necorespunzătoare previzibile în mod rezonabil, în special atunci când astfel de riscuri persistă în pofida aplicării altor cerințe prevăzute în prezentul capitol.

3. Supravegherea umană se asigură prin una dintre sau prin toate următoarele măsuri:

   (a) identificate și încorporate, atunci când este fezabil din punct de vedere tehnic, în sistemul de IA cu grad ridicat de risc de către furnizor înainte ca acesta să fie introdus pe piață sau pus în funcțiune;

   (b) identificate de furnizor înainte de introducerea pe piață sau punerea în funcțiune a sistemului de IA cu grad ridicat de risc și care sunt adecvate pentru a fi puse în aplicare de utilizator.

4. Măsurile menționate la alineatul (3) permit persoanelor cărora li se încredințează supravegherea umană următoarele acțiuni, în funcție de circumstanțe:

   (a) să înțeleagă pe deplin capacitățile și limitările sistemului de IA cu grad ridicat de risc și să fie în măsură să monitorizeze în mod corespunzător funcționarea acestuia, astfel încât semnele de anomalii, disfuncționalități și performanțe neașteptate să poată fi detectate și abordate cât mai curând posibil;

   (b) să rămână conștiente de posibila tendință de a se baza în mod automat sau excesiv pe rezultatele obținute de un sistem de IA cu grad ridicat de risc („părtinire legată de automatizare”), în special în cazul sistemelor de IA cu grad ridicat de risc utilizate pentru a furniza informații sau recomandări pentru decizii care urmează să fie luate de persoanele fizice;

   (c) să poată interpreta în mod corect rezultatele sistemului de IA cu grad ridicat de risc, ținând seama în special de caracteristicile sistemului și de instrumentele și metodele de interpretare disponibile;

   (d) să poată să decidă, în orice situație specială, să nu utilizeze sistemul de IA cu grad ridicat de risc sau să ignore, să anuleze sau să inverseze rezultatele sistemului de IA cu grad ridicat de risc;

   (e) să poată interveni în funcționarea sistemului de IA cu grad ridicat de risc sau să întrerupă sistemul prin intermediul unui buton „stop” sau al unei proceduri similare.

5. În cazul sistemelor de IA cu grad ridicat de risc menționate în anexa III punctul 1 litera (a), măsurile menționate la alineatul (3) sunt de așa natură încât să asigure că, în plus, utilizatorul nu ia nicio măsură sau decizie pe baza identificării care rezultă din sistem, cu excepția cazului în care acest lucru a fost verificat și confirmat de cel puțin două persoane fizice.

Articolul 15

Acuratețe, robustețe și securitate cibernetică

1. Sistemele de IA cu grad ridicat de risc sunt concepute și dezvoltate astfel încât, având în vedere scopul lor preconizat, să atingă un nivel adecvat de acuratețe, robustețe și securitate cibernetică și să funcționeze în mod consecvent în aceste privințe pe parcursul întregului lor ciclu de viață.

2. Nivelurile de acuratețe și indicatorii de precizie relevanți ai sistemelor de IA cu grad ridicat de risc se declară în instrucțiunile de utilizare aferente.

3. Sistemele de IA cu grad ridicat de risc sunt reziliente în ceea ce privește erorile, defecțiunile sau incoerențele care pot apărea în cadrul sistemului sau în mediul în care funcționează sistemul, în special din cauza interacțiunii lor cu persoane fizice sau cu alte sisteme.

   Robustețea sistemelor de IA cu grad ridicat de risc poate fi asigurată prin soluții tehnice redundante, care pot include planuri de rezervă sau de autoprotecție.

   Sistemele de IA cu grad ridicat de risc care continuă să învețe după ce au fost introduse pe piață sau puse în funcțiune sunt dezvoltate astfel încât să se asigure că eventualele rezultate părtinitoare din cauza rezultatelor utilizate ca date de intrare pentru operațiunile viitoare („bucle de feedback”) sunt abordate în mod corespunzător prin măsuri de atenuare adecvate.

4. Sistemele de IA cu grad ridicat de risc sunt reziliente în ceea ce privește încercările unor părți terțe neautorizate de a le modifica utilizarea sau performanța prin exploatarea vulnerabilităților sistemului.

   Soluțiile tehnice menite să asigure securitatea cibernetică a sistemelor de IA cu grad ridicat de risc sunt adecvate circumstanțelor și riscurilor relevante.

   Soluțiile tehnice pentru abordarea vulnerabilităților specifice ale IA includ, după caz, măsuri de prevenire și control al atacurilor ce vizează manipularea setului de date de antrenament („data poisoning”), date de intrare concepute să determine modelul să facă o greșeală („exemple contradictorii”) sau defecte ale modelului.

CAPITOLUL 3

OBLIGAȚIILE FURNIZORILOR ȘI UTILIZATORILOR DE SISTEME DE IA CU GRAD RIDICAT DE RISC ȘI ALE ALTOR PĂRȚI

Articolul 16

Obligațiile furnizorilor de sisteme de IA cu grad ridicat de risc

Furnizorii de sisteme de IA cu grad ridicat de risc:

(a) se asigură că sistemele lor de IA cu grad ridicat de risc respectă cerințele prevăzute în capitolul 2 din prezentul titlu;

(b) dispun de un sistem de management al calității în conformitate cu articolul 17;

(c) întocmesc documentația tehnică a sistemului de IA cu grad ridicat de risc;

(d) atunci când acest lucru este sub controlul lor, păstrează fișierele de jurnalizare generate automat de sistemele lor de IA cu grad ridicat de risc;

(e) se asigură că sistemul de IA cu grad ridicat de risc este supus procedurii relevante de evaluare a conformității, înainte de introducerea sa pe piață sau de punerea sa în funcțiune;

(f) respectă obligațiile de înregistrare menționate la articolul 51;

(g) iau măsurile corective necesare, în cazul în care sistemul de IA cu grad ridicat de risc nu este în conformitate cu cerințele stabilite în capitolul 2 din prezentul titlu;

(h) informează autoritățile naționale competente ale statelor membre în care au pus la dispoziție sau au pus în funcțiune sistemul de IA și, după caz, organismul notificat cu privire la neconformitate și la orice măsură corectivă luată;

(i) aplică marcajul CE pe sistemele lor de IA cu risc ridicat pentru a indica conformitatea cu prezentul regulament în conformitate cu articolul 49;

(j) la cererea unei autorități naționale competente, demonstrează conformitatea sistemului de IA cu grad ridicat de risc cu cerințele prevăzute în capitolul 2 din prezentul titlu.

Articolul 17

Sistemul de management al calității

1. Furnizorii de sisteme de IA cu grad ridicat de risc instituie un sistem de management al calității care asigură conformitatea cu prezentul regulament. Acest sistem este documentat în mod sistematic și ordonat sub formă de politici, proceduri și instrucțiuni scrise și include cel puțin următoarele aspecte:

   (a) o strategie pentru conformitatea cu reglementările, inclusiv conformitatea cu procedurile de evaluare a conformității și cu procedurile de gestionare a modificărilor aduse sistemului de IA cu grad ridicat de risc;

   (b) tehnicile, procedurile și acțiunile sistematice care urmează să fie utilizate pentru proiectarea, controlul proiectării și verificarea proiectării sistemului de IA cu grad ridicat de risc;

   (c) tehnicile, procedurile și acțiunile sistematice care urmează să fie utilizate pentru dezvoltarea, controlul calității și asigurarea calității sistemului de IA cu grad ridicat de risc;

   (d) procedurile de examinare, testare și validare care trebuie efectuate înainte, în timpul și după dezvoltarea sistemului de IA cu grad ridicat de risc, precum și frecvența cu care acestea trebuie efectuate;

   (e) specificațiile tehnice, inclusiv standardele, care urmează să fie aplicate și, în cazul în care normele armonizate relevante nu sunt aplicate integral, mijloacele care trebuie utilizate pentru a se asigura că sistemul de IA cu grad ridicat de risc respectă cerințele prevăzute în capitolul 2 din prezentul titlu;

   (f) sisteme și proceduri pentru gestionarea datelor, inclusiv colectarea datelor, analiza datelor, etichetarea datelor, stocarea datelor, filtrarea datelor, extragerea datelor, agregarea datelor, păstrarea datelor și orice altă operațiune privind datele care este efectuată înainte și în scopul introducerii pe piață sau al punerii în funcțiune a sistemelor de IA cu grad ridicat de risc;

   (g) sistemul de gestionare a riscurilor menționat la articolul 9;

(h) înființarea, implementarea și întreținerea unui sistem de monitorizare ulterioară introducerii pe piață în conformitate cu articolul 61;

(i) procedurile legate de raportarea incidentelor grave și a funcționării defectuoase în conformitate cu articolul 62;

(j) gestionarea comunicării cu autoritățile naționale competente, cu autoritățile competente, inclusiv cu cele sectoriale, care furnizează sau sprijină accesul la date, cu organismele notificate, cu alți operatori, cu clienți sau cu alte părți interesate;

(k) sisteme și proceduri pentru păstrarea evidențelor tuturor documentelor și informațiilor relevante;

(l) gestionarea resurselor, inclusiv măsurile legate de securitatea aprovizionării;

(m) un cadru de asigurare a răspunderii care stabilește responsabilitățile cadrelor de conducere și ale altor categorii de personal în ceea ce privește toate aspectele enumerate la prezentul alineat.

2. Punerea în aplicare a aspectelor menționate la alineatul (1) este proporțională cu dimensiunea organizației furnizorului.

3. În cazul furnizorilor care sunt instituții de credit reglementate prin Directiva 2013/36/UE, se consideră că obligația de a institui un sistem de management al calității este îndeplinită prin respectarea normelor privind măsurile, procesele și mecanismele de guvernanță internă prevăzute la articolul 74 din directiva respectivă. În acest context, se ține seama de toate normele armonizate menționate la articolul 40 din prezentul regulament.

Articolul 18

Obligația de a întocmi documentația tehnică

1. Furnizorii de sisteme de IA cu grad ridicat de risc întocmesc documentația tehnică menționată la articolul 11 în conformitate cu anexa IV.

2. Furnizorii care sunt instituții de credit reglementate de Directiva 2013/36/UE păstrează documentația tehnică ca parte a documentației privind guvernanța internă, modalitățile, procesele și mecanismele interne, în conformitate cu articolul 74 din directiva respectivă.

Articolul 19

Evaluarea conformității

1. Furnizorii de sisteme de IA cu grad ridicat de risc se asigură că sistemele lor sunt supuse procedurii relevante de evaluare a conformității potrivit articolului 43, înainte de introducerea lor pe piață sau de punerea lor în funcțiune. În cazul în care conformitatea sistemelor de IA cu cerințele prevăzute în capitolul 2 din prezentul titlu a fost demonstrată în urma respectivei evaluări a conformității, furnizorii întocmesc o declarație de conformitate UE potrivit articolului 48 și aplică marcajul CE de conformitate potrivit articolului 49.

2. Pentru sistemele de IA cu grad ridicat de risc menționate la punctul 5 litera (b) din anexa III care sunt introduse pe piață sau puse în funcțiune de furnizori care sunt

instituții de credit reglementate de Directiva 2013/36/UE, evaluarea conformității se efectuează în cadrul procedurii menționate la articolele 97-101 din directiva respectivă.

Articolul 20

Fișiere de jurnalizare generate automat

1. Furnizorii de sisteme de IA cu grad ridicat de risc păstrează fișierele de jurnalizare generate automat de sistemele lor de IA cu grad ridicat de risc, în măsura în care astfel de fișiere de jurnalizare se află sub controlul lor în temeiul unui acord contractual cu utilizatorul sau în alt mod în temeiul legii. Fișierele de jurnalizare se păstrează pentru o perioadă adecvată având în vedere scopul preconizat al sistemului de IA cu grad ridicat de risc și obligațiile legale aplicabile în temeiul dreptului Uniunii sau al dreptului intern.
2. Furnizorii care sunt instituții de credit reglementate de Directiva 2013/36/UE păstrează fișierele de jurnalizare generate automat de sistemele lor de IA cu grad ridicat de risc ca parte a documentației prevăzute la articolul 74 din directiva respectivă.

Articolul 21

Acțiuni corective

Furnizorii de sisteme de IA cu grad ridicat de risc care consideră sau au motive să considere că un sistem de IA cu grad ridicat de risc pe care l-au introdus pe piață ori pe care l-au pus în funcțiune nu este în conformitate cu prezentul regulament întreprind imediat acțiunile corective necesare pentru ca sistemul să fie adus în conformitate sau să fie retras sau rechemat, după caz. Aceștia informează în acest sens distribuitorii sistemului de IA cu grad ridicat de risc respectiv și, dacă este cazul, reprezentantul autorizat și importatorii.

Articolul 22

Obligația de informare

În cazul în care sistemul de IA cu grad ridicat de risc prezintă un risc în sensul articolului 65 alineatul (1), iar riscul respectiv este cunoscut de furnizorul sistemului, furnizorul respectiv informează imediat autoritățile naționale competente din statele membre în care a pus la dispoziție sistemul și, după caz, organismul notificat care a eliberat un certificat pentru sistemul de IA cu grad ridicat de risc, în special cu privire la neconformitate și la orice acțiune corectivă întreprinsă.

Articolul 23

Cooperarea cu autoritățile competente

La cererea unei autorități naționale competente, furnizorii de sisteme de IA cu grad ridicat de risc furnizează autorității respective toate informațiile și documentația necesară pentru a demonstra conformitatea sistemului de IA cu grad ridicat de risc cu cerințele prevăzute în capitolul 2 din prezentul titlu, într-o limbă oficială a Uniunii stabilită de statul membru în cauză. Pe baza unei cereri motivate a unei autorități naționale competente, furnizorii oferă, de

asemenea, autorității respective acces la fișierele de jurnalizare generate automat de sistemul de IA cu grad ridicat de risc, în măsura în care astfel de fișiere de jurnalizare se află sub controlul lor în temeiul unui acord contractual cu utilizatorul sau în alt mod în temeiul legii.

Articolul 24

Obligațiile fabricanților de produse

În cazul în care un sistem de IA cu grad ridicat de risc asociat unor produse cărora li se aplică actele juridice enumerate în anexa II secțiunea A este introdus pe piață sau pus în funcțiune împreună cu produsul fabricat în conformitate cu actele juridice respective și sub denumirea fabricantului produsului, acesta din urmă își asumă responsabilitatea pentru conformitatea sistemului de IA cu prezentul regulament și, în ceea ce privește sistemul de IA, are aceleași obligații cu cele impuse furnizorului prin prezentul regulament.

Articolul 25

Reprezentanți autorizați

1. Înainte de a-și pune la dispoziție sistemele pe piața Uniunii, în cazul în care un importator nu poate fi identificat, furnizorii stabiliți în afara Uniunii desemnează, prin mandat scris, un reprezentant autorizat stabilit în Uniune.

2. Reprezentantul autorizat îndeplinește sarcinile prevăzute în mandatul primit de la furnizor. Mandatul autorizează reprezentantul autorizat să îndeplinească următoarele sarcini:

   (a) să păstreze o copie a declarației de conformitate UE și a documentației tehnice la dispoziția autorităților naționale competente și a autorităților naționale menționate la articolul 63 alineatul (7);

   (b) să furnizeze unei autorități naționale competente, pe baza unei cereri motivate, toate informațiile și documentele necesare pentru a demonstra conformitatea unui sistem de IA cu grad ridicat de risc cu cerințele prevăzute în capitolul 2 din prezentul titlu, inclusiv accesul la fișierele de jurnalizare generate automat de sistemul de IA cu grad ridicat de risc, în măsura în care aceste fișiere de jurnalizare se află sub controlul furnizorului în temeiul unui acord contractual cu utilizatorul sau în alt mod în temeiul legii;

   (c) să coopereze cu autoritățile naționale competente, pe baza unei cereri motivate, cu privire la orice acțiune întreprinsă de acestea din urmă în legătură cu sistemul de IA cu grad ridicat de risc.

Articolul 26

Obligațiile importatorilor

1. Înainte de introducerea pe piață a unui sistem de IA cu grad ridicat de risc, importatorii unui astfel de sistem se asigură că:

   (a) procedura corespunzătoare de evaluare a conformității a fost efectuată de furnizorul sistemului de IA respectiv;

   (b) furnizorul a întocmit documentația tehnică în conformitate cu anexa IV;

(c) sistemul poartă marcajul de conformitate necesar și este însoțit de documentația și instrucțiunile de utilizare necesare.

2. În cazul în care un importator consideră sau are motive să considere că un sistem de IA cu grad ridicat de risc nu este în conformitate cu prezentul regulament, acesta nu introduce sistemul respectiv pe piață înainte ca sistemul de IA respectiv să devină conform. În cazul în care sistemul de IA cu grad ridicat de risc prezintă un risc în sensul articolului 65 alineatul (1), importatorul informează în acest sens furnizorul sistemului de IA și autoritățile de supraveghere a pieței.

3. Importatorii indică pe sistemul de IA cu grad ridicat de risc numele lor, denumirea lor comercială înregistrată sau marca lor înregistrată și adresa la care pot fi contactați sau, dacă acest lucru nu este posibil, pe ambalaj sau în documentele care îl însoțesc, după caz.

4. Importatorii se asigură că, pe întreaga perioadă în care un sistem de IA cu grad ridicat de risc se află în responsabilitatea lor, după caz, condițiile de depozitare sau de transport nu periclitează conformitatea sa cu cerințele prevăzute în capitolul 2 din prezentul titlu.

5. Importatorii furnizează autorităților naționale competente, pe baza unei cereri motivate, toate informațiile și documentația necesare pentru a demonstra conformitatea unui sistem de IA cu grad ridicat de risc cu cerințele prevăzute în capitolul 2 din prezentul titlu, într-o limbă care poate fi ușor înțeleasă de autoritatea națională competentă respectivă, inclusiv accesul la fișierele de jurnalizare generate automat de sistemul de IA cu grad ridicat de risc, în măsura în care aceste fișiere de jurnalizare se află sub controlul furnizorului în temeiul unui acord contractual cu utilizatorul sau în alt mod în temeiul legii. De asemenea, aceștia cooperează cu autoritățile respective cu privire la orice acțiune întreprinsă de autoritatea națională competentă în legătură cu sistemul respectiv.

Articolul 27

Obligațiile distribuitorilor

1. Înainte de a pune la dispoziție pe piață un sistem de IA cu grad ridicat de risc, distribuitorii verifică dacă sistemul de IA cu grad ridicat de risc poartă marcajul CE de conformitate necesar, dacă este însoțit de documentația și instrucțiunile de utilizare necesare și dacă furnizorul și importatorul sistemului, după caz, au respectat obligațiile prevăzute în prezentul regulament.

2. În cazul în care un distribuitor consideră sau are motive să considere că un sistem de IA cu grad ridicat de risc nu este în conformitate cu cerințele prevăzute în capitolul 2 din prezentul titlu, acesta nu pune la dispoziție pe piață sistemul de IA cu grad ridicat de risc înainte ca sistemul respectiv să fie adus în conformitate cu cerințele respective. În plus, în cazul în care sistemul prezintă un risc în sensul articolului 65 alineatul (1), distribuitorul informează furnizorul sau importatorul sistemului, după caz, în acest sens.

3. Distribuitorii se asigură că, atât timp cât un sistem de IA cu grad ridicat de risc se află în responsabilitatea lor, după caz, condițiile de depozitare sau de transport nu periclitează conformitatea sistemului cu cerințele prevăzute în capitolul 2 din prezentul titlu.

4. Un distribuitor care consideră sau are motive să considere că un sistem de IA cu grad ridicat de risc pe care l-a pus la dispoziție pe piață nu este în conformitate cu cerințele prevăzute în capitolul 2 din prezentul titlu ia măsurile corective necesare pentru a aduce sistemul în conformitate cu cerințele respective, pentru a-l retrage sau pentru a-l rechema sau se asigură că furnizorul, importatorul sau orice operator relevant, după caz, ia măsurile corective respective. În cazul în care sistemul de IA cu grad ridicat de risc prezintă un risc în sensul articolului 65 alineatul (1), distribuitorul informează imediat în acest sens autoritățile naționale competente din statele membre în care a pus la dispoziție pe piață produsul, indicând detaliile, în special cu privire la neconformitate și la orice măsură corectivă luată.

5. Pe baza unei cereri motivate a unei autorități naționale competente, distribuitorii de sisteme de IA cu grad ridicat de risc furnizează autorității respective toate informațiile și documentația necesare pentru a demonstra conformitatea unui sistem cu risc ridicat cu cerințele prevăzute în capitolul 2 din prezentul titlu. Distribuitorii cooperează, de asemenea, cu autoritatea națională competentă respectivă cu privire la orice acțiune întreprinsă de autoritatea respectivă.

Articolul 28

Obligațiile distribuitorilor, importatorilor, utilizatorilor sau ale oricărei alte părți terțe

1. Se consideră că orice distribuitor, importator, utilizator sau altă parte terță este furnizor în sensul prezentului regulament și este supus obligațiilor care revin furnizorului în temeiul articolului 16, în oricare dintre următoarele situații:

   (a) introduc pe piață sau pun în funcțiune un sistem de IA cu grad ridicat de risc sub denumirea sau marca lor comercială;

   (b) modifică scopul preconizat al unui sistem de IA cu grad ridicat de risc deja introdus pe piață sau pus în funcțiune;

   (c) aduc o modificare substanțială sistemului de IA cu grad ridicat de risc.

2. În cazul în care se produc circumstanțele menționate la alineatul (1) litera (b) sau (c), furnizorul care a introdus inițial pe piață sau a pus în funcțiune sistemul de IA cu grad ridicat de risc nu mai este considerat furnizor în sensul prezentului regulament.

Articolul 29

Obligațiile utilizatorilor de sisteme de IA cu grad ridicat de risc

1. Utilizatorii sistemelor de IA cu grad ridicat de risc utilizează astfel de sisteme în conformitate cu instrucțiunile de utilizare care însoțesc sistemele, în temeiul alineatelor (2) și (5).

2. Obligațiile de la alineatul (1) nu aduc atingere altor obligații ale utilizatorilor în temeiul dreptului Uniunii sau al dreptului intern și nici libertății utilizatorului de a-și organiza propriile resurse și activități în scopul punerii în aplicare a măsurilor de supraveghere umană indicate de furnizor.

3. Fără a aduce atingere alineatului (1), în măsura în care utilizatorul exercită controlul asupra datelor de intrare, utilizatorul respectiv se asigură că datele de intrare sunt relevante având în vedere scopul preconizat al sistemului de IA cu grad ridicat de risc.

4. Utilizatorii monitorizează funcționarea sistemului de IA cu grad ridicat de risc pe baza instrucțiunilor de utilizare. În cazul în care au motive să considere că utilizarea în conformitate cu instrucțiunile de utilizare poate avea ca rezultat un sistem de IA care prezintă un risc în sensul articolului 65 alineatul (1), aceștia informează furnizorul sau distribuitorul și suspendă utilizarea sistemului. De asemenea, aceștia informează furnizorul sau distribuitorul atunci când au identificat orice incident grav sau orice funcționare defectuoasă în sensul articolului 62 și întrerup utilizarea sistemului de IA. În cazul în care utilizatorul nu poate comunica cu furnizorul, articolul 62 se aplică *mutatis mutandis*.

5. În cazul utilizatorilor care sunt instituții de credit reglementate prin Directiva 2013/36/UE, se consideră că obligația de monitorizare prevăzută la primul paragraf este îndeplinită prin respectarea normelor privind mecanismele, procesele și măsurile de guvernanță internă în temeiul articolului 74 din directiva respectivă.

6. Utilizatorii sistemelor de IA cu grad ridicat de risc păstrează fișierele de jurnalizare generate automat de respectivul sistem de IA cu grad ridicat de risc, în măsura în care astfel de fișiere de jurnalizare se află sub controlul lor. Fișierele de jurnalizare se păstrează pentru o perioadă adecvată având în vedere scopul preconizat al sistemului de IA cu grad ridicat de risc și obligațiile legale aplicabile în temeiul dreptului Uniunii sau al dreptului intern.

   Utilizatorii care sunt instituții de credit reglementate de Directiva 2013/36/UE păstrează fișierele de jurnalizare ca parte a documentației privind mecanismele, procesele și măsurile de guvernanță interne, în conformitate cu articolul 74 din directiva respectivă.

7. Utilizatorii de sisteme de IA cu grad ridicat de risc utilizează informațiile furnizate în temeiul articolului 13 pentru a-și respecta obligația de a efectua o evaluare a impactului asupra protecției datelor în temeiul articolului 35 din Regulamentul (UE) 2016/679 sau al articolului 27 din Directiva (UE) 2016/680, după caz.

CAPITOLUL 4

AUTORITĂȚILE DE NOTIFICARE ȘI ORGANISMELE NOTIFICATE

Articolul 30

Autoritățile de notificare

1. Fiecare stat membru desemnează sau instituie o autoritate de notificare responsabilă cu instituirea și îndeplinirea procedurilor necesare pentru evaluarea, desemnarea și notificarea organismelor de evaluare a conformității și pentru monitorizarea acestora.

2. Statele membre pot desemna un organism național de acreditare menționat în Regulamentul (CE) nr. 765/2008 ca autoritate de notificare.

3. Autoritățile de notificare sunt instituite, organizate și administrate astfel încât să nu apară niciun conflict de interese cu organismele de evaluare a conformității și să se protejeze obiectivitatea și imparțialitatea activităților lor.

4. Autoritățile de notificare sunt organizate astfel încât deciziile cu privire la notificarea organismelor de evaluare a conformității să fie luate de persoane competente, altele decât cele care au efectuat evaluarea organismelor respective.

5. Autoritățile de notificare nu oferă și nu prestează activități pe care le prestează organismele de evaluare a conformității și nici servicii de consultanță în condiții comerciale sau concurențiale.

6. Autoritățile de notificare garantează confidențialitatea informațiilor obținute.

7. Autoritățile de notificare au la dispoziție personal competent suficient în vederea îndeplinirii corespunzătoare a sarcinilor lor.

8. Autoritățile de notificare se asigură că evaluările conformității sunt efectuate în mod proporțional, evitând sarcinile inutile pentru furnizori și că organismele notificate își îndeplinesc activitățile ținând seama în mod corespunzător de dimensiunea unei întreprinderi, de sectorul în care aceasta își desfășoară activitatea, de structura sa și de gradul de complexitate al sistemului de IA în cauză.

Articolul 31

Cererea de notificare a unui organism de evaluare a conformității

1. Organismele de evaluare a conformității depun o cerere de notificare la autoritatea de notificare a statului membru în care sunt stabilite.

2. Cererea de notificare este însoțită de o descriere a activităților de evaluare a conformității, a modulului sau modulelor de evaluare a conformității și a tehnologiilor din domeniul inteligenței artificiale pentru care organismul de evaluare a conformității se consideră a fi competent, precum și de un certificat de acreditare, în cazul în care există, eliberat de un organism național de acreditare care să ateste că organismul de evaluare a conformității satisface cerințele prevăzute la articolul 33. Se adaugă orice document valabil referitor la desemnările existente ale organismului notificat solicitant în temeiul oricărei alte legislații de armonizare a Uniunii.

3. În cazul în care un organism de evaluare a conformității nu poate prezenta un certificat de acreditare, acesta prezintă autorității de notificare documentele justificative necesare pentru verificarea, recunoașterea și monitorizarea periodică a conformității acestuia cu cerințele prevăzute la articolul 33. În cazul organismelor notificate care sunt desemnate în temeiul oricărei alte legislații de armonizare a Uniunii, toate documentele și certificatele legate de aceste desemnări pot fi utilizate pentru a sprijini procedura de desemnare a acestora în temeiul prezentului regulament, după caz.

Articolul 32

Procedura de notificare

1. Autoritățile de notificare pot notifica numai organismele de evaluare a conformității care au satisfăcut cerințele prevăzute la articolul 33.

2. Autoritățile de notificare înștiințează Comisia și celelalte state membre folosind instrumentul de notificare electronică dezvoltat și administrat de Comisie.

3. Notificarea include detalii complete ale activităților de evaluare a conformității, ale modulului sau modulelor de evaluare a conformității și ale tehnologiilor din domeniul inteligenței artificiale în cauză.

4. Organismul de evaluare a conformității în cauză poate exercita activitățile unui organism notificat numai în cazul în care nu există obiecții din partea Comisiei sau a celorlalte state membre, transmise în termen de o lună de la notificare.

5. Autoritățile de notificare înștiințează Comisia și celelalte state membre cu privire la orice modificare ulterioară relevantă adusă notificării.

Articolul 33

Organisme notificate

1. Organismele notificate verifică conformitatea sistemului de IA cu grad ridicat de risc în conformitate cu procedurile de evaluare a conformității menționate la articolul 43.

2. Organismele notificate satisfac cerințele organizatorice, de management al calității, de resurse și de proces care sunt necesare pentru îndeplinirea sarcinilor lor.

3. Structura organizațională, alocarea responsabilităților, liniile de raportare și funcționarea organismelor notificate sunt de așa natură încât să asigure încrederea în performanța și în rezultatele activităților de evaluare a conformității pe care le desfășoară organismele notificate.

4. Organismele notificate sunt independente de furnizorul unui sistem de IA cu grad ridicat de risc în legătură cu care efectuează activități de evaluare a conformității. Organismele notificate sunt, de asemenea, independente de orice alt operator care are un interes economic în legătură cu sistemul de IA cu grad ridicat de risc care este evaluat, precum și de orice concurent al furnizorului.

5. Organismele notificate sunt organizate și funcționează astfel încât să garanteze independența, obiectivitatea și imparțialitatea activităților lor. Organismele notificate documentează și pun în aplicare o structură și proceduri pentru garantarea imparțialității și pentru promovarea și punerea în practică a principiilor imparțialității în întreaga organizație, pentru tot personalul lor și pentru toate activitățile lor de evaluare.

6. Organismele notificate dispun de proceduri documentate care să asigure că personalul său, comitetele, filialele, subcontractanții săi, precum și orice organism asociat sau membru al personalului organismelor externe respectă confidențialitatea informațiilor care le parvin în timpul derulării activităților de evaluare a conformității, cu excepția cazurilor în care divulgarea este cerută prin lege. Personalul organismelor notificate este obligat să păstreze secretul profesional referitor la toate informațiile obținute în cursul îndeplinirii sarcinilor sale în temeiul prezentului regulament, excepție făcând relația cu autoritățile de notificare ale statului membru în care se desfășoară activitățile sale.

7. Organismele notificate dispun de proceduri pentru desfășurarea activităților, care să țină seama în mod corespunzător de dimensiunea unei întreprinderi, de sectorul în care aceasta operează, de structura sa și de gradul de complexitate al sistemului de IA în cauză.

8. Organismele notificate încheie o asigurare de răspundere civilă adecvată pentru activitățile lor de evaluare a conformității, cu excepția cazului în care răspunderea este asumată de statul membru în cauză, în conformitate cu dreptul intern, sau în care statul membru respectiv este direct responsabil pentru evaluarea conformității.

9. Organismele notificate sunt capabile să îndeplinească toate sarcinile care le revin în temeiul prezentului regulament cu cel mai înalt grad de integritate profesională și competență necesară în domeniul specific, indiferent dacă sarcinile respective sunt realizate chiar de organismele notificate sau în numele și pe răspunderea acestora.

10. Organismele notificate dispun de suficiente competențe interne pentru a putea evalua în mod eficace sarcinile îndeplinite de părți externe în numele lor. În acest scop, în orice moment, pentru fiecare procedură de evaluare a conformității și pentru fiecare tip de sistem de IA cu grad ridicat de risc în legătură cu care a fost desemnat, organismul notificat dispune în permanență de suficient personal administrativ, tehnic și științific care deține experiență și cunoștințe în ceea ce privește tehnologiile relevante din domeniul inteligenței artificiale, datele și calculul datelor și cerințele prevăzute în capitolul 2 din prezentul titlu.

11. Organismele notificate participă la activitățile de coordonare menționate la articolul 38. De asemenea, acestea participă direct sau sunt reprezentate în cadrul organizațiilor de standardizare europene sau se asigură că sunt la curent cu situația referitoare la standardele relevante.

12. Organismele notificate pun la dispoziția autorității de notificare menționate la articolul 30 și transmit la cerere toată documentația relevantă, inclusiv documentația furnizorilor, pentru a îi permite acesteia să își desfășoare activitățile de evaluare, desemnare, notificare, monitorizare și supraveghere și pentru a facilita evaluarea descrisă în prezentul capitol.

Articolul 34

Filiale ale organismelor notificate și subcontractarea de către organismele notificate

1. În cazul în care un organism notificat subcontractează anumite sarcini legate de evaluarea conformității sau recurge la o filială, acesta se asigură că subcontractantul sau filiala îndeplinește cerințele stabilite la articolul 33 și informează autoritatea de notificare în acest sens.

2. Organismele notificate preiau întreaga responsabilitate pentru sarcinile îndeplinite de subcontractanți sau de filiale, indiferent de locul în care sunt stabilite acestea.

3. Activitățile pot fi subcontractate sau îndeplinite de o filială doar cu acordul furnizorului.

4. Organismele notificate pun la dispoziția autorității de notificare documentele relevante privind evaluarea calificărilor subcontractantului sau ale filialei și privind activitățile îndeplinite de aceștia în temeiul prezentului regulament.

Articolul 35

Numerele de identificare și listele organismelor notificate desemnate în temeiul prezentului Regulament

1. Comisia atribuie un număr de identificare organismelor notificate. Comisia atribuie un singur număr, chiar dacă organismul este notificat în temeiul mai multor acte ale Uniunii.

2. Comisia pune la dispoziția publicului lista organismelor notificate în temeiul prezentului regulament, inclusiv numerele de identificare care le-au fost atribuite și activitățile pentru care au fost notificate. Comisia se asigură că lista este actualizată.

Articolul 36

Modificări ale notificărilor

1. În cazul în care o autoritate de notificare are suspiciuni sau a fost informată că un organism notificat nu mai îndeplinește cerințele prevăzute la articolul 33 sau că acesta nu își îndeplinește obligațiile, autoritatea respectivă investighează fără întârziere chestiunea, cu cea mai mare diligență. În acest context, aceasta informează organismul notificat în cauză cu privire la obiecțiile ridicate și îi oferă posibilitatea de a-și face cunoscute punctele de vedere. În cazul în care autoritatea de notificare ajunge la concluzia că organismul notificat investigat nu mai îndeplinește cerințele prevăzute la articolul 33 sau că nu își îndeplinește obligațiile, aceasta restricționează, suspendă sau retrage notificarea, după caz, în funcție de gravitatea încălcării. De asemenea, autoritatea de notificare informează de îndată Comisia și celelalte state membre în consecință.
2. În caz de restricționare, suspendare sau retragere a notificării sau în cazul în care organismul notificat și-a încetat activitatea, autoritatea de notificare ia măsurile adecvate pentru a se asigura că dosarele acelui organism notificat sunt fie preluate de un alt organism notificat, fie sunt puse la dispoziția autorităților de notificare responsabile, la cererea acestora.

Articolul 37

Contestarea competenței organismelor notificate

1. Dacă este necesar, Comisia investighează toate cazurile în care există motive de îndoială cu privire la îndeplinirea de către un organism notificat a cerințelor prevăzute la articolul 33.
2. Autoritatea de notificare furnizează Comisiei, la cerere, toate informațiile relevante referitoare la notificarea organismului notificat în cauză.
3. Comisia se asigură că toate informațiile confidențiale obținute în cursul investigațiilor sale în temeiul prezentului articol sunt tratate în mod confidențial.
4. În cazul în care Comisia constată că un organism notificat nu îndeplinește sau nu mai îndeplinește cerințele prevăzute la articolul 33, Comisia adoptă o decizie motivată prin care solicită statului membru notificator să ia măsurile corective necesare, inclusiv retragerea notificării, dacă este necesar. Actul de punere în aplicare respectiv se adoptă în conformitate cu procedura de examinare menționată la articolul 74 alineatul (2).

Articolul 38

Coordonarea organismelor notificate

1. Comisia se asigură că, în ceea ce privește domeniile reglementate de prezentul regulament, se instituie și se realizează în mod adecvat o coordonare și o cooperare corespunzătoare între organismele notificate care desfășoară activități în ceea ce

privește procedurile de evaluare a conformității sistemelor de IA în temeiul prezentului regulament, sub forma unui grup sectorial al organismelor notificate**.**

2. Statele membre se asigură că organismele notificate de acestea participă la activitatea grupului respectiv în mod direct sau prin reprezentanți desemnați.

Articolul 39

Organisme de evaluare a conformității din țări terțe

Organismele de evaluare a conformității instituite în temeiul legislației unei țări terțe cu care Uniunea a încheiat un acord pot fi autorizate să desfășoare activitățile organismelor notificate în temeiul prezentului regulament.

CAPITOLUL 5

STANDARDE, EVALUAREA CONFORMITĂȚII, CERTIFICATE, ÎNREGISTRARE

Articolul 40

Norme armonizate

Sistemele de IA cu grad ridicat de risc care sunt în conformitate cu normele armonizate sau cu o parte a acestora, ale căror referințe au fost publicate în *Jurnalul Oficial al Uniunii Europene*, sunt considerate a fi în conformitate cu cerințele stabilite în capitolul 2 din prezentul titlu, în măsura în care standardele respective acoperă cerințele respective.

Articolul 41

Specificații comune

1. În cazul în care normele armonizate menționate la articolul 40 nu există sau în cazul în care Comisia consideră că normele armonizate relevante sunt insuficiente sau că este necesar să se abordeze preocupări specifice legate de siguranță sau de drepturile fundamentale, Comisia poate adopta, prin intermediul unor acte de punere în aplicare, specificații comune în ceea ce privește cerințele prevăzute în capitolul 2 din prezentul titlu. Actele de punere în aplicare respective se adoptă în conformitate cu procedura de examinare menționată la articolul 74 alineatul (2).

2. Atunci când pregătește specificațiile comune menționate la alineatul (1), Comisia colectează opiniile organismelor sau ale grupurilor de experți relevante instituite în temeiul legislației sectoriale relevante a Uniunii.

3. Sistemele de IA cu grad ridicat de risc care sunt în conformitate cu specificațiile comune menționate la alineatul (1) sunt considerate a fi în conformitate cu cerințele prevăzute în capitolul 2 din prezentul titlu, în măsura în care acele specificații comune acoperă cerințele respective.

4. În cazul în care furnizorii nu respectă specificațiile comune menționate la alineatul (1), aceștia justifică în mod corespunzător faptul că au adoptat soluții tehnice cel puțin echivalente cu acestea.

Articolul 42

Prezumția de conformitate cu anumite cerințe

1. Ținând seama de scopul lor preconizat, sistemele de IA cu grad ridicat de risc care au fost antrenate și testate pe baza datelor referitoare la mediul geografic, comportamental și funcțional specific în care sunt destinate să fie utilizate sunt considerate a fi în conformitate cu cerința prevăzută la articolul 10 alineatul (4).

2. Sistemele de IA cu grad ridicat de risc care au fost certificate sau pentru care a fost emisă o declarație de conformitate în cadrul unui sistem de securitate cibernetică în temeiul Regulamentului (UE) 2019/881 al Parlamentului European și al Consiliului[63] și ale căror referințe au fost publicate în *Jurnalul Oficial al Uniunii Europene* sunt considerate a fi în conformitate cu cerințele de securitate cibernetică prevăzute la articolul 15 din prezentul regulament în măsura în care certificatul de securitate cibernetică sau declarația de conformitate sau părți ale acestora acoperă cerințele respective.

Articolul 43

Evaluarea conformității

1. Pentru sistemele de IA cu grad ridicat de risc enumerate la punctul 1 din anexa III, în cazul în care, pentru a demonstra conformitatea unui sistem de IA cu grad ridicat de risc cu cerințele prevăzute în capitolul 2 din prezentul titlu, furnizorul a aplicat normele armonizate menționate la articolul 40 sau, după caz, specificațiile comune menționate la articolul 41, furnizorul urmează una dintre următoarele proceduri:

   (a) procedura de evaluare a conformității bazată pe control intern menționată în anexa VI;

   (b) procedura de evaluare a conformității bazată pe evaluarea sistemului de management al calității și pe examinarea documentației tehnice, cu implicarea unui organism notificat, menționată în anexa VII.

   În cazul în care, pentru a demonstra conformitatea unui sistem de IA cu grad ridicat de risc cu cerințele prevăzute în capitolul 2 din prezentul titlu, furnizorul nu a aplicat sau a aplicat doar parțial normele armonizate menționate la articolul 40 sau în cazul în care astfel de standarde armonizate nu există, iar specificațiile comune menționate la articolul 41 nu sunt disponibile, furnizorul urmează procedura de evaluare a conformității prevăzută în anexa VII.

   În sensul procedurii de evaluare a conformității menționate în anexa VII, furnizorul poate alege oricare dintre organismele notificate. Cu toate acestea, în cazul în care sistemul este destinat să fie pus în funcțiune de către autoritățile de aplicare a legii, autoritățile din domeniul imigrației sau al azilului, precum și de către instituțiile, organismele sau agențiile UE, autoritatea de supraveghere a pieței menționată la articolul 63 alineatul (5) sau (6), după caz, acționează ca organism notificat.

---

63 Regulamentul (UE) 2019/881 al Parlamentului European și al Consiliului din 17 aprilie 2019 privind ENISA (Agenția Uniunii Europene pentru Securitate Cibernetică) și privind certificarea securității cibernetice pentru tehnologia informației și comunicațiilor și de abrogare a Regulamentului (UE) nr. 526/2013 (Regulamentul privind securitatea cibernetică) (JO L 151, 7.6.2019, p. 1).

2. În cazul sistemelor de IA cu grad ridicat de risc menționate la punctele 2-8 din anexa III, furnizorii urmează procedura de evaluare a conformității bazată pe controlul intern, astfel cum se menționează în anexa VI, care nu prevede implicarea unui organism notificat. În cazul sistemelor de IA cu grad ridicat de risc menționate la punctul 5 litera (b) din anexa III introduse pe piață sau puse în funcțiune de instituții de credit reglementate de Directiva 2013/36/UE, evaluarea conformității se efectuează în cadrul procedurii menționate la articolele 97-101 din directiva respectivă.

3. În cazul sistemelor de IA cu grad ridicat de risc cărora li se aplică actele juridice enumerate în anexa II secțiunea A, furnizorul urmează evaluarea conformității relevantă, astfel cum se prevede în actele juridice respective. Cerințele prevăzute în capitolul 2 din prezentul titlu se aplică acestor sisteme de IA cu grad ridicat de risc și fac parte din evaluarea respectivă. Se aplică, de asemenea, punctele 4.3, 4.4, 4.5 și punctul 4.6 al cincilea paragraf din anexa VII.

   În scopul evaluării respective, organismele notificate care au fost notificate în temeiul respectivelor acte juridice au dreptul de a controla conformitatea sistemelor de IA cu grad ridicat de risc cu cerințele prevăzute în capitolul 2 din prezentul titlu, cu condiția ca respectarea de către organismele notificate respective a cerințelor prevăzute la articolul 33 alineatele (4), (9) și (10) să fi fost evaluată în contextul procedurii de notificare în temeiul respectivelor acte juridice.

   În cazul în care actele juridice enumerate în anexa II secțiunea A permit fabricantului produsului să renunțe la evaluarea conformității efectuată de o parte terță, cu condiția ca fabricantul respectiv să fi aplicat toate normele armonizate care acoperă toate cerințele relevante, fabricantul respectiv poate face uz de această opțiune numai dacă a aplicat, de asemenea, standardele armonizate sau, după caz, specificațiile comune menționate la articolul 41, care acoperă cerințele prevăzute în capitolul 2 din prezentul titlu.

4. Sistemele de IA cu grad ridicat de risc fac obiectul unei noi proceduri de evaluare a conformității ori de câte ori sunt modificate substanțial, indiferent dacă sistemul modificat este destinat să fie distribuit ulterior sau dacă utilizatorul curent continuă să utilizeze sistemul modificat.

   În cazul sistemelor de IA cu grad ridicat de risc care continuă să învețe după ce au fost introduse pe piață sau puse în funcțiune, modificările aduse sistemului de IA cu grad ridicat de risc și performanței acestuia care au fost predeterminate de către furnizor la momentul evaluării inițiale a conformității și care fac parte din informațiile conținute în documentația tehnică menționată la punctul 2 litera (f) din anexa IV nu constituie o modificare substanțială.

5. Comisia este împuternicită să adopte acte delegate în conformitate cu articolul 73 în scopul actualizării anexelor VI și VII pentru a introduce elemente ale procedurilor de evaluare a conformității care devin necesare având în vedere progresul tehnic.

6. Comisia este împuternicită să adopte acte delegate pentru a modifica alineatele (1) și (2) în vederea supunerii sistemelor de IA cu grad ridicat de risc menționate la punctele 2-8 din anexa III procedurii de evaluare a conformității menționate în anexa VII sau unei părți ale acesteia. Comisia adoptă astfel de acte delegate ținând seama de eficacitatea procedurii de evaluare a conformității bazate pe controlul intern menționate în anexa VI în ceea ce privește prevenirea sau reducerea la minimum a riscurilor pentru sănătate și siguranță și protecția drepturilor

fundamentale pe care le prezintă astfel de sisteme, precum și disponibilitatea capacităților și a resurselor adecvate în rândul organismelor notificate.

Articolul 44

Certificate

1. Certificatele eliberate de organismele notificate în conformitate cu anexa VII sunt redactate într-o limbă oficială a Uniunii stabilită de statul membru în care este stabilit organismul notificat sau într-o limbă oficială a Uniunii acceptată în alt mod de organismul notificat.
2. Certificatele sunt valabile pentru perioada pe care o menționează, care nu depășește cinci ani. La solicitarea furnizorului, valabilitatea unui certificat poate fi prelungită pentru perioade suplimentare, fiecare dintre acestea nedepășind cinci ani, pe baza unei reevaluări în conformitate cu procedurile aplicabile de evaluare a conformității.
3. În cazul în care un organism notificat constată că un sistem de IA nu mai îndeplinește cerințele prevăzute în capitolul 2 din prezentul titlu, acesta, ținând seama de principiul proporționalității, suspendă sau retrage certificatul eliberat sau impune restricții asupra acestuia, cu excepția cazului în care îndeplinirea cerințelor respective este asigurată prin acțiuni corective adecvate întreprinse de furnizorul sistemului într-un termen adecvat stabilit de organismul notificat. Organismul notificat comunică motivele deciziei sale.

Articolul 45

Căi de atac împotriva deciziilor organismelor notificate

Statele membre se asigură că părțile care au un interes legitim în decizia respectivă au la dispoziție o cale de atac împotriva deciziilor organismelor notificate.

Articolul 46

Obligații de informare care revin organismelor notificate

1. Organismele notificate informează autoritatea de notificare în legătură cu:
   (a) toate certificatele de evaluare a documentației tehnice ale Uniunii, orice completare a certificatelor respective, aprobări ale sistemului de management al calității eliberate în conformitate cu cerințele din anexa VII;
   (b) orice refuz, restricție, suspendare sau retragere a unui certificat de evaluare a documentației tehnice al Uniunii sau a unei aprobări a unui sistem de management al calității eliberată în conformitate cu cerințele din anexa VII;
   (c) orice circumstanță care afectează domeniul de aplicare sau condițiile notificării;
   (d) orice cerere de informații pe care au primit-o de la autoritățile de supraveghere a pieței cu privire la activitățile de evaluare a conformității;
   (e) la cerere, activitățile de evaluare a conformității realizate în limita domeniului de aplicare al notificării și în legătură cu orice altă activitate realizată, inclusiv activități transfrontaliere și subcontractarea.

2. Fiecare organism notificat informează celelalte organisme notificate cu privire la:

(a) aprobările sistemului de management al calității pe care le-a refuzat, suspendat sau retras și, la cerere, aprobările sistemului calității pe care le-a emis;

(b) certificatele de evaluare UE a documentației tehnice sau orice supliment la acestea, pe care le-a refuzat, retras, suspendat sau restricționat în alt mod și, la cerere, certificatele și/sau suplimentele la acestea pe care le-a eliberat.

3. Fiecare organism notificat furnizează celorlalte organisme notificate care îndeplinesc activități similare de evaluare a conformității care acoperă aceleași tehnologii din domeniul inteligenței artificiale informații relevante privind aspecte legate de rezultatele negative ale evaluărilor conformității și, la cerere, de rezultatele pozitive ale evaluărilor conformității.

Articolul 47

Derogare de la procedura de evaluare a conformității

1. Prin derogare de la articolul 43, orice autoritate de supraveghere a pieței poate autoriza introducerea pe piață sau punerea în funcțiune a anumitor sisteme de IA cu grad ridicat de risc pe teritoriul statului membru în cauză, din motive excepționale de siguranță publică sau de protecție a vieții și sănătății persoanelor, de protecție a mediului și de protecție a activelor industriale și de infrastructură esențiale. Autorizația respectivă se acordă pentru o perioadă limitată de timp, cât timp procedurile necesare de evaluare a conformității sunt în desfășurare, și încetează odată ce procedurile respective au fost finalizate. Finalizarea procedurilor respective se efectuează fără întârzieri nejustificate.

2. Autorizația menționată la alineatul (1) se eliberează numai în cazul în care autoritatea de supraveghere a pieței concluzionează că sistemul de IA cu grad ridicat de risc respectă cerințele din capitolul 2 din prezentul titlu. Autoritatea de supraveghere a pieței informează Comisia și celelalte state membre cu privire la orice autorizație eliberată în temeiul alineatului (1).

3. În cazul în care, în termen de 15 zile calendaristice de la primirea informațiilor menționate la alineatul (2), niciun stat membru și nici Comisia nu ridică obiecții cu privire la o autorizație eliberată de o autoritate de supraveghere a pieței dintr-un stat membru în conformitate cu alineatul (1), autorizația respectivă este considerată justificată.

4. În cazul în care, în termen de 15 zile calendaristice de la primirea notificării menționate la alineatul (2), sunt ridicate obiecții de către un stat membru împotriva unei autorizații eliberate de o autoritate de supraveghere a pieței dintr-un alt stat membru sau în cazul în care Comisia consideră că autorizația este contrară dreptului Uniunii sau că concluzia statelor membre cu privire la conformitatea sistemului menționat la alineatul (2) este nefondată, Comisia inițiază fără întârziere consultări cu statul membru în cauză; operatorul (operatorii) în cauză este (sunt) consultat (consultați) și are (au) posibilitatea de a-și prezenta punctele de vedere. În acest sens, Comisia decide dacă autorizația este justificată sau nu. Comisia comunică decizia sa statului membru în cauză și operatorului sau operatorilor relevanți.

5. În cazul în care autorizația este considerată nejustificată, aceasta este retrasă de către autoritatea de supraveghere a pieței din statul membru în cauză.

6. Prin derogare de la alineatele (1) – (5), pentru sistemele de IA cu risc ridicat destinate utilizării drept componente de siguranță ale dispozitivelor sau care sunt ele însele dispozitive care fac obiectul Regulamentului (UE) 2017/745 și al Regulamentului (UE) 2017/746, articolul 59 din Regulamentul (UE) 2017/745 și articolul 54 din Regulamentul (UE) 2017/746 se aplică și în ceea ce privește derogarea de la evaluarea conformității cu cerințele prevăzute în capitolul 2 din prezentul titlu.

Articolul 48

Declarația de conformitate UE

1. Furnizorul întocmește o declarație de conformitate UE scrisă pentru fiecare sistem de IA și o pune la dispoziția autorităților naționale competente pe o perioadă de 10 ani după introducerea pe piață sau punerea în funcțiune a sistemului de IA. Declarația de conformitate UE identifică sistemul de IA pentru care a fost întocmită. O copie a declarației de conformitate UE este pusă la dispoziția autorităților naționale competente relevante, la cerere.
2. Declarația de conformitate UE precizează că sistemul de IA cu grad ridicat de risc în cauză îndeplinește cerințele prevăzute în capitolul 2 din prezentul titlu. Declarația de conformitate UE conține informațiile prevăzute în anexa V și se traduce într-o limbă oficială a Uniunii solicitată sau în limbile oficiale ale Uniunii solicitate de statul (statele) membru (membre) în care se pune la dispoziție sistemul de IA cu grad ridicat de risc.
3. În cazul în care sistemele de IA cu grad ridicat de risc fac obiectul altor acte legislative de armonizare ale Uniunii care necesită, de asemenea, o declarație de conformitate UE, se redactează o singură declarație de conformitate UE cu privire la toate legislațiile Uniunii aplicabile sistemului de IA cu grad ridicat de risc. Declarația conține toate informațiile necesare pentru identificarea legislației de armonizare a Uniunii la care declarația face referire.
4. Prin redactarea declarației de conformitate UE, furnizorul își asumă responsabilitatea pentru conformitatea cu cerințele prevăzute în capitolul 2 din prezentul titlu. Furnizorul actualizează în permanență declarația de conformitate UE, după caz.
5. Comisia este împuternicită să adopte acte delegate în conformitate cu articolul 73 în scopul actualizării conținutului declarației de conformitate UE prevăzute în anexa V pentru a introduce elemente care devin necesare având în vedere progresele tehnice.

Articolul 49

Marcajul CE de conformitate

1. Marcajul CE se aplică în mod vizibil, lizibil și indelebil pentru sistemele de IA cu risc ridicat. În cazul în care acest lucru nu este posibil sau justificat din considerente ținând de natura sistemului de IA cu grad ridicat de risc, marcajul se aplică pe ambalaj și pe documentele de însoțire, după caz.
2. Marcajul CE menționat la alineatul (1) din prezentul articol face obiectul principiilor generale prevăzute la articolul 30 din Regulamentul (CE) nr. 765/2008.

3. Dacă este cazul, marcajul CE este urmat de numărul de identificare al organismului notificat responsabil de procedurile de evaluare a conformității menționate la articolul 43. De asemenea, numărul de identificare se indică în orice material promoțional care menționează faptul că sistemul de IA cu grad ridicat de risc îndeplinește cerințele aferente marcajului CE.

Articolul 50

Păstrarea documentelor

Pentru o perioadă de 10 ani după introducerea pe piață sau punerea în funcțiune a sistemului de IA, furnizorul pune la dispoziția autorităților naționale competente:

(a) documentația tehnică menționată la articolul 11;

(b) documentația privind sistemul de management al calității menționată la articolul 17;

(c) documentația privind modificările aprobate de organismele notificate, după caz;

(d) deciziile și alte documente emise de organismele notificate, după caz;

(e) declarația de conformitate UE prevăzută la articolul 48.

Articolul 51

Înregistrare

Înainte de a introduce pe piață sau de a pune în funcțiune un sistem de IA cu grad ridicat de risc menționat la articolul 6 alineatul (2), furnizorul sau, după caz, reprezentantul autorizat înregistrează sistemul respectiv în baza de date a UE menționată la articolul 60.

TITLUL IV

OBLIGAȚII DE TRANSPARENȚĂ PENTRU ANUMITE SISTEME DE IA

Articolul 52

Obligații de transparență pentru anumite sisteme de IA

1. Furnizorii se asigură că sistemele de IA destinate să interacționeze cu persoane fizice sunt proiectate și dezvoltate astfel încât persoanele fizice să fie informate că interacționează cu un sistem de IA, cu excepția cazului în care acest lucru este evident din circumstanțele și contextul de utilizare. Această obligație nu se aplică sistemelor de IA autorizate prin lege pentru a detecta, a preveni, a investiga și a urmări penal infracțiunile, cu excepția cazului în care aceste sisteme sunt disponibile publicului pentru a denunța o infracțiune.

2. Utilizatorii unui sistem de recunoaștere a emoțiilor sau ai unui sistem biometric de clasificare informează persoanele fizice expuse la sistem cu privire la funcționarea acestuia. Această obligație nu se aplică sistemelor de IA utilizate pentru clasificarea biometrică, care sunt autorizate prin lege să detecteze, să prevină și să investigheze infracțiunile.

3. Utilizatorii unui sistem de IA care generează sau manipulează imagini, conținuturi audio sau video care seamănă în mod considerabil cu persoane, obiecte, locuri sau

alte entități sau evenimente existente și care ar crea unei persoane impresia falsă că sunt autentice sau adevărate („deepfake”), trebuie să facă cunoscut faptul că respectivul conținut a fost generat sau manipulat artificial.

Cu toate acestea, primul paragraf nu se aplică în cazul în care utilizarea este autorizată prin lege pentru a detecta, a preveni, a investiga și a urmări penal infracțiunile sau este necesară pentru exercitarea dreptului la libertatea de exprimare și a dreptului la libertatea artelor și științelor garantate în Carta drepturilor fundamentale a UE și sub rezerva unor garanții adecvate pentru drepturile și libertățile terților.

4. Alineatele (1), (2) și (3) nu aduc atingere cerințelor și obligațiilor prevăzute în titlul III din prezentul regulament.

TITLUL V

MĂSURI DE SPRIJINIRE A INOVĂRII

Articolul 53

Spațiile de testare în materie de reglementare a IA

1. Spațiile de testare în materie de reglementare a IA instituite de una sau mai multe autorități competente ale statelor membre sau de Autoritatea Europeană pentru Protecția Datelor asigură un mediu controlat care facilitează dezvoltarea, testarea și validarea sistemelor de IA inovatoare pentru o perioadă limitată de timp înainte de introducerea lor pe piață sau de punerea lor în funcțiune, conform unui plan specific. Acest lucru are loc sub supravegherea și îndrumarea directă a autorităților competente în vederea asigurării conformității cu cerințele prezentului regulament și, după caz, cu alte acte legislative ale Uniunii și ale statelor membre supravegheate în spațiul de testare.

2. Statele membre se asigură că, în măsura în care sistemele de IA inovatoare implică prelucrarea de date cu caracter personal sau intră în alt mod în competența de supraveghere a altor autorități naționale sau autorități competente care furnizează sau sprijină accesul la date, autoritățile naționale de protecție a datelor și celelalte autorități naționale respective sunt asociate funcționării spațiului de testare în materie de reglementare a IA.

3. Spațiile de testare în materie de reglementare a IA nu afectează competențele de supraveghere și atribuțiile corective ale autorităților competente. Orice risc semnificativ pentru sănătate, siguranță și drepturile fundamentale identificat în cursul dezvoltării și testării unor astfel de sisteme conduce la atenuarea imediată și, în cazul în care atenuarea nu este posibilă, la suspendarea procesului de dezvoltare și testare până la efectuarea unei astfel de atenuări.

4. Participanții la spațiul de testare în materie de reglementare a IA rămân responsabili, în temeiul legislației aplicabile a Uniunii și a statelor membre în materie de răspundere, pentru orice prejudiciu adus terților ca urmare a experimentării care are loc în spațiul de testare.

5. Autoritățile competente ale statelor membre care au instituit spații de testare în materie de reglementare a IA își coordonează activitățile și cooperează în cadrul Comitetului european pentru inteligența artificială. Acestea prezintă comitetului și

Comisiei rapoarte anuale cu privire la rezultatele punerii în aplicare a sistemului respectiv, inclusiv bune practici, lecții învățate și recomandări privind structura acestora și, după caz, privind aplicarea prezentului regulament și a altor acte legislative ale Uniunii supravegheate în spațiul de testare.

6. Modalitățile și condițiile de funcționare a spațiilor de testare în materie de reglementare a IA, inclusiv criteriile de eligibilitate și procedura de depunere a cererii, de selecție, de participare și de ieșire din spațiul de testare, precum și drepturile și obligațiile participanților sunt stabilite în acte de punere în aplicare. Actele de punere în aplicare respective se adoptă în conformitate cu procedura de examinare menționată la articolul 74 alineatul (2).

Articolul 54

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 a IA

1. În spațiul de testare în materie de reglementare a IA, datele cu caracter personal colectate în mod legal în alte scopuri sunt prelucrate în scopul dezvoltării și testării anumitor sisteme de IA inovatoare în spațiul de testare, în următoarele condiții:

   (a) sistemele de IA inovatoare sunt dezvoltate pentru a proteja un interes public substanțial în unul sau mai multe dintre următoarele domenii:

      (i) prevenirea, investigarea, depistarea sau urmărirea penală a infracțiunilor sau executarea sancțiunilor penale, inclusiv protejarea împotriva amenințărilor la adresa securității publice și prevenirea acestora, sub controlul și responsabilitatea autorităților competente. Prelucrarea se bazează pe legislația statului membru sau a Uniunii;

      (ii) siguranța publică și sănătatea publică, inclusiv prevenirea, controlul și tratarea bolilor;

      (iii) un nivel ridicat de protecție și de îmbunătățire a calității mediului;

   (b) datele prelucrate sunt necesare pentru a respecta una sau mai multe dintre cerințele menționate în titlul III capitolul 2, în cazul în care cerințele respective nu pot fi îndeplinite în mod eficace prin prelucrarea datelor anonimizate, sintetice sau a altor date fără caracter personal;

   (c) există mecanisme eficace de monitorizare pentru a identifica dacă pot apărea riscuri ridicate la adresa drepturilor fundamentale ale persoanelor vizate în timpul experimentării în spațiul de testare, precum și mecanisme de răspuns pentru a atenua cu promptitudine aceste riscuri și, dacă este necesar, pentru a opri prelucrarea;

   (d) toate datele cu caracter personal care urmează să fie prelucrate în contextul spațiului de testare se află într-un mediu de prelucrare a datelor separat din punct de vedere funcțional, izolat și protejat, aflat sub controlul participanților și numai persoanele autorizate au acces la datele respective;

   (e) datele cu caracter personal prelucrate nu sunt transmise, transferate sau accesate în alt mod de către alte părți;

   (f) nicio prelucrare a datelor cu caracter personal în contextul spațiului de testare nu conduce la măsuri sau la decizii care afectează persoanele vizate;

(g) toate datele cu caracter personal prelucrate în contextul spațiului de testare sunt șterse după ce participarea la spațiul respectiv a încetat sau datele cu caracter personal au ajuns la sfârșitul perioadei de păstrare;

(h) fișierele de jurnalizare a prelucrării datelor cu caracter personal în contextul spațiului de testare sunt păstrate pe durata participării la spațiul de testare și timp de 1 an de la încetarea acesteia, exclusiv în scopul îndeplinirii obligațiilor de responsabilitate și documentare în temeiul prezentului articol sau al altei aplicări a legislației Uniunii sau a statelor membre, și numai atât timp cât este necesar pentru aceasta;

(i) descrierea completă și detaliată a procesului și a motivelor care stau la baza antrenării, testării și validării sistemului de IA este păstrată împreună cu rezultatele testelor, ca parte a documentației tehnice menționate în anexa IV;

(j) un scurt rezumat al proiectului de IA elaborat în spațiul de testare, obiectivele și rezultatele preconizate ale acestuia, publicate pe site-ul web al autorităților competente.

2. Alineatul (1) nu aduce atingere legislației Uniunii sau a statelor membre care exclude prelucrarea în alte scopuri decât cele menționate în mod explicit în legislația respectivă.

Articolul 55

Măsuri pentru micii furnizori și utilizatori

1. Statele membre întreprind următoarele acțiuni:

(a) oferă micilor furnizori și întreprinderilor nou-înființate acces prioritar la spațiile de testare în materie de reglementare a IA, în măsura în care îndeplinesc condițiile de eligibilitate;

(b) organizează activități specifice de sensibilizare cu privire la aplicarea prezentului regulament, adaptate la nevoile micilor furnizori și utilizatori;

(c) după caz, stabilesc un canal special de comunicare cu micii furnizori și utilizatori, precum și cu alți inovatori, pentru a oferi orientări și a răspunde la întrebări legate de punerea în aplicare a prezentului regulament.

2. Interesele și nevoile specifice ale micilor furnizori sunt luate în considerare la stabilirea taxelor pentru evaluarea conformității în temeiul articolului 43, taxele respective fiind reduse proporțional cu mărimea și cu dimensiunea lor de piață.

TITLUL VI

GUVERNANȚA

CAPITOLUL 1

COMITETUL EUROPEAN PENTRU INTELIGENȚA ARTIFICIALĂ

Articolul 56

Instituirea Comitetului european pentru inteligența artificială

1. Se instituie un „Comitet european pentru inteligența artificială” (denumit în continuare „comitetul”).

2. Comitetul oferă consiliere și asistență Comisiei pentru:

   (a) a contribui la cooperarea eficace dintre autoritățile naționale de supraveghere și Comisie în ceea ce privește aspectele reglementate de prezentul regulament;

   (b) a coordona și contribui la orientările și analizele Comisiei și ale autorităților naționale de supraveghere, precum și ale altor autorități competente referitoare la problemele susceptibile să apară pe piața internă în ceea ce privește aspectele reglementate de prezentul regulament;

   (c) a sprijini autoritățile naționale de supraveghere și Comisia în ceea ce privește asigurarea aplicării consecvente a prezentului regulament.

Articolul 57

Structura comitetului

1. Comitetul este alcătuit din autoritățile naționale de supraveghere, care sunt reprezentate de șeful autorității respective sau de un înalt funcționar echivalent al acesteia, precum și din Autoritatea Europeană pentru Protecția Datelor. La reuniuni pot fi invitate și alte autorități naționale în cazul în care chestiunile discutate le privesc.

2. Comitetul își adoptă regulamentul de procedură cu majoritatea simplă a membrilor săi, pe baza unei propuneri a Comisiei. Regulamentul de procedură conține, de asemenea, aspecte operaționale legate de executarea sarcinilor comitetului, astfel cum sunt enumerate la articolul 58. Comitetul poate înființa subgrupuri, după caz, în scopul examinării unor chestiuni specifice.

3. Comitetul este prezidat de Comisie. Comisia convoacă reuniunile și stabilește ordinea de zi în conformitate cu sarcinile care revin comitetului în temeiul prezentului regulament și cu regulamentul său de procedură. Comisia furnizează sprijin administrativ și analitic pentru activitățile desfășurate de comitet în temeiul prezentului regulament.

4. Comitetul poate invita experți și observatori externi să participe la reuniunile sale și poate organiza schimburi cu părți terțe interesate ale căror rezultate să contribuie la activitățile sale, într-o măsură adecvată. În acest scop, Comisia poate facilita

schimburile dintre comitet și alte organisme, oficii, agenții și grupuri consultative ale Uniunii.

Articolul 58

Sarcinile comitetului

Atunci când oferă consiliere și asistență Comisiei în contextul articolului 56 alineatul (2), comitetul, în special:

(a) asigură colectarea și schimbul de expertiză și de bune practici între statele membre;

(b) contribuie la practici administrative uniforme în statele membre, inclusiv pentru funcționarea spațiilor de testare în materie de reglementare menționate la articolul 53;

(c) emite avize, recomandări sau contribuții scrise cu privire la aspecte legate de punerea în aplicare a prezentului regulament, în special

(i) privind specificațiile tehnice sau standardele existente referitoare la cerințele prevăzute în titlul III capitolul 2;

(ii) privind utilizarea normelor armonizate sau a specificațiilor comune menționate la articolele 40 și 41;

(iii) privind pregătirea documentelor de orientare, inclusiv a orientărilor referitoare la stabilirea amenzilor administrative menționate la articolul 71.

CAPITOLUL 2

AUTORITĂȚILE NAȚIONALE COMPETENTE

Articolul 59

Desemnarea autorităților naționale competente

1. Fiecare stat membru instituie sau desemnează autorități naționale competente cu scopul de a asigura aplicarea și punerea în aplicare a prezentului regulament. Autoritățile naționale competente sunt organizate astfel încât să garanteze obiectivitatea și imparțialitatea activităților și sarcinilor lor.

2. Fiecare stat membru desemnează o autoritate națională de supraveghere din rândul autorităților naționale competente. Autoritatea națională de supraveghere acționează ca autoritate de notificare și autoritate de supraveghere a pieței, cu excepția cazului în care un stat membru are motive organizatorice și administrative pentru a desemna mai multe autorități.

3. Statele membre informează Comisia cu privire la desemnarea sau desemnările lor și, după caz, cu privire la motivele desemnării mai multor autorități.

4. Statele membre se asigură că autoritățile naționale competente dispun de resurse financiare și umane adecvate pentru a-și îndeplini sarcinile care le revin în temeiul prezentului regulament. În special, autoritățile naționale competente dispun în permanență de un personal suficient ale cărui competențe și expertiză includ o înțelegere aprofundată a tehnologiilor din domeniul inteligenței artificiale, a datelor

și a calculului de date, a drepturilor fundamentale, a riscurilor în materie de sănătate și siguranță, precum și cunoașterea standardelor și a cerințelor legale existente.

5. Statele membre raportează anual Comisiei cu privire la situația resurselor financiare și umane ale autorităților naționale competente, evaluând gradul lor de adecvare. Comisia transmite aceste informații comitetului pentru a fi discutate și pentru a formula eventuale recomandări.

6. Comisia facilitează schimbul de experiență între autoritățile naționale competente.

7. Autoritățile naționale competente pot oferi orientări și consiliere cu privire la punerea în aplicare a prezentului regulament, inclusiv micilor furnizori. Ori de câte ori autoritățile naționale competente intenționează să ofere orientări și consiliere cu privire la un sistem de IA în domenii reglementate de alte acte legislative ale Uniunii, autoritățile naționale competente în temeiul legislației respective a Uniunii sunt consultate, după caz. Statele membre pot stabili, de asemenea, un punct central de contact pentru comunicarea cu operatorii.

8. Atunci când instituțiile, agențiile și organele Uniunii intră în domeniul de aplicare al prezentului regulament, Autoritatea Europeană pentru Protecția Datelor acționează ca autoritate competentă pentru supravegherea lor.

TITLUL VII

BAZA DE DATE A UE PENTRU SISTEME AUTONOME DE IA CU GRAD RIDICAT DE RISC

Articolul 60

Baza de date a UE pentru sisteme autonome de IA cu grad ridicat de risc

1. Comisia, în colaborare cu statele membre, creează și întreține o bază de date a UE care conține informațiile menționate la alineatul (2) privind sistemele de IA cu grad ridicat de risc menționate la articolul 6 alineatul (2) care sunt înregistrate în conformitate cu articolul 51.

2. Datele enumerate în anexa VIII se introduc în baza de date a UE de către furnizori. Comisia le furnizează acestora sprijin tehnic și administrativ.

3. Informațiile conținute în baza de date a UE sunt accesibile publicului.

4. Baza de date a UE conține date cu caracter personal numai în măsura în care acest lucru este necesar pentru colectarea și prelucrarea informațiilor în conformitate cu prezentul regulament. Aceste informații includ numele și datele de contact ale persoanelor fizice responsabile cu înregistrarea sistemului și care au autoritatea legală de a-l reprezenta pe furnizor.

5. Comisia este operatorul bazei de date a UE. Totodată, aceasta asigură furnizorilor sprijin tehnic și administrativ adecvat.

TITLUL VIII

MONITORIZAREA ULTERIOARĂ INTRODUCERII PE PIAȚĂ, SCHIMBUL DE INFORMAȚII, SUPRAVEGHEREA PIEȚEI

CAPITOLUL 1

MONITORIZAREA ULTERIOARĂ INTRODUCERII PE PIAȚĂ

Articolul 61

Monitorizarea ulterioară introducerii pe piață de către furnizori și planul de monitorizare ulterioară introducerii pe piață pentru sistemele de IA cu grad ridicat de risc

1. Furnizorii instituie și documentează un sistem de monitorizare ulterioară introducerii pe piață într-un mod care să fie proporțional cu natura tehnologiilor din domeniul inteligenței artificiale și cu riscurile sistemului de IA cu grad ridicat de risc.

2. Sistemul de monitorizare ulterioară introducerii pe piață colectează, documentează și analizează în mod activ și sistematic datele relevante furnizate de utilizatori sau colectate din alte surse cu privire la performanța sistemelor de IA cu grad ridicat de risc pe toată durata lor de viață și permite furnizorului să evalueze conformitatea continuă a sistemelor de IA cu cerințele prevăzute în titlul III capitolul 2.

3. Sistemul de monitorizare ulterioară introducerii pe piață se bazează pe un plan de monitorizare ulterioară introducerii pe piață. Planul de monitorizare ulterioară introducerii pe piață face parte din documentația tehnică menționată în anexa IV. Comisia adoptă un act de punere în aplicare prin care stabilește dispoziții detaliate de instituire a unui model pentru planul de monitorizare ulterioară introducerii pe piață și a listei elementelor care trebuie incluse în plan.

4. Pentru sistemele de IA cu grad ridicat de risc reglementate de actele juridice menționate în anexa II, în cazul în care s-au instituit deja un sistem și un plan de monitorizare ulterioară introducerii pe piață în temeiul legislației respective, elementele descrise la alineatele (1), (2) și (3) sunt integrate în sistemul respectiv și în planul respectiv, după caz.

   Primul paragraf se aplică, de asemenea, sistemelor de IA cu grad ridicat de risc menționate la punctul 5 litera (b) din anexa III, introduse pe piață sau puse în funcțiune de instituțiile de credit reglementate de Directiva 2013/36/UE.

CAPITOLUL 2

SCHIMBUL DE INFORMAȚII PRIVIND INCIDENTELE ȘI FUNCȚIONAREA DEFECTUOASĂ

Articolul 62

Raportarea incidentelor grave și a funcționării defectuoase

1. Furnizorii de sisteme de IA cu grad ridicat de risc introduse pe piața Uniunii raportează autorităților de supraveghere a pieței din statele membre în care s-a produs incidentul grav sau încălcarea respectivă orice incident grav sau orice funcționare defectuoasă a sistemelor respective, care constituie o încălcare a obligațiilor în temeiul dreptului Uniunii menite să protejeze drepturile fundamentale.

   O astfel de notificare se efectuează imediat după ce furnizorul a stabilit o legătură de cauzalitate între sistemul de IA și incident sau funcționarea defectuoasă sau probabilitatea rezonabilă a unei astfel de legături și, în orice caz, nu mai târziu de 15 zile de la data la care furnizorii au luat cunoștință de incidentul grav sau de funcționarea defectuoasă.

2. La primirea unei notificări referitoare la o încălcare a obligațiilor instituite în temeiul dreptului Uniunii menite să protejeze drepturile fundamentale, autoritatea de supraveghere a pieței informează autoritățile sau organismele publice naționale menționate la articolul 64 alineatul (3). Comisia elaborează orientări specifice pentru a facilita respectarea obligațiilor prevăzute la alineatul (1). Orientările respective se emit în termen de cel mult 12 luni de la intrarea în vigoare a prezentului regulament.

3. În cazul sistemelor de IA cu grad ridicat de risc menționate la punctul 5 litera (b) din anexa III care sunt introduse pe piață sau puse în funcțiune de furnizori care sunt instituții de credit reglementate de Directiva 2013/36/UE și pentru sistemele de IA cu grad ridicat de risc care sunt componente de siguranță ale dispozitivelor sau sunt ele însele dispozitive care fac obiectul Regulamentului (UE) 2017/745 și al Regulamentului (UE) 2017/746, notificarea incidentelor grave sau a funcționării defectuoase se limitează la cele care constituie o încălcare a obligațiilor în temeiul dreptului Uniunii menite să protejeze drepturile fundamentale.

CAPITOLUL 3

ASIGURAREA PUNERII ÎN APLICARE

Articolul 63

Supravegherea pieței și controalele asupra sistemelor de IA pe piața Uniunii

1. Regulamentul (UE) 2019/1020 se aplică sistemelor de IA care intră sub incidența prezentului regulament. Cu toate acestea, în scopul aplicării efective a prezentului regulament:

   (a) orice trimitere la un operator economic în temeiul Regulamentului (UE) 2019/1020 se interpretează ca incluzând toți operatorii identificați în titlul III capitolul 3 din prezentul regulament;

(b) orice trimitere la un produs în temeiul Regulamentului (UE) 2019/1020 se interpretează ca incluzând toate sistemele de IA care intră în domeniul de aplicare al prezentului regulament.

2. Autoritatea națională de supraveghere raportează periodic Comisiei rezultatele activităților relevante de supraveghere a pieței. Autoritatea națională de supraveghere raportează fără întârziere Comisiei și autorităților naționale de concurență relevante toate informațiile identificate în cursul activităților de supraveghere a pieței care ar putea prezenta un potențial interes pentru aplicarea dreptului Uniunii privind normele în materie de concurență.

3. În cazul sistemelor de IA cu grad ridicat de risc legate de produsele cărora li se aplică actele juridice enumerate în anexa II secțiunea A, autoritatea de supraveghere a pieței în sensul prezentului regulament este autoritatea responsabilă cu activitățile de supraveghere a pieței desemnată în temeiul respectivelor acte juridice.

4. Pentru sistemele de IA introduse pe piață, puse în funcțiune sau utilizate de instituțiile financiare reglementate de legislația Uniunii privind serviciile financiare, autoritatea de supraveghere a pieței în sensul prezentului regulament este autoritatea relevantă responsabilă cu supravegherea financiară a instituțiilor respective în temeiul legislației respective.

5. Pentru sistemele de IA enumerate la alineatul 1 litera (a), în măsura în care sistemele sunt utilizate în scopul asigurării respectării legii, precum și la punctele 6 și 7 din anexa III, statele membre desemnează drept autorități de supraveghere a pieței în sensul prezentului regulament fie autoritățile de supraveghere în materie de protecție a datelor competente în temeiul Directivei (UE) 2016/680 sau al Regulamentului 2016/679, fie autoritățile naționale competente care supraveghează activitățile autorităților de aplicare a legii, de imigrație sau de azil ce pun în funcțiune sau utilizează sistemele respective.

6. În cazul în care instituțiile, agențiile și organele Uniunii intră în domeniul de aplicare al prezentului regulament, Autoritatea Europeană pentru Protecția Datelor acționează în calitate de autoritate de supraveghere a pieței.

7. Statele membre facilitează coordonarea dintre autoritățile de supraveghere a pieței desemnate în temeiul prezentului regulament și alte autorități sau organisme naționale relevante care supraveghează aplicarea legislației de armonizare a Uniunii enumerate în anexa II sau a altor acte legislative ale Uniunii care ar putea fi relevante pentru sistemele de IA cu grad ridicat de risc menționate în anexa III.

Articolul 64

Accesul la date și la documentație

1. În ceea ce privește accesul la date și la documentație în contextul activităților lor, autorităților de supraveghere a pieței li se acordă acces deplin la seturile de date de antrenament, de validare și de testare utilizate de furnizor, inclusiv prin interfețe de programare a aplicațiilor („IPA”) sau prin alte mijloace și instrumente adecvate care permit accesul de la distanță.

2. În cazul în care este necesar pentru a evalua conformitatea sistemului de IA cu grad ridicat de risc cu cerințele prevăzute în capitolul 2 titlul III și în urma unei cereri motivate, autorităților de supraveghere a pieței li se acordă, de asemenea, acces la codul sursă al sistemului de IA.

3. Autoritățile sau organismele publice naționale care supraveghează sau asigură respectarea obligațiilor în temeiul dreptului Uniunii care protejează drepturile fundamentale în ceea ce privește utilizarea sistemelor de IA cu grad ridicat de risc menționate în anexa III au competența de a solicita și de a accesa orice documentație creată sau păstrată în temeiul prezentului regulament atunci când accesul la documentația respectivă este necesar pentru îndeplinirea competențelor care le revin în temeiul mandatului lor, în limitele jurisdicției lor. Autoritatea sau organismul public relevant informează autoritatea de supraveghere a pieței din statul membru în cauză cu privire la orice astfel de cerere.

4. În termen de 3 luni de la intrarea în vigoare a prezentului regulament, fiecare stat membru identifică autoritățile sau organismele publice menționate la alineatul (3) și pune la dispoziția publicului o listă pe site-ul web al autorității naționale de supraveghere. Statele membre notifică lista Comisiei și tuturor celorlalte state membre și o actualizează.

5. În cazul în care documentația menționată la alineatul (3) este insuficientă pentru a stabili dacă a avut loc sau nu o încălcare a obligațiilor prevăzute de dreptul Uniunii menite să protejeze drepturile fundamentale, autoritatea sau organismul public menționat la alineatul (3) poate adresa autorității de supraveghere a pieței o cerere motivată de organizare a testării sistemului de IA cu grad ridicat de risc prin mijloace tehnice. Autoritatea de supraveghere a pieței organizează testarea implicând îndeaproape autoritatea sau organismul public solicitant, într-un termen rezonabil de la primirea cererii.

6. Toate informațiile și documentele obținute de autoritățile sau organismele publice naționale menționate la alineatul (3) în temeiul dispozițiilor prezentului articol sunt tratate în conformitate cu obligațiile de confidențialitate prevăzute la articolul 70.

Articolul 65

Procedura aplicabilă sistemelor de IA care prezintă un risc la nivel național

1. Prin sisteme de IA care prezintă un risc se înțelege un produs ce prezintă un risc definit la articolul 3 punctul 19 din Regulamentul (UE) 2019/1020 în ceea ce privește riscurile pentru sănătate sau siguranță sau pentru protecția drepturilor fundamentale ale persoanelor.

2. În cazul în care autoritatea de supraveghere a pieței dintr-un stat membru are suficiente motive să considere că un sistem de IA prezintă un risc astfel cum se menționează la alineatul (1), aceasta efectuează o evaluare a sistemului de IA în cauză din punctul de vedere al conformității sale cu toate cerințele și obligațiile prevăzute în prezentul regulament. Atunci când există riscuri pentru protecția drepturilor fundamentale, autoritatea de supraveghere a pieței informează, de asemenea, autoritățile sau organismele publice naționale relevante menționate la articolul 64 alineatul (3). Operatorii relevanți cooperează, după caz, cu autoritățile de supraveghere a pieței și cu celelalte autorități sau organisme publice naționale menționate la articolul 64 alineatul (3).

   În cazul în care, pe parcursul evaluării respective, autoritatea de supraveghere a pieței constată că sistemul de IA nu respectă cerințele și obligațiile prevăzute în prezentul regulament, aceasta solicită de îndată operatorului relevant să ia toate măsurile corective adecvate pentru a asigura conformitatea sistemului de IA, pentru a retrage

sistemul de IA de pe piață sau pentru a-l rechema într-un termen rezonabil, proporțional cu natura riscului, indicat de aceasta.

Autoritățile de supraveghere a pieței informează organismul notificat relevant în consecință. Articolul 18 din Regulamentul (UE) 2019/1020 se aplică măsurilor menționate la al doilea paragraf.

3. În cazul în care autoritatea de supraveghere a pieței consideră că neconformitatea nu se limitează la teritoriul său național, informează Comisia și celelalte state membre cu privire la rezultatele evaluării și la măsurile pe care le-a impus operatorului.

4. Operatorul se asigură că sunt întreprinse toate măsurile corective adecvate pentru toate sistemele de IA vizate pe care acesta le-a pus la dispoziție pe piață în cadrul Uniunii.

5. În cazul în care operatorul unui sistem de IA nu întreprinde acțiunile corective adecvate în termenul menționat la alineatul (2), autoritatea de supraveghere a pieței ia toate măsurile provizorii corespunzătoare pentru a interzice sau a restricționa punerea la dispoziție a sistemului de IA pe piața sa națională, pentru a retrage produsul de pe piață sau pentru a-l rechema. Autoritatea respectivă informează Comisia și celelalte state membre, fără întârziere, cu privire la măsurile respective.

6. Informațiile menționate la alineatul (5) includ toate detaliile disponibile, în special cu privire la datele necesare pentru a identifica sistemul de IA neconform, originea sistemului de IA, natura neconformității invocate și riscul implicat, natura și durata măsurilor naționale luate, precum și argumentele prezentate de operatorul respectiv. În special, autoritățile de supraveghere a pieței indică dacă neconformitatea se datorează unuia sau mai multora dintre următoarele motive:

   (a) nerespectarea de către sistemul de IA a cerințelor prevăzute în titlul III capitolul 2;

   (b) existența unor deficiențe în ceea ce privește normele armonizate sau specificațiile comune menționate la articolele 40 și 41 care conferă o prezumție de conformitate.

7. Autoritățile de supraveghere a pieței din statele membre, altele decât autoritatea de supraveghere a pieței din statul membru care a inițiat procedura, informează imediat Comisia și celelalte state membre cu privire la toate măsurile adoptate și la toate informațiile suplimentare deținute referitoare la neconformitatea sistemelor de IA în cauză și, în cazul unui dezacord cu măsura națională notificată, cu privire la obiecțiile lor.

8. În cazul în care, în termen de trei luni de la primirea informațiilor menționate la alineatul (5), niciun stat membru și nici Comisia nu ridică vreo obiecție cu privire la o măsură provizorie luată de un stat membru, măsura respectivă este considerată justificată. Acest lucru nu aduce atingere drepturilor procedurale ale operatorului în cauză în conformitate cu articolul 18 din Regulamentul (UE) 2019/1020.

9. Autoritățile de supraveghere a pieței din toate statele membre se asigură că se iau măsuri restrictive adecvate în ceea ce privește produsul în cauză, cum ar fi retragerea fără întârziere a produsului de pe piețele lor.

Articolul 66

Procedura de salvgardare a Uniunii

1. Dacă, în termen de trei luni de la primirea notificării menționate la articolul 65 alineatul (5), se ridică obiecții de către un stat membru împotriva unei măsuri adoptate de un alt stat membru, sau în cazul în care Comisia consideră că măsura este contrară dreptului Uniunii, Comisia inițiază fără întârziere consultări cu statul membru și cu operatorul sau operatorii în cauză și evaluează măsura națională. Pe baza rezultatelor evaluării respective, Comisia decide dacă măsura națională este justificată sau nu în termen de 9 luni de la notificarea menționată la articolul 65 alineatul (5) și notifică această decizie statului membru în cauză.

2. În cazul în care măsura națională este considerată justificată, toate statele membre adoptă măsurile necesare pentru a se asigura că sistemul de IA neconform este retras de pe piețele lor și informează Comisia în consecință. În cazul în care măsura națională este considerată nejustificată, statul membru în cauză retrage măsura.

3. Atunci când măsura națională este considerată justificată, iar neconformitatea sistemului de IA este atribuită unor deficiențe ale normelor armonizate sau ale specificațiilor comune menționate la articolele 40 și 41 din prezentul regulament, Comisia aplică procedura prevăzută la articolul 11 din Regulamentul (UE) nr. 1025/2012.

Articolul 67

Sisteme de IA conforme care prezintă un risc

1. În cazul în care, după efectuarea unei evaluări în temeiul articolului 65, autoritatea de supraveghere a pieței dintr-un stat membru constată că, deși un sistem de IA este în conformitate cu prezentul regulament, acesta prezintă un risc pentru sănătatea sau siguranța persoanelor, pentru respectarea obligațiilor prevăzute de dreptul Uniunii sau de dreptul intern menite să protejeze drepturile fundamentale sau alte aspecte legate de protecția interesului public, aceasta solicită operatorului relevant să ia toate măsurile corespunzătoare pentru a se asigura că sistemul de IA în cauză, atunci când este introdus pe piață sau pus în funcțiune, nu mai prezintă riscul respectiv și să retragă de pe piață sau să recheme sistemul de IA într-un termen rezonabil, proporțional cu natura riscului, indicat de aceasta.

2. Furnizorul sau alți operatori relevanți se asigură că sunt întreprinse acțiuni corective cu privire la toate sistemele de IA în cauză pe care aceștia le-au pus la dispoziție pe piață în întreaga Uniune, în termenul prevăzut de autoritatea de supraveghere a pieței din statul membru menționată la alineatul (1).

3. Statul membru informează imediat Comisia și celelalte state membre. Informațiile includ toate detaliile disponibile, în special datele necesare pentru identificarea sistemului de IA în cauză, originea și a lanțul de aprovizionare aferent acestuia, natura riscului implicat, precum și natura și durata măsurilor naționale luate.

4. Comisia inițiază fără întârziere consultări cu statele membre și cu operatorul relevant și evaluează măsurile naționale luate. Pe baza rezultatelor evaluării respective, Comisia decide dacă măsura este justificată sau nu și, dacă este cazul, propune măsuri adecvate.

5. Comisia comunică decizia sa celorlalte state membre.

Articolul 68

Neconformitatea formală

1. Autoritatea de supraveghere a pieței dintr-un stat membru solicită operatorului relevant să pună capăt neconformității în cauză, atunci când constată una dintre situațiile următoare:

   (a) marcajul de conformitate a fost aplicat cu încălcarea articolului 49;

   (b) marcajul de conformitate nu este aplicat;

   (c) declarația de conformitate UE nu a fost redactată;

   (d) declarația de conformitate UE nu a fost redactată corect;

   (e) numărul de identificare al organismului notificat, care este implicat în procedura de evaluare a conformității, după caz, nu a fost aplicat.

2. În cazul în care neconformitatea menționată la alineatul (1) persistă, statul membru în cauză ia toate măsurile corespunzătoare pentru a restricționa sau a interzice punerea la dispoziție pe piață a sistemului de IA cu grad ridicat de risc sau se asigură că acesta este rechemat sau retras de pe piață.

TITLUL IX

CODURI DE CONDUITĂ

Articolul 69

Coduri de conduită

1. Comisia și statele membre încurajează și facilitează elaborarea de coduri de conduită menite să promoveze aplicarea voluntară pentru sistemele de IA, altele decât sistemele de IA cu grad ridicat de risc, a cerințelor prevăzute în titlul III capitolul 2, pe baza unor specificații și soluții tehnice care sunt mijloace adecvate de asigurare a conformității cu aceste cerințe, având în vedere scopul preconizat al sistemelor.

2. Comisia și comitetul încurajează și facilitează elaborarea de coduri de conduită menite să promoveze aplicarea voluntară, pentru sistemele de IA, a cerințelor legate, de exemplu, de durabilitatea mediului, de accesibilitatea pentru persoanele cu handicap, de participarea părților interesate la proiectarea și dezvoltarea sistemelor de IA și de diversitatea echipelor de dezvoltare, pe baza unor obiective clare și a unor indicatori-cheie de performanță pentru a măsura realizarea obiectivelor respective.

3. Codurile de conduită pot fi elaborate de furnizori individuali de sisteme de IA sau de organizații care îi reprezintă sau de ambele, inclusiv cu implicarea utilizatorilor și a oricăror părți interesate și a organizațiilor lor reprezentative. Codurile de conduită pot acoperi unul sau mai multe sisteme de IA, ținând seama de similaritatea scopului preconizat al sistemelor relevante.

4. Comisia și comitetul țin seama de interesele și nevoile specifice ale micilor furnizori și ale întreprinderilor nou-înființate atunci când încurajează și facilitează elaborarea de coduri de conduită.

TITLUL X

CONFIDENȚIALITATE ȘI SANCȚIUNI

Articolul 70

Confidențialitate

1. Autoritățile naționale competente și organismele notificate implicate în aplicarea prezentului regulament respectă confidențialitatea informațiilor și a datelor obținute în îndeplinirea sarcinilor și a activităților lor într-un mod care să protejeze, în special:

   (a) drepturile de proprietate intelectuală și informațiile comerciale confidențiale sau secretele comerciale ale unei persoane fizice sau juridice, inclusiv codul sursă, cu excepția cazurilor menționate la articolul 5 din Directiva 2016/943 privind protecția know-how-ului și a informațiilor de afaceri nedivulgate (secrete comerciale) împotriva dobândirii, utilizării și divulgării ilegale;

   (b) punerea efectivă în aplicare a prezentului regulament, în special în scopul inspecțiilor, investigațiilor sau auditurilor; (c) interesele de securitate publică și națională;

   (c) integritatea procedurilor penale sau administrative.

2. Fără a aduce atingere alineatului (1), informațiile care au făcut obiectul unui schimb în condiții de confidențialitate între autoritățile naționale competente și între autoritățile naționale competente și Comisie nu se divulgă fără consultarea prealabilă a autorității naționale competente emitente și a utilizatorului atunci când sistemele de IA cu grad ridicat de risc menționate la punctele 1, 6 și 7 din anexa III sunt utilizate de autoritățile de aplicare a legii, de imigrație sau de azil, în cazul în care o astfel de divulgare ar pune în pericol interesele publice și de securitate națională.

   În cazul în care autoritățile de aplicare a legii, din domeniul imigrației sau al azilului sunt furnizori de sisteme de IA cu grad ridicat de risc menționate la punctele 1, 6 și 7 din anexa III, documentația tehnică menționată în anexa IV rămâne la sediul autorităților respective. Autoritățile respective se asigură că autoritățile de supraveghere a pieței menționate la articolul 63 alineatul (5) și alineatul (6), după caz, pot, la cerere, să acceseze imediat documentația sau să obțină o copie a acesteia. Numai personalului autorității de supraveghere a pieței care deține nivelul corespunzător de autorizație de securitate i se permite accesul la documentația respectivă sau la orice copie a acesteia.

3. Alineatele (1) și (2) nu aduc atingere drepturilor și obligațiilor care revin Comisiei, statelor membre și organismelor notificate cu privire la schimbul de informații și difuzarea avertizărilor și nici obligațiilor părților în cauză de a furniza informații în temeiul dreptului penal al statelor membre.

4. Comisia și statele membre pot face schimb, atunci când este necesar, de informații confidențiale cu autoritățile de reglementare din țări terțe cu care au încheiat acorduri de confidențialitate bilaterale sau multilaterale care garantează un nivel adecvat de confidențialitate.

Articolul 71

Sancțiuni

1. În conformitate cu clauzele și condițiile prevăzute în prezentul regulament, statele membre stabilesc normele privind sancțiunile, inclusiv amenzile administrative, aplicabile în cazul încălcării prezentului regulament, și iau toate măsurile necesare pentru a se asigura că acestea sunt puse în aplicare în mod corespunzător și cu eficacitate. Sancțiunile prevăzute sunt eficace, proporționale și disuasive. Acestea țin seama în special de interesele micilor furnizori și ale întreprinderilor nou-înființate, precum și de viabilitatea lor economică.

2. Statele membre notifică normele respective Comisiei și îi comunică acesteia, fără întârziere, orice modificare ulterioară privind aceste norme.

3. Următoarele încălcări fac obiectul unor amenzi administrative de până la 30 000 000 EUR sau, în cazul în care autorul infracțiunii este o întreprindere, de până la 6 % din cifra sa de afaceri mondială totală anuală pentru exercițiul financiar precedent, luându-se în considerare valoarea cea mai mare:

   (a) nerespectarea interdicției privind practicile în domeniul inteligenței artificiale menționate la articolul 5;

   (b) neconformitatea sistemului de IA cu cerințele prevăzute la articolul 10.

4. Neconformitatea sistemului de IA cu oricare dintre cerințele sau obligațiile în temeiul prezentului regulament, altele decât cele prevăzute la articolele 5 și 10, face obiectul unor amenzi administrative de până la 20 000 000 EUR sau, în cazul în care autorul infracțiunii este o întreprindere, de până la 4 % din cifra sa de afaceri mondială totală anuală pentru exercițiul financiar precedent, luându-se în considerare valoarea cea mai mare dintre acestea.

5. Furnizarea de informații incorecte, incomplete sau înșelătoare organismelor notificate și autorităților naționale competente ca răspuns la o cerere face obiectul unor amenzi administrative de până la 10 000 000 EUR sau, în cazul în care autorul infracțiunii este o întreprindere, de până la 2 % din cifra sa de afaceri mondială totală anuală pentru exercițiul financiar precedent, luându-se în considerare valoarea cea mai mare dintre acestea.

6. Atunci când se decide cu privire la cuantumul amenzii administrative în fiecare caz în parte, se iau în considerare toate circumstanțele relevante ale situației specifice și se acordă atenția cuvenită următoarelor aspecte:

   (a) natura, gravitatea și durata încălcării și a consecințelor acesteia;

   (b) dacă alte autorități de supraveghere a pieței au aplicat deja amenzi administrative aceluiași operator pentru aceeași încălcare;

   (c) dimensiunea și cota de piață ale operatorului care a săvârșit încălcarea.

7. Fiecare stat membru stabilește norme pentru a stabili dacă și în ce măsură pot fi impuse amenzi administrative autorităților și organismelor publice stabilite în statul membru respectiv.

8. În funcție de sistemul juridic al statelor membre, normele privind amenzile administrative pot fi aplicate astfel încât amenzile să fie impuse de instanțele naționale competente ale altor organisme, astfel cum sunt aplicabile în statele

membre respective. Aplicarea unor astfel de norme în statele membre respective are un efect echivalent.

Articolul 72

Amenzi administrative aplicate instituțiilor, agențiilor și organelor Uniunii

1. Autoritatea Europeană pentru Protecția Datelor poate impune amenzi administrative instituțiilor, agențiilor și organelor Uniunii care intră în domeniul de aplicare al prezentului regulament. Atunci când se decide dacă să se impună o amendă administrativă și cu privire la cuantumul amenzii administrative în fiecare caz în parte, se iau în considerare toate circumstanțele relevante ale situației specifice și se acordă atenția cuvenită următoarelor aspecte:

   (a) natura, gravitatea și durata încălcării și a consecințelor acesteia;

   (b) cooperarea cu Autoritatea Europeană pentru Protecția Datelor pentru a remedia încălcarea și a atenua posibilele efecte negative ale încălcării, inclusiv conformitatea cu oricare dintre măsurile dispuse anterior de Autoritatea Europeană pentru Protecția Datelor împotriva instituției, agenției sau a organului Uniunii în cauză cu privire la același subiect;

   (c) eventualele încălcări anterioare similare comise de instituția, agenția sau de organul Uniunii.

2. Următoarele încălcări fac obiectul unor amenzi administrative de până la 500 000 EUR:

   (a) nerespectarea interdicției privind practicile în domeniul inteligenței artificiale menționate la articolul 5;

   (b) neconformitatea sistemului de IA cu cerințele prevăzute la articolul 10.

3. Neconformitatea sistemului de IA cu oricare dintre cerințele sau obligațiile în temeiul prezentului regulament, altele decât cele prevăzute la articolele 5 și 10, face obiectul unor amenzi administrative de până la 250 000 EUR.

4. Înaintea adoptării unor decizii în temeiul prezentului articol, Autoritatea Europeană pentru Protecția Datelor oferă instituției, agenției sau organului Uniunii care face obiectul procedurilor desfășurate de Autoritatea Europeană pentru Protecția Datelor posibilitatea de a fi audiat cu privire la posibila încălcare. Autoritatea Europeană pentru Protecția Datelor își fundamentează deciziile doar pe elementele și circumstanțele asupra cărora părțile în cauză au putut formula observații. Reclamanții, dacă există, sunt implicați îndeaproape în proceduri.

5. Drepturile la apărare ale părților în cauză sunt pe deplin respectate în cadrul procedurilor. Părțile au drept de acces la dosarul Autorității Europene pentru Protecția Datelor, sub rezerva interesului legitim al persoanelor fizice sau al întreprinderilor în ceea ce privește protecția datelor cu caracter personal sau a secretelor comerciale ale acestora.

6. Fondurile colectate prin aplicarea amenzilor prevăzute la prezentul articol constituie venituri la bugetul general al Uniunii.

TITLUL XI

DELEGAREA DE COMPETENȚE ȘI PROCEDURA COMITETULUI

Articolul 73

Exercitarea delegării

1. Competența de a adopta acte delegate este conferită Comisiei în condițiile prevăzute la prezentul articol.

2. Delegarea de competențe menționată la articolul 4, la articolul 7 alineatul (1), la articolul 11 alineatul (3), la articolul 43 alineatele (5) și (6) și la articolul 48 alineatul (5) se conferă Comisiei pe o perioadă nedeterminată de la [*intrarea în vigoare a regulamentului*].

3. Delegarea de competențe menționată la articolul 4, la articolul 7 alineatul (1), la articolul 11 alineatul (3), la articolul 43 alineatele (5) și (6) și la articolul 48 alineatul (5) poate fi revocată oricând de Parlamentul European sau de Consiliu. O decizie de revocare pune capăt delegării de competențe specificate în decizia respectivă. Decizia produce efecte din ziua următoare datei publicării acesteia în *Jurnalul Oficial al Uniunii Europene* sau de la o dată ulterioară menționată în decizie. Decizia nu aduce atingere actelor delegate care sunt deja în vigoare.

4. De îndată ce adoptă un act delegat, Comisia îl notifică simultan Parlamentului European și Consiliului.

5. Orice act delegat adoptat în temeiul articolului 4, al articolului 7 alineatul (1), al articolului 11 alineatul (3), al articolului 43 alineatele (5) și (6) și al articolului 48 alineatul (5) intră în vigoare numai în cazul în care nici Parlamentul European, nici Consiliul nu ridică obiecții în termen de trei luni de la data la care le-a fost notificat actul în cauză sau dacă, înainte de expirarea termenului respectiv, atât Parlamentul European, cât și Consiliul au informat Comisia că nu vor ridica obiecții. Respectivul termen se prelungește cu trei luni la inițiativa Parlamentului European sau a Consiliului.

Articolul 74

Procedura comitetului

1. Comisia este asistată de un comitet. Acesta reprezintă un comitet în sensul Regulamentului (UE) nr. 182/2011.

2. În cazul în care se face trimitere la prezentul alineat, se aplică articolul 5 din Regulamentul (UE) nr. 182/2011.

TITLUL XII

DISPOZIȚII FINALE

Articolul 75

Modificare adusă Regulamentului (CE) nr. 300/2008

La articolul 4 alineatul (3) din Regulamentul (CE) nr. 300/2008, se adaugă următorul paragraf:

„La adoptarea măsurilor detaliate referitoare la specificațiile tehnice și procedurile de aprobare și utilizare a echipamentelor de securitate privind sistemele de inteligență artificială în sensul Regulamentului (UE) YYY/XX [privind inteligența artificială] al Parlamentului European și al Consiliului*, se ține seama de cerințele prevăzute în titlul III capitolul 2 din regulamentul respectiv.

_____

* Regulamentul (UE) YYY/XX [privind inteligența artificială] (JO...).”

Articolul 76

Modificare adusă Regulamentului (UE) nr. 167/2013

La articolul 17 alineatul (5) din Regulamentul (UE) nr. 167/2013, se adaugă următorul paragraf:

„La adoptarea actelor delegate în temeiul primului paragraf privind sistemele de inteligență artificială care sunt componente de siguranță în sensul Regulamentului (UE) YYY/XX [privind inteligența artificială] al Parlamentului European și al Consiliului*, se ține seama de cerințele prevăzute în titlul III capitolul 2 din regulamentul respectiv.

_____

* Regulamentul (UE) YYY/XX [privind inteligența artificială] (JO...).”

Articolul 77

Modificare adusă Regulamentului (UE) nr. 168/2013

La articolul 22 alineatul (5) din Regulamentul (UE) nr. 168/2013, se adaugă următorul paragraf:

„La adoptarea actelor delegate în temeiul primului paragraf privind sistemele de inteligență artificială care sunt componente de siguranță în sensul Regulamentului (UE) YYY/XX [privind inteligența artificială] al Parlamentului European și al Consiliului*, se ține seama de cerințele prevăzute în titlul III capitolul 2 din regulamentul respectiv.

_____

* Regulamentul (UE) YYY/XX [privind inteligența artificială] (JO...).”

Articolul 78

Modificare adusă Directivei 2014/90/UE

La articolul 8 din Directiva 2014/90/UE, se adaugă următorul alineat:

„(4). Pentru sistemele de inteligență artificială care sunt componente de siguranță în sensul Regulamentului (UE) YYY/XX [privind inteligența artificială] al Parlamentului European și al Consiliului*, atunci când își desfășoară activitățile în temeiul alineatului (1) și atunci când adoptă specificații tehnice și standarde de testare în conformitate cu alineatele (2) și (3), Comisia ține seama de cerințele prevăzute în titlul III capitolul 2 din regulamentul respectiv.

_____

* Regulamentul (UE) YYY/XX [privind inteligența artificială] (JO...).”

Articolul 79

Modificare adusă Directivei (UE) 2016/797

La articolul 5 din Directiva (UE) 2016/797, se adaugă următorul alineat:

„(12) La adoptarea actelor delegate în temeiul alineatului (1) și a actelor de punere în aplicare în temeiul alineatului (11) privind sistemele de inteligență artificială care sunt componente de siguranță în sensul Regulamentului (UE) YYY/XX [privind inteligența artificială] al Parlamentului European și al Consiliului*, se ține seama de cerințele prevăzute în titlul III capitolul 2 din regulamentul respectiv.

_____

* Regulamentul (UE) YYY/XX [privind inteligența artificială] (JO...).”

Articolul 80

Modificare adusă Regulamentului (UE) 2018/858

La articolul 5 din Regulamentul (UE) 2018/858, se adaugă următorul alineat:

„(4). La adoptarea actelor delegate în temeiul alineatului (3) privind sistemele de inteligență artificială care sunt componente de siguranță în sensul Regulamentului (UE) YYY/XX [privind inteligența artificială] al Parlamentului European și al Consiliului*, se ține seama de cerințele prevăzute în titlul III capitolul 2 din regulamentul respectiv.

_____

* Regulamentul (UE) YYY/XX [privind inteligența artificială] (JO...).”

Articolul 81

Modificări aduse Regulamentului (UE) 2018/1139

Regulamentul (UE) 2018/1139 se modifică după cum urmează:

(1) La articolul 17, se adaugă următorul alineat:

„(3) Fără a aduce atingere alineatului (2), la adoptarea actelor de punere în aplicare în temeiul alineatului (1) privind sistemele de inteligență artificială care sunt componente de siguranță în

sensul Regulamentului (UE) YYY/XX [*privind inteligența artificială*] al Parlamentului European și al Consiliului*, se ține seama de cerințele prevăzute în titlul III capitolul 2 din regulamentul respectiv.

_____

* Regulamentul (UE) YYY/XX [privind inteligența artificială] (JO...).”

(2) La articolul 19, se adaugă următorul alineat:

„(4). La adoptarea actelor delegate în temeiul alineatelor (1) și (2) privind sistemele de inteligență artificială care sunt componente de siguranță în sensul Regulamentului (UE) YYY/XX [privind inteligența artificială], se ține seama de cerințele prevăzute în titlul III capitolul 2 din regulamentul respectiv.”

(3) La articolul 43, se adaugă următorul alineat:

„(4). La adoptarea actelor de punere în aplicare în temeiul alineatului (1) privind sistemele de inteligență artificială care sunt componente de siguranță în sensul Regulamentului (UE) YYY/XX [privind inteligența artificială], se ține seama de cerințele prevăzute în titlul III capitolul 2 din regulamentul respectiv.”

(4) La articolul 47, se adaugă următorul alineat:

„(3) La adoptarea actelor delegate în temeiul alineatelor (1) și (2) privind sistemele de inteligență artificială care sunt componente de siguranță în sensul Regulamentului (UE) YYY/XX [privind inteligența artificială], se ține seama de cerințele prevăzute în titlul III capitolul 2 din regulamentul respectiv.”

(5) La articolul 57, se adaugă următorul alineat:

„La adoptarea actelor de punere în aplicare privind sistemele de inteligență artificială care sunt componente de siguranță în sensul Regulamentului (UE) YYY/XX [privind inteligența artificială], se ține seama de cerințele prevăzute în titlul III capitolul 2 din regulamentul respectiv.”

(6) La articolul 58, se adaugă următorul alineat:

„(3) La adoptarea actelor delegate în temeiul alineatelor (1) și (2) privind sistemele de inteligență artificială care sunt componente de siguranță în sensul Regulamentului (UE) YYY/XX [privind inteligența artificială], se ține seama de cerințele prevăzute în titlul III capitolul 2 din regulamentul respectiv.”

Articolul 82

Modificări aduse Regulamentului (UE) 2019/2144

La articolul 11 din Regulamentul (UE) 2019/2144 se adaugă următorul alineat:

„(3) La adoptarea actelor de punere în aplicare în temeiul alineatului (2) privind sistemele de inteligență artificială care sunt componente de siguranță în sensul Regulamentului (UE) YYY/XX [privind inteligența artificială] al Parlamentului European și al Consiliului*, se ține seama de cerințele prevăzute în titlul III capitolul 2 din regulamentul respectiv.

_____

* Regulamentul (UE) YYY/XX [privind inteligența artificială] (JO...).”

Articolul 83

Sisteme de IA deja introduse pe piață sau puse în funcțiune

1. Prezentul regulament nu se aplică sistemelor IA care sunt componente ale sistemelor informatice la scară largă instituite prin actele juridice enumerate în anexa IX și care au fost introduse pe piață sau puse în funcțiune înainte de *[12 luni de la data aplicării prezentului regulament menționată la articolul 85 alineatul (2)]*, cu excepția cazului în care înlocuirea sau modificarea respectivelor acte juridice duce la o modificare semnificativă a proiectării sau a scopului preconizat al sistemului sau sistemelor de IA în cauză.

   Cerințele prevăzute în prezentul regulament sunt luate în considerare, după caz, la evaluarea fiecărui sistem informatic la scară largă instituit prin actele juridice enumerate în anexa IX care urmează să fie întreprinsă, astfel cum se prevede în actele respective.

2. Prezentul regulament se aplică sistemelor de IA cu grad ridicat de risc, altele decât cele menționate la alineatul (1), care au fost introduse pe piață sau puse în funcțiune înainte de [*data aplicării prezentului regulament menționată la articolul 85 alineatul (2)*], numai dacă, de la data respectivă, sistemele respective fac obiectul unor modificări semnificative în ceea ce privește proiectarea sau scopul preconizat.

Articolul 84

Evaluarea și revizuirea

1. Comisia evaluează necesitatea modificării listei din anexa III o dată pe an după intrarea în vigoare a prezentului regulament.

2. Până la [*trei ani de la data aplicării prezentului regulament menționată la articolul 85 alineatul (2)*] și, ulterior, o dată la patru ani, Comisia prezintă Parlamentului European și Consiliului un raport privind evaluarea și revizuirea prezentului regulament. Rapoartele sunt făcute publice.

3. Rapoartele menționate la alineatul (2) acordă o atenție deosebită următoarelor aspecte:

   (a) situația resurselor financiare și umane ale autorităților naționale competente în vederea îndeplinirii cu eficacitate a sarcinilor care le-au fost încredințate în temeiul prezentului regulament;

   (b) nivelul sancțiunilor, în special al amenzilor administrative, astfel cum sunt menționate la articolul 71 alineatul (1), aplicate de statele membre în cazul încălcării dispozițiilor prezentului regulament.

4. În termen de [*trei ani de la data aplicării prezentului regulament, menționată la articolul 85 alineatul (2)*] și, ulterior, o dată la patru ani, Comisia evaluează impactul și eficacitatea codurilor de conduită pentru a încuraja aplicarea cerințelor prevăzute în titlul III capitolul 2 și, eventual, a altor cerințe suplimentare pentru sistemele de IA, altele decât sistemele de IA cu grad ridicat de risc.

5. În sensul alineatelor (1) – (4), comitetul, statele membre și autoritățile naționale competente furnizează Comisiei informații la cererea acesteia.

6. La efectuarea evaluărilor și a revizuirilor menționate la alineatele (1) – (4), Comisia ține seama de pozițiile și constatările comitetului, ale Parlamentului European, ale Consiliului, precum și ale altor organisme sau surse relevante.

7. Comisia transmite, dacă este necesar, propuneri corespunzătoare de modificare a prezentului regulament, în special ținând seama de evoluțiile din domeniul tehnologiei și având în vedere progresele societății informaționale.

Articolul 85

Intrare în vigoare și aplicare

1. Prezentul regulament intră în vigoare în a douăzecea zi de la data publicării în *Jurnalul Oficial al Uniunii Europene*.

2. Prezentul regulament se aplică de la [24 luni de la intrarea în vigoare a regulamentului].

3. Prin derogare de la alineatul (2):

   (a) titlul III, capitolul 4 și titlul VI se aplică de la [*trei luni de la intrarea în vigoare a prezentului regulament*];

   (b) articolul 71 se aplică de la [douăsprezece luni de la intrarea în vigoare a prezentului regulament].

Prezentul regulament este obligatoriu în toate elementele sale și se aplică direct în toate statele membre.

Adoptat la Bruxelles,

Pentru Parlamentul European,	*Pentru Consiliu,*
Președintele	*Președintele*

FIȘĂ FINANCIARĂ LEGISLATIVĂ

1. CADRUL PROPUNERII/INIȚIATIVEI

1.1. Titlul propunerii/inițiativei

1.2. Domeniul (domeniile) de politică vizat(e)

1.3. Obiectul propunerii/inițiativei:

1.4. Obiectiv(e)

1.4.1. Obiectiv(e) general(e)

1.4.2. Obiectiv(e) specific(e)

1.4.3. Rezultatul (rezultatele) și impactul preconizate

1.4.4. Indicatori de performanță

1.5. Motivele propunerii/inițiativei

1.5.1. Cerința (cerințele) care trebuie îndeplinită (îndeplinite) pe termen scurt sau lung, inclusiv un calendar detaliat pentru punerea în aplicare a inițiativei

1.5.2. Valoarea adăugată a intervenției Uniunii (aceasta poate rezulta din diferiți factori, de exemplu o mai bună coordonare, securitatea juridică, o mai mare eficacitate sau complementaritate). În sensul prezentului punct, „valoarea adăugată a intervenției Uniunii” este valoarea ce rezultă din intervenția Uniunii care depășește valoarea ce ar fi fost obținută dacă ar fi acționat doar statele membre.

1.5.3. Învățăminte desprinse din experiențele anterioare similare

1.5.4. Compatibilitatea cu cadrul financiar multianual și posibilele sinergii cu alte instrumente corespunzătoare

1.5.5 Evaluarea diferitelor opțiuni de finanțare disponibile, inclusiv a posibilităților de redistribuire

1.6. Durata și impactul financiar ale propunerii/inițiativei

1.7. Modul (modurile) de gestiune preconizat(e)

2. MĂSURI DE GESTIUNE

2.1. Norme în materie de monitorizare și raportare

2.2. Sistemul de gestiune și de control

2.2.1. Justificarea modului/modurilor de gestiune, a mecanismului/mecanismelor de punere în aplicare a finanțării, a modalităților de plată și a strategiei de control propuse

2.2.2. Informații privind riscurile identificate și sistemul (sistemele) de control intern instituit(e) pentru atenuarea lor

2.2.3. Estimarea și justificarea raportului cost-eficacitate al controalelor (raportul „costurile controalelor ÷ valoarea fondurilor aferente gestionate”) și evaluarea nivelurilor preconizate ale riscurilor de eroare (la plată și la închidere)

2.3. Măsuri de prevenire a fraudelor și a neregulilor

3. IMPACTUL FINANCIAR ESTIMAT AL PROPUNERII/INIȚIATIVEI

3.1. Rubrica (rubricile) din cadrul financiar multianual și linia (liniile) bugetară (bugetare) de cheltuieli afectată (afectate)

3.2. Impactul financiar estimat al propunerii asupra creditelor

3.2.1. Sinteza impactului estimat asupra creditelor operaționale

3.2.2. Realizările preconizate finanțate din credite operaționale

3.2.3. Sinteza impactului estimat asupra creditelor administrative

3.2.4. Compatibilitatea cu cadrul financiar multianual actual

3.2.5. Contribuțiile terților

3.3. Impactul estimat asupra veniturilor

FIȘĂ FINANCIARĂ LEGISLATIVĂ

1. CADRUL PROPUNERII/INIȚIATIVEI

1.1. Titlul propunerii/inițiativei

Regulament al Parlamentului European și al Consiliului de stabilire a unor norme armonizate privind inteligența artificială (Legea privind inteligența artificială) și de modificare a anumitor acte legislative ale Uniunii

1.2. Domeniul (domeniile) de politică vizat(e)

Rețele de comunicare, conținut și tehnologie;

Piață internă, industrie, antreprenoriat și IMM-uri;

Impactul bugetar se referă la noile sarcini încredințate Comisiei, inclusiv la sprijinul acordat Comitetului pentru IA al UE;

Activitatea: Conturarea viitorului digital al Europei.

1.3. Obiectul propunerii/inițiativei:

X **o acțiune nouă**

☐ **o acțiune nouă întreprinsă ca urmare a unui proiect-pilot/a unei acțiuni pregătitoare**[64]

☐ **prelungirea unei acțiuni existente**

☐ **o acțiune reorientată către o acțiune nouă**

1.4. Obiectiv(e)

1.4.1. Obiectiv(e) general(e)

Obiectivul general al intervenției este de a asigura buna funcționare a pieței unice prin crearea condițiilor pentru dezvoltarea și utilizarea inteligenței artificiale de încredere în Uniune.

1.4.2. Obiectiv(e) specific(e)

Obiectivul specific nr. 1

Stabilirea unor cerințe specifice pentru sistemele de IA și a unor obligații pentru toți participanții la lanțul valoric, pentru a se asigura că sistemele de IA introduse pe piață și utilizate sunt sigure și respectă legislația existentă privind drepturile fundamentale și valorile Uniunii;

Obiectivul specific nr. 2

Asigurarea securității juridice pentru a facilita investițiile și inovarea în domeniul IA prin precizarea cerințelor esențiale, a obligațiilor, precum și a procedurilor de conformitate care trebuie urmate pentru a introduce sau utiliza un sistem de IA pe piața Uniunii;

Obiectivul specific nr. 3

[64] Astfel cum se menționează la articolul 54 alineatul (2) litera (a) sau (b) din Regulamentul financiar.

Consolidarea guvernanței și a aplicării eficace a legislației existente privind drepturile fundamentale și a cerințelor de siguranță aplicabile sistemelor de IA, prin indicarea de noi competențe, resurse și norme clare pentru autoritățile relevante în ceea ce privește procedurile de evaluare a conformității și de monitorizare *ex post,* precum și repartizarea sarcinilor de guvernanță și de supraveghere între nivelul național și nivelul UE;

Obiectivul specific nr. 4

Facilitarea dezvoltării unei piețe unice pentru aplicații de IA legale, sigure și de încredere și prevenirea fragmentării pieței prin luarea de măsuri la nivelul UE pentru a stabili cerințe minime pentru ca sistemele de IA să fie introduse și utilizate pe piața Uniunii în conformitate cu legislația în vigoare privind drepturile fundamentale și siguranța.

1.4.3. Rezultatul (rezultatele) și impactul preconizate

A se preciza efectele pe care ar trebui să le aibă propunerea/inițiativa asupra beneficiarilor vizați/grupurilor vizate.

Furnizorii de IA ar trebui să beneficieze de un set minim, dar clar, de cerințe, care să garanteze securitate juridică și să asigure accesul la întreaga piață unică.

Utilizatorii IA ar trebui să beneficieze de securitatea juridică că sistemele de IA cu grad ridicat de risc pe care le cumpără respectă legile și valorile europene.

Consumatorii ar trebui să beneficieze de reducerea riscului de încălcare a siguranței sau a drepturilor lor fundamentale.

1.4.4. Indicatori de performanță

A se specifica indicatorii pentru monitorizarea punerii în aplicare a propunerii/inițiativei.

Indicatorul 1

Numărul de incidente grave sau de performanțe IA care constituie un incident grav sau o încălcare a obligațiilor privind drepturile fundamentale (semestrial) pe domenii de aplicare și calculate a) în termeni absoluți, b) ca procent al aplicațiilor utilizate și c) ca procent al cetățenilor vizați.

Indicatorul 2

a) Totalul investițiilor în IA în UE (anual)

b) Totalul investițiilor în IA per stat membru (anual)

c) Procentul întreprinderilor care utilizează IA (anual)

d) Procentul IMM-urilor care utilizează IA (anual)

a) și b) vor fi calculate pe baza surselor oficiale și vor fi comparate cu estimările private

c) și d) vor fi colectate prin anchete periodice în rândul întreprinderilor

1.5. Motivele propunerii/inițiativei

1.5.1. Cerința (cerințele) care trebuie îndeplinită (îndeplinite) pe termen scurt sau lung, inclusiv un calendar detaliat pentru punerea în aplicare a inițiativei

Regulamentul ar trebui să fie pe deplin aplicabil la un an și jumătate de la adoptarea sa. Cu toate acestea, înainte de această dată ar trebui să fie instituite elemente ale structurii de guvernanță. În special, statele membre trebuie să fi numit în prealabil autorități existente și/sau să fi instituit autorități noi care să îndeplinească sarcinile prevăzute în legislație, iar Comitetul pentru IA al UE ar trebui să fie înființat și eficace. Până la momentul aplicabilității, baza de date europeană a sistemelor de IA ar trebui să fie pe deplin operațională. Prin urmare, în paralel cu procesul de adoptare, este necesară dezvoltarea bazei de date, astfel încât dezvoltarea sa să se încheie odată cu intrarea în vigoare a regulamentului.

1.5.2. Valoarea adăugată a intervenției Uniunii (aceasta poate rezulta din diferiți factori, de exemplu o mai bună coordonare, securitatea juridică, o mai mare eficacitate sau complementaritate). În sensul prezentului punct, „valoarea adăugată a intervenției Uniunii" este valoarea ce rezultă din intervenția Uniunii care depășește valoarea ce ar fi fost obținută dacă ar fi acționat doar statele membre în mod individual.

Apariția unui cadru neuniform de norme naționale potențial divergente va împiedica furnizarea fără sincope a sistemelor de IA în întreaga UE și este ineficace în asigurarea siguranței și a protecției drepturilor fundamentale și a valorilor Uniunii în diferitele state membre. O acțiune legislativă comună a UE privind IA ar putea stimula piața internă și are un mare potențial de a oferi industriei europene un avantaj competitiv la nivel mondial și economii de scară care nu pot fi realizate de statele membre în mod individual.

1.5.3. Învățăminte desprinse din experiențele anterioare similare

Directiva 2000/31/CE privind comerțul electronic oferă cadrul principal pentru funcționarea pieței unice și supravegherea serviciilor digitale și stabilește o structură de bază pentru un mecanism de cooperare generală între statele membre, care acoperă, în principiu, toate cerințele aplicabile serviciilor digitale. Evaluarea directivei a evidențiat deficiențe în privința mai multor aspecte ale acestui mecanism de cooperare, inclusiv aspecte procedurale importante, cum ar fi lipsa unor termene clare în care statele membre trebuie să formuleze un răspuns, la care se adaugă o lipsă generală de reacție la solicitările omologilor lor. Acest lucru a dus de-a lungul anilor la o lipsă de încredere între statele membre în abordarea preocupărilor legate de furnizorii care oferă servicii digitale la nivel transfrontalier. Evaluarea directivei a demonstrat necesitatea definirii unui set diferențiat de norme și cerințe la nivel european. Din acest motiv, punerea în aplicare a obligațiilor specifice prevăzute în prezentul regulament ar necesita un mecanism specific de cooperare la nivelul UE, cu o structură de guvernanță care să asigure coordonarea organismelor responsabile specifice la nivelul UE.

1.5.4. Compatibilitatea cu cadrul financiar multianual și posibilele sinergii cu alte instrumente corespunzătoare

Regulamentul de stabilire a unor norme armonizate privind inteligența artificială și de modificare a anumitor acte legislative ale Uniunii definește un nou cadru comun de cerințe aplicabile sistemelor de IA, care depășește cadrul prevăzut de legislația existentă. De aceea, prin prezenta propunere trebuie să se instituie o nouă funcție de reglementare și supraveghere la nivel național și european.

În ceea ce privește posibilele sinergii cu alte instrumente adecvate, rolul autorităților de notificare la nivel național poate fi îndeplinit de autoritățile naționale care îndeplinesc funcții similare în temeiul altor regulamente ale UE.

În plus, prin creșterea gradului de încredere în IA și, astfel, prin încurajarea investițiilor în dezvoltarea și adoptarea IA, aceasta completează programul „Europa digitală", pentru care promovarea difuzării IA este una dintre cele cinci priorități.

1.5.5. Evaluarea diferitelor opțiuni de finanțare disponibile, inclusiv a posibilităților de redistribuire

Personalul va fi redistribuit. Celelalte costuri vor fi finanțate din pachetul DEP. având în vedere că obiectivul prezentului regulament – asigurarea unei inteligențe

artificiale de încredere – contribuie în mod direct la un obiectiv-cheie al programului „Europa digitală” – accelerarea dezvoltării și a implementării IA în Europa.

1.6. Durata și impactul financiar ale propunerii/inițiativei

☐ **durată limitată**

– ☐ de la [ZZ/LL]AAAA până la [ZZ/LL]AAAA

– ☐ Impact financiar din AAAA până în AAAA pentru creditele de angajament și din AAAA până în AAAA pentru creditele de plată.

X **durată nelimitată**

– Punere în aplicare cu o perioadă de începere de unu/doi (urmează să fie confirmat) ani,

– urmată de o perioadă de funcționare la capacitate maximă.

1.7. Modul (modurile) de gestiune preconizat(e)[65]

X **Gestiune directă** asigurată de Comisie

– ☐ prin intermediul departamentelor sale, inclusiv al personalului din delegațiile Uniunii;

– ☐ prin intermediul agențiilor executive

☐ **Gestiune partajată** cu statele membre

☐ **Gestiune indirectă**, cu delegarea sarcinilor de execuție bugetară către:

– ☐ țări terțe sau organisme pe care le-au desemnat acestea;

– ☐ organizații internaționale și agenții ale acestora (a se preciza);

– ☐ BEI și Fondului european de investiții;

– ☐ organismele menționate la articolele 70 și 71 din Regulamentul financiar;

– ☐ organisme de drept public;

– ☐ organisme de drept privat cu misiune de serviciu public, cu condiția să prezinte garanții financiare adecvate;

– ☐ organisme de drept privat dintr-un stat membru care sunt responsabile cu punerea în aplicare a unui parteneriat public-privat și care prezintă garanții financiare adecvate;

– ☐ persoane cărora li se încredințează executarea unor acțiuni specifice în cadrul PESC, în temeiul titlului V din TUE, și care sunt identificate în actul de bază relevant.

– *Dacă se indică mai multe moduri de gestiune, a se furniza detalii suplimentare în secțiunea „Observații”.*

Observații

[65] Explicații detaliate privind modurile de gestiune, precum și trimiterile la Regulamentul financiar sunt disponibile pe site-ul BudgWeb: http://www.cc.cec/budg/man/budgmanag/budgmanag_en.html.

2. MĂSURI DE GESTIUNE

2.1. Norme în materie de monitorizare și raportare

A se preciza frecvența și condițiile.

Regulamentul va fi revizuit și evaluat la cinci ani de la intrarea în vigoare a regulamentului. Comisia trebuie va prezenta Parlamentului European, Consiliului și Comitetului Economic și Social European un raport privind constatările evaluării.

2.2. Sistemul (sistemele) de gestiune și de control

2.2.1. Justificarea modului/modurilor de gestiune, a mecanismului/mecanismelor de punere în aplicare a finanțării, a modalităților de plată și a strategiei de control propuse

Regulamentul stabilește o nouă politică în ceea ce privește normele armonizate pentru furnizarea de sisteme de inteligență artificială pe piața internă, asigurând în același timp respectarea siguranței și a drepturilor fundamentale. Aceste noi norme necesită un mecanism pentru asigurarea coerenței pentru aplicarea transfrontalieră a obligațiilor în temeiul prezentului regulament, sub forma unui nou grup consultativ care coordonează activitățile autorităților naționale.

Este necesar să se aloce resurse adecvate serviciilor Comisiei pentru a le permite să facă față acestor noi sarcini. Se estimează că punerea în aplicare a noului regulament necesită 10 ENI în total (5 ENI pentru sprijinirea activităților comitetului și 5 ENI pentru Autoritatea Europeană pentru Protecția Datelor, care acționează în calitate de organism de notificare pentru sistemele de IA implementate de un organism al Uniunii Europene).

2.2.2. Informații privind riscurile identificate și sistemul (sistemele) de control intern instituit(e) pentru atenuarea lor

Pentru a se asigura că membrii comitetului au posibilitatea de a efectua analize în cunoștință de cauză pe baza unor dovezi concrete, se prevede ca acesta să fie sprijinit de structura administrativă a Comisiei și să se creeze un grup de experți care să furnizeze expertiză suplimentară atunci când este necesar.

2.2.3. Estimarea și justificarea raportului cost-eficacitate al controalelor (raportul „costurile controalelor ÷ valoarea fondurilor aferente gestionate”) și evaluarea nivelurilor preconizate ale riscurilor de eroare (la plată și la închidere)

Pentru cheltuielile legate de reuniuni, având în vedere valoarea scăzută per tranzacție (de exemplu, rambursarea cheltuielilor de deplasare pentru un delegat pentru o reuniune), procedurile standard de control par a fi suficiente. În ceea ce privește dezvoltarea bazei de date, atribuirea contractelor dispune de un sistem solid de control intern în cadrul DG CNECT, prin intermediul unor activități centralizate de achiziții publice.

2.3. Măsuri de prevenire a fraudelor și a neregulilor

A se preciza măsurile de prevenire și de protecție existente sau preconizate, de exemplu din strategia antifraudă.

Măsurile de prevenire a fraudei aplicabile Comisiei se vor aplica și creditelor suplimentare necesare pentru punerea în aplicare a prezentului regulament.

3. IMPACTUL FINANCIAR ESTIMAT AL PROPUNERII/INIȚIATIVEI

3.1. Rubrica (rubricile) din cadrul financiar multianual și linia (liniile) bugetară (bugetare) de cheltuieli afectată (afectate)

- Linii bugetare existente

În ordinea rubricilor din cadrul financiar multianual și a liniilor bugetare.

Rubrica din cadrul financiar multianual	Linia bugetară	Tip de cheltuieli	Contribuție			
	Număr	Dif./Nedif. [66]	din partea țărilor AELS[67]	din partea țărilor candidate[68]	din partea țărilor terțe	în sensul articolului 21 alineatul (2) litera (b) din Regulamentul financiar
7	20 02 06 Cheltuieli administrative	Nedif.	NU	NU	NU	NU
1	02 04 03 DEP inteligență artificială	Dif.	DA	NU	NU	NU
1	02 01 30 01 Cheltuieli de sprijin pentru programul Europa digitală	Nedif.	DA	NU	NU	NU

3.2. Impactul financiar estimat al propunerii asupra creditelor

3.2.1. Sinteza impactului estimat asupra cheltuielilor cu creditelor operaționale

– ☐ Propunerea/inițiativa nu implică utilizarea de credite operaționale

– X Propunerea/inițiativa implică utilizarea de credite operaționale, conform explicațiilor de mai jos:

[66] Dif. = credite diferențiate / Nedif. = credite nediferențiate.
[67] AELS: Asociația Europeană a Liberului Schimb.
[68] Țările candidate și, după caz, țările potențial candidate din Balcanii de Vest.

milioane EUR (cu trei zecimale)

Rubrica din cadrul financiar multianual	1	

DG: CNECT				**2022**	**2023**	**2024**	**2025**	**2026**	**2027**[69]	**TOTAL**	
• Credite operaționale											
Linia bugetară[70] 02 04 03		Angajamente	(1a)		1,000						**1,000**
		Plăți	(2a)		0,600	0,100	0,100	0,100	0,100		**1,000**
Linia bugetară		Angajamente	(1b)								
		Plăți	(2b)								
Credite cu caracter administrativ finanțate din bugetul unor programe specifice[71]											
Linia bugetară 02 01 30 01			(3)		0,240	0,240	0,240	0,240	0,240		**1,200**
TOTAL credite pentru DG CNECT		Angajamente	=1a+1b +3		**1,240**		**0,240**	**0,240**	**0,240**		**2,200**
		Plăți	=2a+2b +3		**0,840**	**0,340**	**0,340**	**0,340**	**0,340**		**2,200**

69 Orientativ și în funcție de disponibilitățile bugetare.

70 În conformitate cu nomenclatura bugetară oficială.

71 Asistență tehnică și/sau administrativă și cheltuieli de sprijin pentru punerea în aplicare a programelor și/sau a acțiunilor UE (fostele linii „BA”), cercetare indirectă și cercetare directă.

• TOTAL credite operaționale	Angajamente	(4)		1,000						**1,000**
	Plăți	(5)		0,600	0,100	0,100	0,100	0,100		**1,000**
• TOTAL credite cu caracter administrativ finanțate din bugetul unor programe specifice		(6)		**0,240**	**0,240**	**0,240**	**0,240**	**0,240**		**1,200**
TOTAL credite la RUBRICA 1 din cadrul financiar multianual	Angajamente	=4+6		1,240	0,240	0,240	0,240	0,240		**2,200**
	Plăți	=5+6		0,840	0,340	0,340	0,340	0,340		**2,200**

<u>În cazul în care propunerea/inițiativa afectează mai multe rubrici operaționale, a se repeta secțiunea de mai sus:</u>

• TOTAL credite operaționale (toate rubricile operaționale)	Angajamente	(4)								
	Plăți	(5)								
• TOTAL credite cu caracter administrativ finanțate din bugetul unor programe specifice (toate rubricile operaționale)		(6)								
TOTAL credite de la RUBRICILE 1-6 din cadrul financiar multianual (Suma de referință)	Angajamente	=4+6								
	Plăți	=5+6								

Rubrica din cadrul financiar multianual	**7**	„Cheltuieli administrative”

Această secțiune ar trebui completată utilizând „datele bugetare cu caracter administrativ” care trebuie introduse mai întâi în anexa la fișa financiară legislativă (anexa V la normele interne), încărcată în DECIDE pentru consultarea interservicii.

milioane EUR (cu trei zecimale)

		2023	**2024**	**2025**	**2026**	Anul **2027**	**După 2027**[72]	**TOTAL**
DG: CNECT								
• Resurse umane		0,760	0,760	0,760	0,760	0,760	0,760	**3,800**
• Alte cheltuieli administrative		**0,010**	**0,010**	**0,010**	**0,010**	**0,010**	**0,010**	**0,050**
TOTAL DG CNECT	**Credite**	**0,760**	**0,760**	**0,760**	**0,760**	**0,760**	**0,760**	**3,850**
Autoritatea Europeană pentru Protecția Datelor								
• Resurse umane		0,760	0,760	0,760	0,760	0,760	0,760	**3,800**
• Alte cheltuieli administrative								
TOTAL AEPD	**Credite**	**0,760**	**0,760**	**0,760**	**0,760**	**0,760**	**0,760**	**3,800**
TOTAL credite de la RUBRICA 7 din cadrul financiar multianual	(Total angajamente = Total plăți)	1,530	1,530	1,530	1,530	1,530	1,530	**7,650**

milioane EUR (cu trei zecimale)

	2022	**2023**	**2024**	**2025**	Anul **2026**	Anul **2027**		**TOTAL**

[72] Toate cifrele din această coloană sunt orientative și sunt furnizate sub rezerva continuării programelor și a disponibilității creditelor.

TOTAL credite de la RUBRICILE 1-7 din cadrul financiar multianual	Angajamente		2,770	1,770	1,770	1,770	1,770		**9,850**
	Plăți		2,370	1,870	1,870	1,870	1,870		**9,850**

3.2.2. Realizările preconizate finanțate din credite operaționale

Credite de angajament în milioane EUR (cu trei zecimale)

A se indica obiectivele și realizările ⇩			Anul **2022**		Anul **2023**		Anul **2024**		Anul **2025**		Anul **2026**		Anul **2027**		După anul **2027**[73]		**TOTAL**	
	REALIZĂRI																	
	Tip	Costuri medii	Nr.	Costuri	Nr.	Costuri	Nr.	Costuri	Nr.	Costuri	Nr.	Costuri	Nr.	Costuri	Nr.	Costuri	Total nr.	Total costuri
OBIECTIVUL SPECIFIC NR. 1[74]…																		
Baza de date					1	1,000	1		1		1		1		1	0,100	1	1,000
Reuniuni – Realizare					10	0,200	10	0,200	10	0,200	10	0,200	10	0,200	10	0,200	50	1,000
Activități de comunicare					2	0,040	2	0,040	2	0,040	2	0,040	2	0,040	2	0,040	10	0,040
Subtotal pentru obiectivul specific nr. 1																		
OBIECTIVUL SPECIFIC NR. 2…																		
– Realizare																		
Subtotal pentru obiectivul specific nr. 2																		
TOTALURI					13	0,240	13	0,240	13	0,240	13	0,240	13	0,240	13	0,100	65	2,200

[73] Toate cifrele din această coloană sunt orientative și sunt furnizate sub rezerva continuării programelor și a disponibilității creditelor.

[74] Conform descrierii de la punctul 1.4.2. „Obiectiv(e) specific(e)…”.

3.2.3. Sinteza impactului estimat asupra creditelor administrative

– ☐ Propunerea/inițiativa nu implică utilizarea de credite cu caracter administrativ

– X Propunerea/inițiativa implică utilizarea de credite cu caracter administrativ, conform explicațiilor de mai jos:

milioane EUR (cu trei zecimale)

	Anul **2022**	Anul **2023**	Anul **2024**	Anul **2025**	Anul **2026**	Anul **2027**	**Anual după 2027**[75]	**TOTAL**
HEADING 7 din cadrul financiar multianual								
Resurse umane		1,520	1,520	1,520	1,520	1,520	**1,520**	**7,600**
Alte cheltuieli administrative		0,010	0,010	0,010	0,010	0,010	**0,010**	**0,050**
Subtotal HEADING 7 din cadrul financiar multianual		1,530	1,530	1,530	1,530	1,530	**1,530**	**7,650**

În afara RUBRICII 7[76] **din cadrul financiar multianual**								
Resurse umane								
Alte cheltuieli cu caracter administrativ		0,240	0,240	0,240	0,240	0,240	**0,240**	**1,20**
Subtotal în afara RUBRICII 7 cadrului financiar multianual		0,240	0,240	0,240	0,240	0,240	**0,240**	**1,20**

TOTAL		**1,770**	**1,770**	**1,770**	**1,770**	**1,770**	**1,770**	**8,850**

Necesarul de credite pentru resursele umane și pentru alte cheltuieli cu caracter administrativ va fi acoperit de creditele direcției generale (DG) respective care sunt deja alocate pentru gestionarea acțiunii și/sau au fost redistribuite intern în cadrul DG-ului respectiv, completate, după caz, cu resurse suplimentare care ar putea fi alocate DG-ului care gestionează acțiunea în cadrul procedurii anuale de alocare și ținând seama de constrângerile bugetare.

75 Toate cifrele din această coloană sunt orientative și sunt furnizate sub rezerva continuării programelor și a disponibilității creditelor.

76 Asistență tehnică și/sau administrativă și cheltuieli de sprijin pentru punerea în aplicare a programelor și/sau a acțiunilor UE (fostele linii „BA”), cercetare indirectă și cercetare directă.

3.2.3.1. Necesarul de resurse umane estimat

– ☐ Propunerea/inițiativa nu implică utilizarea de resurse umane.

– X Propunerea/inițiativa implică utilizarea de resurse umane, conform explicațiilor de mai jos:

Estimări în echivalent normă întreagă

.		Anul **2023**	Anul **2024**	Anul **2025**	**2026**	**2027**	**După 2027**[77]	
•Posturi din schema de personal (funcționari și agenți temporari)								
20 01 02 01 (sediu și în reprezentanțele Comisie)		10	10	10	10	10	10	
20 01 02 03 (delegații)								
01 01 01 01 (cercetare indirectă)								
01 01 01 11 (cercetare directă)								
Alte linii bugetare (a se preciza)								
• Personal extern (în echivalent normă întreagă: ENI)[78]								
20 02 01 (AC, END, INT din „pachetul global")								
20 02 03 (AC, AL, END, INT și JPD în delegații)								
XX 01 xx **yy zz** [79]	- la sediu							
	- în delegații							
01 01 01 02 (AC, END, INT – cercetare indirectă)								
01 01 01 12 (AC, END, INT - cercetare directă)								
Alte linii bugetare (a se preciza)								
TOTAL		**10**	**10**	**10**	**10**	**10**	**10**	

XX este domeniul de politică sau titlul din buget în cauză.

Necesarul de resurse umane va fi asigurat din efectivele de personal ale DG-ului în cauză alocate deja pentru gestionarea acțiunii și/sau redistribuite intern în cadrul DG-ului, completate, după caz, cu resurse suplimentare ce ar putea fi acordate DG-ului care gestionează acțiunea în cadrul procedurii anuale de alocare și ținând seama de constrângerile bugetare.

Se preconizează că AEPD va furniza jumătate din resursele necesare.

Descrierea sarcinilor care trebuie efectuate:

Funcționari și personal temporar	Pentru a pregăti un total de 13-16 reuniuni, proiecte de rapoarte, continuarea activității în materie de politici, de exemplu în ceea ce privește viitoarele modificări ale listei aplicațiilor de IA cu grad ridicat de risc și menținerea relațiilor cu autoritățile statelor membre, vor fi necesare patru posturi AD ENI și 1 post AST ENI. În ceea ce privește sistemele de IA dezvoltate de instituțiile UE, Autoritatea Europeană pentru Protecția Datelor este responsabilă. Pe baza experienței anterioare, se poate estima că sunt necesare 5 posturi de AD ENI pentru îndeplinirea responsabilităților AEPD în temeiul proiectului legislativ.

[77] Toate cifrele din această coloană sunt orientative și sunt furnizate sub rezerva continuării programelor și a disponibilității creditelor.

[78] AC = agent contractual; AL= agent local; END = expert național detașat; INT = personal pus la dispoziție de agenți de muncă temporară; JPD = tânăr profesionist în delegații.

[79] Subplafonul pentru personal extern acoperit din creditele operaționale (fostele linii „BA").

Personal extern	

3.2.4. Compatibilitatea cu cadrul financiar multianual actual

Propunerea/inițiativa:

– X poate fi finanțată integral prin realocarea creditelor în cadrul rubricii relevante din cadrul financiar multianual (CFM).

Nu este necesară reprogramarea.

– ☐ necesită utilizarea marjei nealocate din cadrul rubricii corespunzătoare din CFM și/sau utilizarea instrumentelor speciale, astfel cum sunt definite în Regulamentul privind CFM.

A se explica necesitatea efectuării acestei acțiuni, precizând rubricile și liniile bugetare vizate, sumele aferente și instrumentele propuse a fi utilizate.

– ☐ necesită revizuirea CFM.

A se explica necesitatea efectuării acestei acțiuni, precizând rubricile și liniile bugetare vizate, precum și sumele aferente.

3.2.5. Contribuțiile terților

Propunerea/inițiativa:

– X nu prevede cofinanțare din partea terților

– ☐prevede cofinanțare din partea terților, estimată mai jos:

Credite în milioane EUR (cu trei zecimale)

	Anul N[80]	**Anul N+1**	**Anul N+2**	**Anul N+3**	A se introduce atâția ani câți sunt considerați necesari pentru a reflecta durata impactului (a se vedea punctul 1.6)			Total
A se preciza organismul care asigură cofinanțarea								
TOTAL credite cofinanțate								

[80] Anul N este anul în care începe punerea în aplicare a propunerii/inițiativei. Vă rugăm să înlocuiți „N” cu primul an estimat de punere în aplicare (de exemplu: 2021). Se procedează la fel pentru anii următori.

3.3. Impactul estimat asupra veniturilor

– ☐ Propunerea/inițiativa are următorul impact financiar:

– ☐ Propunerea/inițiativa are următorul impact financiar:

  – ☐ asupra altor venituri

  – ☐ asupra altor venituri

  – vă rugăm să precizați dacă veniturile sunt alocate unor linii de cheltuieli☐

milioane EUR (cu trei zecimale)

Linia bugetară pentru venituri:	Credite disponibile pentru exercițiul financiar în curs	Impactul propunerii/inițiativei[81]						
		Anul **N**	**Anul N+1**	**Anul N+2**	**Anul N+3**	A se introduce atâția ani câți sunt considerați necesari pentru a reflecta durata impactului (a se vedea punctul 1.6)		
Articolul …..								

Pentru veniturile alocate, a se preciza linia (liniile) bugetară (bugetare) de cheltuieli afectată (afectate).

Alte observații (de exemplu, metoda/formula utilizată pentru calcularea impactului asupra veniturilor sau orice altă informație).

[81] În ceea ce privește resursele proprii tradiționale (taxe vamale, cotizații pentru zahăr), sumele indicate trebuie să fie sume nete, și anume sumele brute după deducerea unei cote de 20 % pentru costurile de colectare.