Consiliul
Uniunii Europene

Bruxelles, 25 noiembrie 2022
(OR. en)

14954/22

Dosar interinstituțional:
2021/0106(COD)

LIMITE

TELECOM 472
JAI 1494
COPEN 396
CYBER 374
DATAPROTECT 320
EJUSTICE 89
COSI 293
IXIM 267
ENFOPOL 569
RELEX 1556
MI 843
COMPET 918
CODEC 1773

NOTĂ

Sursă:	Comitetul Reprezentanților Permanenți (partea I)
Destinatar:	Consiliul
Nr. doc. ant.:	14336/22
Nr. doc. Csie:	8115/21
Subiect:	Propunere de regulament al Parlamentului European și al Consiliului de stabilire a unor norme armonizate privind inteligența artificială (Actul privind inteligența artificială) și de modificare a anumitor acte legislative ale Uniunii - Abordare generală

I. INTRODUCERE

1. Comisia a adoptat propunerea de regulament de stabilire a unor norme armonizate privind inteligența artificială (**Actul privind inteligența artificială**) la 21 aprilie 2021.

2. Obiectivele propunerii Comisiei sunt garantarea faptului că sistemele de IA introduse pe piața Uniunii și utilizate în Uniune 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 siguranța, precum și facilitarea dezvoltării unei piețe unice pentru aplicații de IA legale, sigure și de încredere, prevenind în același timp fragmentarea pieței.

II. LUCRĂRILE DESFĂȘURATE ÎN CADRUL ALTOR INSTITUȚII

3. În cadrul Parlamentului European dezbaterile sunt conduse de Comisia pentru piața internă și protecția consumatorilor (IMCO; raportor: Brando Benifei, S&D, Italia) și Comisia pentru libertăți civile, justiție și afaceri interne (LIBE; raportor: Dragos Tudorache, Renew, România) în cadrul procedurii reuniunilor comune ale comisiilor. Comisia pentru afaceri juridice (JURI), Comisia pentru industrie, cercetare și energie (ITRE) și Comisia pentru cultură și educație (CULT) sunt asociate la activitatea legislativă cu competențe partajate și/sau exclusive. Cei doi coraportori și-au prezentat proiectul de raport în aprilie 2022, iar votul privind raportul comun IMCO-LIBE este programat pentru primul trimestru al anului 2023.

4. Comitetul Economic și Social European și-a emis avizul cu privire la propunere la 22 septembrie 2021, iar Comitetul European al Regiunilor i-a urmat cu propriul său aviz la 2 decembrie 2021.

5. La 18 iunie 2021, Comitetul european pentru protecția datelor (CEPD) și Autoritatea Europeană pentru Protecția Datelor (AEPD) au emis un aviz comun cu privire la propunere.

6. Banca Centrală Europeană (BCE) și-a emis avizul la 29 decembrie 2021 și l-a prezentat Grupului de lucru pentru telecomunicații și societatea informațională (denumit în continuare „Grupul de lucru TELECOM”) la 10 februarie 2022.

III. STADIUL LUCRĂRILOR ÎN CADRUL CONSILIULUI

1. În cadrul Consiliului, propunerea a fost examinată în cadrul Grupului de lucru TELECOM. Grupul de lucru TELECOM a început discuțiile cu privire la propunere în timpul președinției portugheze, în perioada aprilie-iunie 2021 fiind organizate mai multe reuniuni și ateliere. Lucrările cu privire la propunere au continuat în timpul președinției slovene, care a elaborat prima propunere parțială de compromis care vizează **articolele 1-7** și anexele I-III. În plus, președinția slovenă a organizat o reuniune informală de o jumătate de zi a Consiliului miniștrilor telecomunicațiilor dedicată exclusiv propunerii de Act privind inteligența artificială, în cursul căreia miniștrii și-au confirmat sprijinul pentru abordarea orizontală și centrată pe factorul uman a reglementării IA. Președinția franceză a continuat procesul de examinare și, până la sfârșitul mandatului său, a reformulat părțile rămase ale textului (**articolele 8-85 și anexele IV-IX**), iar la 17 iunie 2022 a prezentat prima propunere de compromis consolidată integrală referitoare la Actul privind IA.

2. La 5 iulie 2022, președinția cehă a organizat o dezbatere de orientare în cadrul Grupului de lucru TELECOM pe baza unui document privind opțiunile de politică, ale cărui rezultate au fost utilizate pentru pregătirea **celui de al doilea text de compromis**. Pe baza reacțiilor delegațiilor la acest compromis, președinția cehă a pregătit **cel de al treilea text de compromis**, care a fost prezentat și discutat în cadrul Grupului de lucru TELECOM la 22 și 29 septembrie 2022. În urma acestor discuții, delegațiilor li s-a solicitat să prezinte observații scrise suplimentare, care au fost utilizate de președinția cehă pentru a redacta **cea de a patra propunere de compromis**. Pe baza discuțiilor privind cea de a patra propunere de compromis, care au avut loc în cadrul Grupului de lucru TELECOM la 25 octombrie 2022 și la 8 noiembrie 2022, și ținând seama de observațiile scrise finale din partea statelor membre, președinția cehă a pregătit **versiunea finală a textului de compromis**, care figurează în anexă. La 18 noiembrie, Coreperul a examinat această propunere de compromis și **a convenit în unanimitate să o transmită Consiliului TTE (Telecomunicații), fără modificări, în vederea unei abordări generale** în cadrul reuniunii sale din 6 decembrie 2022.

IV. PRINCIPALELE ELEMENTE ALE PROPUNERII DE COMPROMIS

1. **Definiția unui sistem de IA, practicile interzise în domeniul IA, lista cazurilor de utilizare a IA cu grad ridicat de risc din anexa III și clasificarea sistemelor de IA ca prezentând un grad ridicat de risc**

1.1 Pentru a se asigura că definiția unui sistem de IA oferă criterii suficient de clare pentru a distinge IA de sistemele software mai clasice, textul de compromis restrânge definiția de la **articolul 3 alineatul (1)** la sistemele dezvoltate prin abordări bazate pe învățarea automată și abordări bazate pe logică și pe cunoaștere.

1.2 În ceea ce privește delegarea de competențe către Comisie pentru actualizările definiției unui sistem de IA, au fost eliminate **anexa I** și delegarea corespunzătoare de competențe Comisiei pentru a actualiza definiția prin intermediul unor acte delegate. În schimb, au fost adăugate noile **considerente 6a și 6b** pentru a clarifica ce ar trebui să se înțeleagă prin abordările bazate pe învățarea automată și prin abordări bazate pe logică și pe cunoaștere. Pentru a se asigura că Actul privind IA rămâne flexibil și adaptat exigențelor viitorului, la **articolul 4** a fost adăugată posibilitatea de a adopta acte de punere în aplicare pentru a detalia și a actualiza tehnicile din cadrul abordărilor bazate pe învățarea automată și al abordărilor bazate pe logică și pe cunoaștere.

1.3 În ceea ce privește practicile interzise în domeniul IA, **la articolul 5**, textul de compromis cuprinde extinderea interdicției de a utiliza IA pentru evaluarea comportamentului social inclusiv la actorii privați. În plus, dispoziția care interzice utilizarea sistemelor de IA ce exploatează vulnerabilitățile unui anumit grup de persoane acoperă în prezent și persoanele care sunt vulnerabile din cauza situației lor sociale sau economice. În ceea ce privește interzicerea utilizării sistemelor de identificare biometrică la distanță „în timp real” în spațiile accesibile publicului de către autoritățile de aplicare a legii, textul de compromis clarifică obiectivele pentru cazurile în care o astfel de utilizare este considerată strict necesară în scopul asigurării respectării legii și în care, în consecință, autorităților de aplicare a legii ar trebui să li se permită în mod excepțional să utilizeze astfel de sisteme.

1.4 În ceea ce privește lista cazurilor de utilizare a IA cu grad ridicat de risc din **anexa III**, trei dintre acestea au fost eliminate (detectarea deepfake-urilor de către autoritățile de aplicare a legii, analiza infracționalității, verificarea autenticității documentelor de călătorie), două au fost adăugate (infrastructura digitală critică și asigurările de viață și de sănătate), iar altele au fost adaptate. În același timp, **articolul 7 alineatul (1)** a fost modificat pentru a oferi, pe lângă posibilitatea de a adăuga pe listă cazurile de utilizare cu risc ridicat prin intermediul actelor delegate, și posibilitatea de a le elimina. Pentru a se asigura că drepturile fundamentale sunt protejate în mod adecvat în cazul unor astfel de eliminări, la **articolul 7 alineatul (3)** au fost adăugate dispoziții suplimentare care precizează condițiile care ar trebui îndeplinite înainte de adoptarea unui act delegat.

1.5 În ceea ce privește clasificarea sistemelor de IA ca prezentând un grad ridicat de risc, propunerea de compromis include acum un nivel orizontal suplimentar, pe lângă clasificarea gradelor ridicate de risc efectuată în **anexa III**, pentru a garanta că sistemele de IA care nu sunt susceptibile de a cauza încălcări grave ale drepturilor fundamentale sau alte riscuri semnificative nu sunt incluse. Mai precis, **articolul 6 alineatul (3)** conține noi dispoziții conform cărora, atunci când sistemele de IA sunt clasificate ca prezentând un grad ridicat de risc ar trebui, de asemenea, să fie luată în considerare semnificația rezultatului produs de sistemul de IA cu privire la acțiunea relevantă sau la o decizie care urmează să fie luată. Importanța rezultatului unui sistem de IA ar urma să fie evaluată ținând seama dacă acesta este sau nu pur accesoriu în raport cu acțiunea relevantă sau decizia care urmează să fie luată.

2. Cerințe pentru sistemele de IA cu grad ridicat de risc și responsabilitățile diferiților actori din lanțul valoric al IA

2.1 Multe dintre cerințele pentru sistemele de IA cu grad ridicat de risc, menționate în **titlul III capitolul 2** din propunere, au fost clarificate și ajustate astfel încât să fie mai fezabile din punct de vedere tehnic și mai puțin împovărătoare pentru părțile interesate, de exemplu în ceea ce privește calitatea datelor sau documentația tehnică care ar trebui elaborată de IMM-uri pentru a demonstra că sistemele lor de IA cu grad ridicat de risc respectă cerințele.

2.2 Având în vedere că sistemele de IA sunt dezvoltate și distribuite prin lanțuri valorice complexe, textul de compromis include modificări care clarifică alocarea responsabilităților și a rolurilor. De exemplu, la **articolele 13 și 14** au fost adăugate dispoziții suplimentare care permit o cooperare mai eficace între furnizori și utilizatori. Textul de compromis urmărește, de asemenea, să clarifice relația dintre responsabilitățile în temeiul Actului privind IA și responsabilitățile care există deja în temeiul altor acte legislative, cum ar fi legislația relevantă a Uniunii privind protecția datelor sau legislația sectorială, inclusiv în ceea ce privește sectorul serviciilor financiare. În plus, noul **articolul 23a** indică mai clar situațiile în care alți actori din lanțul valoric sunt obligați să își asume responsabilitățile unui furnizor.

3. **Sisteme de IA de uz general**

3.1 A fost adăugat un nou **titlu IA** pentru a ține seama de situațiile în care sistemele de IA pot fi utilizate în multe scopuri diferite (IA de uz general) și de posibilele circumstanțe în care tehnologia IA de uz general este integrată într-un alt sistem care poate deveni cu risc ridicat. La articolul **4b alineatul (1)**, textul de compromis precizează că anumite cerințe pentru sistemele de IA cu grad ridicat de risc ar urma să se aplice și sistemelor de IA de uz general. Cu toate acestea, în locul aplicării directe a acestor cerințe, un act de punere în aplicare ar urma să specifice modul în care acestea ar trebui aplicate în raport cu sistemele de IA de uz general, pe baza unei consultări și a unei evaluări detaliate a impactului și ținând seama de caracteristicile specifice ale acestor sisteme și ale lanțului valoric aferent, de fezabilitatea tehnică și de evoluțiile tehnologice și ale pieței. Recurgerea la un act de punere în aplicare va garanta faptul că statele membre vor fi implicate în mod corespunzător și că vor avea ultimul cuvânt asupra modului în care vor fi aplicate cerințele în acest context.

3.2 În plus, textul de compromis de la **articolul 4b alineatul (5)** include și posibilitatea de a adopta acte de punere în aplicare suplimentare care ar stabili modalitățile de cooperare dintre furnizorii de sisteme de IA de uz general și alți furnizori care intenționează să pună în funcțiune sau să introducă astfel de sisteme pe piața Uniunii ca sisteme de IA cu grad ridicat de risc, în special cu privire la furnizarea de informații.

(4) **Clarificarea domeniului de aplicare al propunerii de Act privind IA și a dispozițiilor referitoare la autoritățile de aplicare a legii**

4.1 La **articolul 2** s-a făcut o trimitere explicită la excluderea obiectivelor de securitate națională, de apărare și militare din domeniul de aplicare al Actului privind IA. În mod similar, s-a clarificat faptul că Actul privind IA nu ar trebui să se aplice sistemelor de IA și rezultatelor acestora utilizate exclusiv în scopul cercetării și dezvoltării, și nici obligațiilor persoanelor care utilizează IA în scopuri neprofesionale, acestea neintrând în domeniul de aplicare al Actului privind IA, cu excepția obligațiilor în materie de transparență.

4.2 Pentru a ține seama de particularitățile autorităților de aplicare a legii, au fost aduse mai multe modificări dispozițiilor privind utilizarea sistemelor de IA în scopul asigurării respectării legii. În special, unele dintre definițiile conexe de la **articolul 3**, cum ar fi „sistemul de identificare biometrică la distanță” și „sistemul de identificare biometrică la distanță în timp real”, au fost adaptate pentru a clarifica situațiile care ar intra în categoria interdicției aferente și a cazurilor de utilizare cu grad ridicat de risc, precum și situațiile care nu ar intra în această categorie. Propunerea de compromis conține, de asemenea, alte modificări care, sub rezerva unor garanții adecvate, sunt menite să asigure un nivel corespunzător de flexibilitate în utilizarea sistemelor de IA cu grad ridicat de risc de către autoritățile de aplicare a legii sau să reflecteze asupra necesității de a respecta confidențialitatea datelor operaționale sensibile în raport cu activitățile lor.

(5) **Evaluările conformității, cadrul de guvernanță, supravegherea pieței, asigurarea respectării legii și sancțiuni**

5.1 Pentru a simplifica cadrul de conformitate pentru Actul privind IA, textul de compromis conține o serie de clarificări și simplificări ale dispozițiilor privind procedurile de evaluare a conformității. Dispozițiile privind supravegherea pieței au fost, de asemenea, clarificate și simplificate pentru a deveni mai eficiente și mai ușor de pus în aplicare, ținând seama de necesitatea adoptării unei abordări proporționale în această privință. În plus, **articolul 41** fost revizuit în detaliu pentru a limita marja de apreciere a Comisiei în ceea ce privește adoptarea de acte de punere în aplicare de stabilire a unor specificații tehnice comune pentru cerințele aplicabile sistemelor de IA cu grad ridicat de risc și sistemelor de IA de uz general.

5.2 Textul de compromis modifică, de asemenea, în mod substanțial dispozițiile privind Comitetul pentru IA (denumit în continuare „comitetul”), cu scopul de a-i asigura o mai mare autonomie și de a-i consolida rolul în arhitectura de guvernanță a Actului privind inteligența artificială. În acest context, **articolele 56 și 58** au fost revizuite pentru a consolida rolul comitetului, astfel încât acesta să poată oferi sprijin statelor membre într-o mai mare măsură în punerea în aplicare și asigurarea respectării Actului privind IA. Mai precis, sarcinile comitetului au fost extinse și a fost precizată componența acestuia. Pentru a asigura implicarea părților interesate în ceea ce privește toate aspectele legate de punerea în aplicare a Actului privind IA, inclusiv pregătirea actelor de punere în aplicare și a actelor delegate, a fost adăugată o nouă cerință pentru comitet, acesta având obligația de a crea un subgrup permanent care să servească drept platformă pentru o gamă largă de părți interesate. Ar trebui, de asemenea, instituite alte două subgrupuri permanente pentru autoritățile de supraveghere a pieței și pentru autoritățile de notificare, pentru a consolida coerența guvernanței și asigurarea respectării Actului privind IA în întreaga Uniune.

5.3 Pentru a îmbunătăți în continuare cadrul de guvernanță, textul de compromis include noile **articole 68a și 68b**. **Articolul 68a** include o cerință adresată Comisiei de a desemna una sau mai multe instalații de testare ale Uniunii în domeniul inteligenței artificiale, care ar trebui să ofere consiliere tehnică sau științifică independentă la cererea comitetului sau a autorităților de supraveghere a pieței, în timp ce **articolul 68b** instituie obligația Comisiei de a crea un grup central de experți independenți care să sprijine activitățile de asigurare a respectării legii necesare în temeiul Actului privind IA. În cele din urmă, există, de asemenea, un nou **articol 58a** care prevede obligația Comisiei de a elabora orientări privind aplicarea Actului privind IA.

5.4 În ceea ce privește sancțiunile pentru încălcarea dispozițiilor Actului privind IA, la **articolul 71**, textul de compromis prevede plafoane mai proporționale pentru cuantumul amenzilor administrative pentru IMM-uri și întreprinderi nou-înființate. În plus, la **articolul 71 alineatul (6)** au fost adăugate alte patru criterii pentru a decide cu privire la cuantumul amenzilor administrative, pentru a garanta în continuare proporționalitatea lor globală.

(6) **Transparența și alte dispoziții în favoarea persoanelor afectate**

6.1 Propunerea de compromis include o serie de modificări care sporesc transparența în ceea ce privește utilizarea sistemelor de IA cu grad ridicat de risc. În special, **articolul 51** a fost actualizat pentru a indica faptul că anumiți utilizatori ai sistemului de IA cu grad ridicat de risc care sunt autorități, agenții sau organisme publice vor fi, de asemenea, obligați să se înregistreze în baza de date a UE pentru sistemele de IA cu grad ridicat de risc enumerate în anexa III. În plus, **articolul 52 alineatul (2a),** recent adăugat, pune accentul pe obligația utilizatorilor unui sistem de recunoaștere a emoțiilor de a informa persoanele fizice atunci când sunt expuse la un astfel de sistem.

6.2 Propunerea de compromis clarifică, de asemenea, la **articolul 63 alineatul (11),** recent adăugat, faptul că o persoană fizică sau juridică care are motive să considere că a avut loc o încălcare a dispozițiilor Actului privind IA poate depune o plângere la autoritatea relevantă de supraveghere a pieței și se poate aștepta ca o astfel de plângere să fie tratată în conformitate cu procedurile specifice ale autorității respective.

7. **Măsuri de sprijinire a inovării**

7.1 Cu scopul de a crea un cadru juridic mai favorabil inovării și pentru a promova învățarea bazată pe dovezi în materie de reglementare, dispozițiile privind măsurile de sprijinire a inovării de la **articolul 53** au fost modificate substanțial în textul de compromis. În special, s-a clarificat faptul că spațiile de testare în materie de reglementare a IA, care au rolul de a crea un mediu controlat pentru dezvoltarea, testarea și validarea sistemelor de IA inovatoare sub supravegherea directă și îndrumarea din partea autorităților naționale competente, ar trebui, de asemenea, să permită testarea sistemelor IA inovatoare în condiții reale. În plus, la **articolele 54a și 54b** au fost adăugate noi dispoziții care permit testarea nesupravegheată în condiții reale a sistemelor de IA, în condiții și cu garanții specifice. În ambele cazuri, textul de compromis clarifică modul în care aceste noi norme trebuie interpretate în raport cu alte acte legislative sectoriale existente privind spațiile de testare în materie de reglementare.

7.2 În cele din urmă, pentru a reduce sarcina administrativă pentru întreprinderile mai mici, la **articolul 55** textul de compromis include o listă de acțiuni care trebuie întreprinse de Comisie pentru a sprijini astfel de operatori, iar la **articolul 55a** prevede unele derogări limitate și clar specificate.

V. CONCLUZIE

1. În lumina celor de mai sus, se solicită Consiliului:
   - să examineze textul de compromis, astfel cum figurează în anexa la prezenta notă;
   - să confirme o abordare generală cu privire la propunerea de regulament de stabilire a unor norme armonizate privind inteligența artificială (Actul privind inteligența artificială) în cadrul reuniunii Consiliului TTE (Telecomunicații) din 6 decembrie 2022.

_____

ANEXĂ

Propunere de

REGULAMENT AL PARLAMENTULUI EUROPEAN ȘI AL CONSILIULUI

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

(Text cu relevanță pentru SEE)

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[1],

având în vedere avizul Comitetului Regiunilor[2],

având în vedere avizul Băncii Centrale Europene[3],

hotărând în conformitate cu procedura legislativă ordinară,

întrucât:

[1] JO C […], […], p. […].
[2] JO C […], […], p. […].
[3] Trimitere la avizul BCE.

(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, importă 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 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 și prin valorificarea activității Grupului de experți la nivel înalt privind inteligența artificială, astfel cum este reflectată în Orientările în materie de etică pentru inteligența artificială de încredere în UE, 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[4], și asigură protecția principiilor etice, astfel cum a solicitat în mod expres Parlamentul European[5].

---

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

5 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).

(5a) Normele armonizate privind introducerea pe piață, punerea în funcțiune și utilizarea sistemelor de IA prevăzute în prezentul regulament ar trebui să se aplice în toate sectoarele și, în conformitate cu abordarea bazată pe noul cadru legislativ, nu ar trebui să aducă atingere dreptului existent al Uniunii, în special în ceea ce privește protecția datelor, protecția consumatorilor, drepturile fundamentale, ocuparea forței de muncă și siguranța produselor, cu care prezentul regulament este complementar. În consecință, toate drepturile și căile de atac prevăzute de dreptul Uniunii pentru consumatori și alte persoane care ar putea fi afectate negativ de sistemele de IA, inclusiv în ceea ce privește despăgubirea pentru eventualele prejudicii în temeiul Directivei 85/374/CEE a Consiliului din 25 iulie 1985 de apropiere a actelor cu putere de lege și a actelor administrative ale statelor membre cu privire la răspunderea pentru produsele cu defect, rămân neafectate și pe deplin aplicabile. În plus, prezentul regulament urmărește să consolideze eficacitatea acestor drepturi și căi de atac existente prin stabilirea unor cerințe și obligații specifice, inclusiv în ceea ce privește transparența, documentația tehnică și păstrarea evidențelor sistemelor de IA. În plus, obligațiile impuse diferiților operatori implicați în lanțul valoric al IA în temeiul prezentului regulament ar trebui să se aplice fără a aduce atingere dreptului intern, în conformitate cu dreptul Uniunii, având ca efect limitarea utilizării anumitor sisteme de IA în cazul în care astfel de acte legislative nu intră în domeniul de aplicare al prezentului regulament sau urmăresc alte obiective legitime de interes public decât cele urmărite de prezentul regulament. De exemplu, dreptul intern al muncii și legislația privind protecția minorilor (adică a persoanelor cu vârsta sub 18 ani), ținând seama de Comentariul general nr. 25 (2021) al Organizației Națiunilor Unite privind drepturile copiilor, în măsura în care nu sunt specifice sistemelor de IA și urmăresc alte obiective legale de interes public, nu ar trebui să fie afectate de prezentul regulament.

(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 inteligenței artificiale, cum ar fi capacitățile sale de învățare, de raționament sau de modelare, care o diferențiază de sistemele software și de abordările de programare mai simple. În special, în sensul prezentului regulament, sistemele de IA ar trebui să aibă capacitatea, pe baza datelor și a datelor de intrare furnizate automat și/sau de factorul uman, de a deduce o modalitate prin care să atingă o serie de obiective finale care le sunt atribuite de oameni, utilizând abordări bazate pe învățarea automată și/sau pe logică și pe cunoaștere, și de a produce rezultate de tipul conținutului pentru sisteme de IA generative (de exemplu, de tip text, video sau imagine), previziunilor, recomandărilor sau deciziilor, influențând mediul cu care interacționează sistemul, fie în dimensiunea sa fizică, fie în cea digitală. Un sistem care utilizează norme definite exclusiv de persoane fizice pentru a executa în mod automat operațiuni nu ar trebui să fie considerat un sistem de IA. 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). Conceptul de autonomie a unui sistem de IA se referă la măsura în care un astfel de sistem funcționează fără implicare umană.

(6a) Abordările bazate pe învățarea automată se axează pe dezvoltarea unor sisteme capabile să învețe și să facă deducții pe baza datelor pentru a rezolva o problemă dintr-o aplicație fără a fi programate în mod explicit cu un set de instrucțiuni pas cu pas de la datele de intrare până la rezultate. Învățarea se referă la procesul de calcul de optimizare, pe baza unor date, a parametrilor unui model, care este o construcție matematică care generează un rezultat pornind de la date de intrare. Gama de probleme abordate de învățarea automată implică, de regulă, sarcini pentru care alte abordări nu funcționează, fie pentru că nu există o formalizare adecvată a problemei, fie pentru că problema nu poate fi soluționată prin abordări care nu sunt bazate pe învățare. Abordările bazate pe învățarea automată includ, de exemplu, învățarea supravegheată, nesupravegheată și prin întărire, utilizând o varietate de metode, inclusiv învățarea profundă cu rețele neuronale, tehnicile statistice pentru învățare și deducție (inclusiv, de exemplu, regresia logistică, estimarea bayeziană) și metode de căutare și optimizare.

(6b) Abordările bazate pe logică și pe cunoaștere se axează pe dezvoltarea de sisteme cu capacități de raționament logic pe baza cunoștințelor, pentru a rezolva o problemă dintr-o aplicație. Astfel de sisteme implică, de regulă, o bază de cunoștințe și un motor de deducție care generează rezultate efectuând raționamente asupra bazei de cunoștințe. Baza de cunoștințe, care este de obicei creată de experți umani, reprezintă entitățile și relațiile logice relevante pentru problema dintr-o aplicație prin formalizări bazate pe reguli, ontologii sau grafice ale cunoștințelor. Motorul de deducție acționează asupra bazei de cunoștințe și extrage informații noi prin operațiuni precum sortarea, căutarea, corelarea sau înlănțuirea. Abordările bazate pe logică și pe cunoaștere, includ, de exemplu, reprezentarea cunoștințelor, programarea inductivă (logică), baze de cunoștințe, motoare inductive și deductive, sisteme de raționament (simbolic), sisteme expert și metode de optimizare.

(6c) Pentru a asigura condiții uniforme de punere în aplicare a prezentului regulament în ceea ce privește abordările bazate pe învățarea automată și abordările bazate pe logică și pe cunoaștere și pentru a ține seama de evoluțiile pieței și de evoluțiile tehnologice, Comisiei ar trebui să îi fie conferite competențe de executare.

(6d) Noțiunea de „utilizator” menționată în prezentul regulament ar trebui interpretată ca fiind orice persoană fizică sau juridică, inclusiv o autoritate publică, o agenție sau un alt organism, care utilizează un sistem de IA, sub a cărui autoritate este utilizat sistemul. În funcție de tipul de sistem de IA, utilizarea sistemului poate afecta alte persoane decât utilizatorul.

(7) Noțiunea de date biometrice utilizată în prezentul regulament ar trebui interpretată într-un mod consecvent 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[6], la articolul 3 alineatul (18) din Regulamentul (UE) 2018/1725 al Parlamentului European și al Consiliului[7] și la articolul 3 alineatul (13) din Directiva (UE) 2016/680 a Parlamentului European și a Consiliului[8] și ar trebui interpretată în concordanță cu aceasta.

[6] 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).

[7] 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).

[8] 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).

(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, de regulă la distanță, fără implicarea activă a acestora, prin compararea datelor biometrice ale unei persoane cu datele biometrice conținute într-un depozit de date de referință, indiferent de tehnologia, procesele sau tipurile specifice de date biometrice utilizate. Astfel de sisteme de identificare biometrică la distanță sunt utilizate, de regulă, pentru a percepe (scana) mai multe persoane sau comportamentul acestora simultan, pentru a facilita în mod semnificativ identificarea unui număr de persoane fără implicarea lor activă. O astfel de definiție exclude sistemele de verificare/autentificare al căror unic scop ar fi să confirme că o anumită persoană fizică este persoana care susține că este, precum și sistemele utilizate pentru a confirma identitatea unei persoane fizice cu unicul scop de a avea acces la un serviciu, la un dispozitiv sau la o incintă. Această excludere este justificată de faptul că, cel mai probabil, astfel de sisteme au un impact minor asupra drepturilor fundamentale ale persoanelor fizice în comparație cu sistemele de identificare biometrică la distanță care ar putea fi utilizate pentru prelucrarea datelor biometrice ale unui număr mare de persoane. 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.

(9) În sensul prezentului regulament, noțiunea de spațiu accesibil publicului ar trebui înțeleasă ca referindu-se la orice loc fizic accesibil unui număr nedeterminat de persoane fizice, indiferent dacă locul în cauză este proprietate privată sau publică și indiferent de activitatea pentru care poate fi utilizat locul, de exemplu, comerț (precum magazine, restaurante, cafenele), servicii (precum bănci, activități profesionale, structuri de primire turistică), sport (precum piscine, săli de sport, stadioane), transporturi (precum stații de autobuz, metrou și gări, aeroporturi, mijloace de transport), divertisment (precum cinematografe, teatre, muzee, săli de concerte și conferințe) de agrement sau de alt tip (precum drumuri și piețe publice, parcuri, păduri, terenuri de joacă). Un loc ar trebui clasificat ca fiind accesibil publicului și în cazul în care, indiferent de capacitatea potențială sau de restricțiile de securitate, accesul este supus anumitor condiții prestabilite, care pot fi îndeplinite de un număr nedeterminat de persoane, cum ar fi achiziționarea unui bilet sau a unui titlu de transport, înregistrarea prealabilă sau o anumită vârstă. În schimb, un loc nu ar trebui să fie considerat accesibil publicului dacă accesul este limitat la anumite persoane fizice definite ca atare fie prin dreptul Uniunii, fie prin cel intern, în legătură directă cu siguranța sau securitatea publică sau prin manifestarea clară de voință a persoanei care deține autoritatea necesară asupra locului. Simpla posibilitate de acces (de exemplu, o ușă care nu este blocată, o poartă deschisă a unui gard) nu implică faptul că locul este accesibil publicului în prezența unor indicații sau circumstanțe care sugerează contrariul (de exemplu, semne care interzic sau restricționează accesul). Sediile întreprinderilor și ale fabricilor, precum și birourile și locurile de muncă care sunt destinate a fi accesate numai de către angajații și prestatorii de servicii competenți sunt locuri care nu sunt accesibile publicului. Spațiile accesibile publicului nu ar trebui să includă închisori sau zone de control la frontieră. Alte zone pot fi formate atât din zone care nu sunt accesibile publicului, cât și din zone accesibile publicului, cum ar fi holul unei clădiri rezidențiale private care trebuie parcurs pentru a avea acces la un cabinet medical, sau un aeroport. Spațiile online nu fac nici ele obiectul, deoarece nu sunt spații fizice. 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. 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 viitoare 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. Autoritățile statelor membre destinatare și instituțiile, oficiile, organismele Uniunii și organismele care utilizează astfel de rezultate în Uniune rămân responsabile pentru asigurarea faptului că utilizarea lor respectă dreptul Uniunii. Atunci când acordurile internaționale respective sunt revizuite sau altele noi sunt încheiate în viitor, părțile contractante ar trebui să depună toate eforturile pentru a alinia acordurile respective la cerințele prezentului regulament.

(12) Prezentul regulament ar trebui să se aplice, de asemenea, instituțiilor, oficiilor, organismelor și agențiilor Uniunii atunci când acestea acționează în calitate de furnizor sau utilizator al unui sistem de IA.

(-12a) În cazul și în măsura în care sisteme de IA sunt introduse pe piață, sunt puse în funcțiune sau utilizate cu sau fără modificarea lor în scopuri militare, de apărare sau de securitate națională, sistemele respective ar trebui excluse din domeniul de aplicare al prezentului regulament, indiferent de tipul de entitate care desfășoară activitățile respective, de exemplu dacă este o entitate publică sau privată. În ceea ce privește scopurile militare și de apărare, o astfel de excludere este justificată atât de articolul 4 alineatul (2) din TUE, cât și de particularitățile politicii de apărare comune a statelor membre și a Uniunii care intră sub incidența titlului V capitolul 2 din Tratatul privind Uniunea Europeană (TUE), care fac obiectul dreptului internațional public, care este, prin urmare, cadrul juridic mai adecvat pentru reglementarea sistemelor de IA în contextul utilizării forței letale și al altor sisteme de IA în contextul activităților militare și de apărare. În ceea ce privește obiectivele de securitate națională, excluderea este justificată atât de faptul că securitatea națională rămâne responsabilitatea exclusivă a statelor membre în conformitate cu articolul 4 alineatul (2) TUE, cât și de natura specifică și de nevoile operaționale ale activităților de securitate națională și de normele naționale specifice aplicabile activităților respective. Însă, în cazul în care un sistem de IA dezvoltat, introdus pe piață, pus în funcțiune sau utilizat în scopuri militare, de apărare sau de securitate națională este utilizat, temporar sau permanent, în afara acestora, în alte scopuri (de exemplu, în scopuri civile sau umanitare, de asigurare a respectării legii sau de securitate publică), un astfel de sistem ar intra în domeniul de aplicare al prezentului regulament. În acest caz, entitatea care utilizează sistemul în alte scopuri decât cele militare, de apărare sau de securitate națională ar trebui să asigure conformitatea sistemului cu prezentul regulament, cu excepția cazului în care sistemul respectă deja prezentul regulament. Sistemele de IA introduse pe piață sau puse în funcțiune pentru un scop exclus din domeniul de aplicare al prezentului regulament (și anume, militar, de apărare sau de securitate națională) și pentru unul sau mai multe scopuri care nu sunt excluse (de exemplu, scopurile civile, asigurarea respectării legii etc.) intră în domeniul de aplicare al prezentului regulament, iar furnizorii acestor sisteme ar trebui să asigure conformitatea cu prezentul regulament. În aceste cazuri, faptul că un sistem de IA poate intra în domeniul de aplicare al prezentului regulament nu ar trebui să afecteze posibilitatea ca entitățile care desfășoară activități de securitate națională, de apărare și militare, indiferent de tipul de entitate care desfășoară activitățile respective, să utilizeze sisteme de IA în scopuri de securitate națională, militare și de apărare, a căror utilizare este exclusă din domeniul de aplicare al prezentului regulament. Un sistem de IA introdus pe piață în scopuri civile sau de asigurare a respectării legii și care este utilizat cu sau fără modificări în scopuri militare, de apărare sau de securitate națională nu ar trebui să intre în domeniul de aplicare al prezentului regulament, indiferent de tipul de entitate care desfășoară activitățile respective.

(12a) 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].

(12b) Prezentul regulament nu ar trebui să submineze activitatea de cercetare și dezvoltare și ar trebui să respecte libertatea științei. Prin urmare, este necesar să se excludă din domeniul său de aplicare sistemele de IA dezvoltate și puse în funcțiune în scopul cercetării și dezvoltării științifice și să se garanteze faptul că regulamentul nu afectează într-un alt mod activitatea de cercetare și dezvoltare științifică privind sistemele de IA. În ceea ce privește activitatea de cercetare orientată către produse desfășurată de furnizori, dispozițiile prezentului regulament nu ar trebui să se aplice. Acest lucru nu aduce atingere obligației de a respecta prezentul regulament atunci când un sistem de IA aflat sub incidența prezentului regulament este introdus pe piață sau pus în funcțiune ca urmare a unei astfel de activități de cercetare și dezvoltare, și nici aplicării dispozițiilor privind spațiile de testare în materie de reglementare și testarea în condiții reale. În plus, fără a aduce atingere celor de mai sus cu privire la sistemele de IA dezvoltate și puse în funcțiune în scopul unic al cercetării și dezvoltării științifice, orice alt sistem de IA care poate fi utilizat pentru desfășurarea oricărei activități de cercetare și dezvoltare ar trebui să facă în continuare obiectul dispozițiilor prezentului regulament. În orice situație, orice activitate de cercetare și dezvoltare ar trebui să se desfășoare în conformitate cu standardele etice și profesionale recunoscute pentru cercetarea științifică.

(12c) Având în vedere natura și complexitatea lanțului valoric pentru sistemele de IA, este esențial să se clarifice rolul actorilor care pot contribui la dezvoltarea sistemelor de IA, în special a sistemelor de IA cu grad ridicat de risc. În special, este necesar să se clarifice faptul că sistemele de IA de uz general sunt sisteme de IA care sunt concepute de furnizor astfel încât să îndeplinească funcții general aplicabile, cum ar fi recunoașterea de imagini/vocală, și într-o multitudine de contexte. Ele pot fi utilizate ca sisteme de IA cu grad ridicat de risc autonome sau pot fi componente ale altor sisteme de IA cu grad ridicat de risc. Prin urmare, având în vedere natura lor specială și pentru a asigura o partajare echitabilă a responsabilităților de-a lungul lanțului valoric al IA, astfel de sisteme ar trebui să facă obiectul unor cerințe și obligații proporționale și mai clar precizate în temeiul prezentului regulament, asigurându-se, în același timp, un nivel ridicat de protecție a drepturilor fundamentale, a sănătății și a siguranței. În plus, furnizorii de sisteme de IA de uz general, indiferent dacă acestea pot fi utilizate în mod autonom drept sisteme de IA cu grad ridicat de risc de către alți furnizori sau drept componente ale unor sisteme de IA cu grad ridicat de risc, ar trebui să coopereze, după caz, cu furnizorii respectivelor sisteme de IA cu grad ridicat de risc pentru a permite respectarea de către acestea a obligațiilor relevante în temeiul prezentului regulament, precum și cu autoritățile competente instituite în temeiul prezentului regulament. Pentru a ține seama de caracteristicile specifice ale sistemelor de IA de uz general și de evoluțiile rapide ale pieței și tehnologiei din domeniu, ar trebui să i se confere Comisiei competențe de executare pentru a specifica și a adapta aplicarea cerințelor stabilite în temeiul prezentului regulament la sistemele de IA de uz general, precum și pentru a preciza informațiile care trebuie să fie partajate de furnizorii de sisteme de IA de uz general pentru a le permite furnizorilor respectivului sistem de IA cu grad ridicat de risc să își respecte obligațiile în temeiul prezentului regulament.

(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) Tehnicile de manipulare bazate pe IA pot fi utilizate pentru a convinge anumite persoane să manifeste comportamente nedorite sau pentru a le înșela, sugerându-li-se într-un mod subtil decizii într-un mod care le subminează și le afectează autonomia, procesul decizional și libera alegere. Introducerea pe piață, punerea în funcțiune sau utilizarea anumitor sisteme de IA care denaturează în mod material comportamentul uman, susceptibile de a cauza prejudicii fizice sau psihologice, sunt deosebit de periculoase și, prin urmare, ar trebui interzise. Astfel de sisteme de IA implementează componente subliminale, cum ar fi stimuli audio, sub formă de imagini sau video, pe care o persoană nu le poate percepe, întrucât stimulii respectivi depășesc percepția umană, sau alte tehnici subliminale care subminează sau afectează autonomia, procesul decizional sau libera alegere ale unei persoane în moduri de care persoana respectivă nu este conștientă, sau chiar dacă este conștientă, nu le poate controla sau nu li se poate opune, de exemplu în cazul interfețelor mașină-creier sau al realității virtuale. În plus, sistemele de IA pot exploata și în alte moduri vulnerabilitățile unui anumit grup de persoane din cauza vârstei sau a handicapului acestora în sensul Directivei (UE) 2019/882 sau din cauza unei situații sociale sau economice specifice care este susceptibilă să sporească vulnerabilitatea la exploatare a persoanelor respective, cum ar fi persoanele care trăiesc în sărăcie extremă, minoritățile etnice sau religioase. Astfel de sisteme de IA pot fi introduse pe piață, puse în funcțiune sau utilizate având drept obiectiv sau drept efect denaturarea materială a comportamentului unei persoane, într-un mod care cauzează sau este susceptibil în mod rezonabil să cauzeze prejudicii fizice sau psihologice persoanei respective, sau unei alte persoane ori unor grupuri de persoane, inclusiv prejudicii care se pot acumula în timp. Intenția de a denatura comportamentul nu poate fi prezumată în cazul în care denaturarea rezultă din factori asupra cărora furnizorul sau utilizatorul nu dețin controlul, adică factori care nu pot fi prevăzuți și atenuați în mod rezonabil de către furnizorul sau utilizatorul sistemului de IA. În orice caz, nu este necesar ca furnizorul sau utilizatorul să aibă intenția de a cauza prejudiciul fizic sau psihologic, atât timp cât un astfel de prejudiciu rezultă din practicile manipulatoare sau abuzive bazate pe IA. Interdicțiile privind astfel de practici în domeniul IA sunt complementare dispozițiilor cuprinse în Directiva 2005/29/CE, în special faptul că practicile comerciale neloiale care conduc la prejudicii economice sau financiare pentru consumatori sunt interzise în toate circumstanțele, indiferent dacă sunt instituite prin intermediul sistemelor de IA sau în alt mod. Interdicțiile privind practicile de manipulare și exploatare prevăzute în prezentul regulament nu ar trebui să afecteze practicile legale în contextul tratamentului medical, cum ar fi tratamentul psihologic al unei boli mintale sau reabilitarea fizică, atunci când practicile respective se desfășoară în conformitate cu standardele și legislația medicală aplicabile. În plus, practicile comerciale comune și legitime care sunt în conformitate cu legislația aplicabilă nu ar trebui considerate, în sine, ca reprezentând practici dăunătoare de manipulare a IA.

(17) Sistemele de IA care oferă o evaluare a comportamentului social al persoanelor fizice de către autoritățile publice sau de către actori privați 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 persoanele 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, sistemele de IA care implică astfel de practici inacceptabile de evaluare ar trebui interzise. Această interdicție nu ar trebui să afecteze practicile legale de evaluare a persoanelor fizice efectuate într-unul sau mai multe scopuri specifice, în conformitate cu legislația.

(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 situațiilor 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[9], 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. În plus, prezentul regulament ar trebui să mențină capacitatea autorităților responsabile în materie de aplicare a legii, de control la frontiere, de imigrație sau de azil de a efectua controale de identitate în prezența persoanei vizate, în conformitate cu condițiile prevăzute în dreptul Uniunii și în cel intern pentru astfel de controale. În special, autoritățile responsabile în materie de aplicare a legii, de control la frontiere, de imigrație sau de azil. ar trebui să poată utiliza sistemele de informații, în conformitate cu dreptul Uniunii sau cu cel intern, pentru a identifica o persoană care, în cursul unui control de identitate, fie refuză să fie identificată, fie este incapabilă să își declare sau să își dovedească identitatea, fără a fi obligate prin prezentul regulament să obțină o autorizație prealabilă. Ar putea fi, de exemplu, o persoană implicată într-o infracțiune, care nu dorește sau nu poate, din cauza unui accident sau a unei afecțiuni medicale, să își divulge identitatea autorităților de aplicare a legii.

[9] 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).

(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 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 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 situațiile 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 utilizarea sistemului în vederea identificării uneia sau mai multor persoane. Ar trebui să fie permise excepții față de această regulă în situații 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 reglementată de prezentul regulament, ar trebui să respecte în continuare toate cerințele care decurg din articolul 10 din Directiva (UE) 2016/680. În alte scopuri decât asigurarea respectării legii, articolul 9 alineatul (1) din Regulamentul (UE) 2016/679 și articolul 10 alineatul (1) din Regulamentul (UE) 2018/1725 interzic prelucrarea datelor biometrice în scopul identificării unice a unei persoane fizice, cu excepția cazului în care se aplică una dintre situațiile prevăzute la al doilea paragraf al celor două articole.

(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), (3) și (4) 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), (3) și (4) 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[10], al Regulamentului (UE) nr. 167/2013 al Parlamentului European și al Consiliului[11], al Regulamentului (UE) nr. 168/2013 al Parlamentului European și al Consiliului[12], al Directivei 2014/90/UE a Parlamentului European și a Consiliului[13], al Directivei (UE) 2016/797 a Parlamentului European și a Consiliului[14], al Regulamentului (UE) 2018/858 al Parlamentului European și al Consiliului[15], al Regulamentului (UE) 2018/1139 al Parlamentului European și al Consiliului[16] și al Regulamentului (UE) 2019/2144[17] al Parlamentului European și al Consiliului, 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.

---

10 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);

11 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);

12 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);

13 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);

14 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);

15 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);

16 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).

17 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);

(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[18] și al Regulamentului (UE) 2017/746 al Parlamentului European și al Consiliului[19], care prevăd o evaluare a conformității de către o parte terță pentru produsele cu risc mediu și cu risc ridicat.

[18] 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).

[19] 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).

(32) În ceea ce privește sistemele de IA cu grad ridicat de risc altele 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. Este, de asemenea, important să se clarifice faptul că, în cadrul scenariilor cu grad ridicat de risc menționate în anexa III, pot exista sisteme care nu conduc la un risc semnificativ pentru interesele juridice protejate în cadrul scenariilor respective, ținând seama de rezultatele generate de sistemul de IA. Prin urmare, numai atunci când un astfel de rezultat are un grad ridicat de importanță (și anume, nu este pur accesoriu) în ceea ce privește acțiunea sau decizia relevantă, astfel încât să genereze un risc semnificativ pentru interesele juridice protejate, sistemul de IA care generează un astfel de rezultat ar trebui să fie considerat ca prezentând un grad ridicat de risc. De exemplu, atunci când informațiile furnizate factorului uman de sistemele de IA constau în crearea de profiluri ale persoanelor fizice în sensul articolului 4 alineatul (4) din Regulamentul (UE) 2016/679, al articolului 3 alineatul (4) din Directiva (UE) 2016/680 și al articolului 3 alineatul (5) din Regulamentul (UE) 2018/1725, astfel de informații nu ar trebui, de regulă, să fie considerate ca fiind de natură accesorie în contextul sistemelor de IA cu grad ridicat de risc, menționate în anexa III. Cu toate acestea, în cazul în care rezultatul sistemului de IA are doar o relevanță neglijabilă sau minoră pentru acțiunea sau decizia umană, acesta poate fi considerat pur accesoriu, inclusiv, de exemplu, în cazul sistemelor de IA utilizate pentru traducere în scopuri informative sau pentru gestionarea documentelor.

(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, rasa, 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 infrastructurii digitale critice, astfel cum este menționată la anexa I punctul 8 din Directiva privind reziliența entităților critice, a 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. Componentele de siguranță ale infrastructurii critice, inclusiv infrastructura digitală critică, sunt sisteme utilizate pentru a proteja în mod direct integritatea fizică a infrastructurii critice sau sănătatea și siguranța persoanelor și a bunurilor, dar care nu sunt necesare pentru funcționarea sistemului. Defectarea sau funcționarea defectuoasă a unor astfel de componente ar putea conduce în mod direct la riscuri pentru integritatea fizică a infrastructurii critice și, prin urmare, la riscuri pentru sănătatea și siguranța persoanelor și a bunurilor. Componentele destinate a fi utilizate exclusiv în scopuri de securitate cibernetică nu ar trebui să se califice drept componente de siguranță. Printre exemplele de componente de siguranță ale unei astfel de infrastructuri critice se numără sisteme de monitorizare a presiunii apei sau sisteme de control al alarmei de incendiu în centrele de cloud computing.

(35) Sistemele de IA utilizate în educație sau în formarea profesională, în special pentru a stabili accesul, admisia sau pentru a repartiza persoane fizice la instituțiile de învățământ și formare profesională sau în programele de formare profesională la toate nivelurile, sau pentru a evalua rezultatele învățării 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 pe baza comportamentului individual sau a trăsăturilor sau caracteristicilor personale, 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 microîntreprinderi sau de către întreprinderi mici, astfel cum sunt descrise în anexa la recomandarea 2003/361/CE a Comisiei, pentru uzul propriu. Persoanele fizice care solicită sau primesc prestații și servicii esențiale 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, inclusiv în cazul în care beneficiarii au dreptul legitim la astfel de beneficii sau servicii, sistemele respective 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. Sistemele de IA sunt, de asemenea, utilizate din ce în ce mai mult pentru evaluarea riscurilor în ceea ce privește persoanele fizice și stabilirea prețurilor în cazul asigurărilor de viață și de sănătate care, dacă nu sunt concepute, dezvoltate și utilizate în mod corect, pot conduce la consecințe grave pentru viața și sănătatea oamenilor, inclusiv la excluziune financiară și discriminare. Pentru a asigura o abordare coerentă în sectorul serviciilor financiare, excepția sus-menționată pentru microîntreprinderi sau întreprinderi mici pentru uz propriu ar trebui să se aplice în măsura în care întreprinderile respective furnizează și pun în funcțiune ele însele un sistem de IA în scopul vânzării propriilor produse de asigurare.

(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 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. Sistemele de IA destinate în mod special utilizării în proceduri administrative de către autoritățile fiscale și vamale, precum și de către unitățile de informații financiare care efectuează sarcini administrative prin care analizează informații în temeiul legislației Uniunii de combatere a spălării banilor, 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, 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[20], de Regulamentul (CE) nr. 810/2009 al Parlamentului European și al Consiliului[21] și de alte acte legislative relevante.

[20] 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).

[21] 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).

(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 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 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 și sarcinile administrative.

(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 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, cu excepția cazului în care se specifică altfel în cuprinsul prezentului regulament.

(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, 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. În special, sistemul de gestionare a riscurilor ar trebui să constea într-un proces iterativ continuu desfășurat și rulat pe parcursul întregului ciclu de viață al unui sistem de IA cu grad ridicat de risc. Acest proces ar trebui să garanteze faptul că furnizorul identifică și analizează riscurile la adresa sănătății, siguranței și drepturilor fundamentale ale persoanelor care pot fi afectate de sistem având în vedere scopul preconizat al acestuia, inclusiv posibilele riscuri care decurg din interacțiunea dintre sistemul de IA și mediul în care funcționează, și, în consecință, adoptă măsuri adecvate de gestionare a riscurilor având în vedere stadiul actual al tehnologiei.

(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 să aibă 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. Aceste seturi de date ar trebui, de asemenea, să nu conțină erori și să fie cât mai complete posibil având în vedere scopul preconizat al sistemului de IA, ținând seama, în mod proporțional, de fezabilitatea tehnică și de stadiul actual al tehnologiei, de disponibilitatea datelor și de punerea în aplicare a unor măsuri adecvate de gestionare a riscurilor, astfel încât posibilele deficiențe ale seturilor de date să fie abordate corespunzător. Cerința ca seturile de date să fie complete și să nu fie afectate de erori nu ar trebui să afecteze utilizarea tehnicilor de conservare a vieții private în contextul dezvoltării și testării sistemelor de IA. 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 lor 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 în sensul articolului 9 alineatul (2) litera (g) din Regulamentul (UE) 2016/679 și al articolului 10 alineatul (2) litera (g) din Regulamentul (UE) 2018/1725, pentru a asigura monitorizarea, detectarea și corectarea părtinirii în ceea ce privește sistemele de IA cu grad ridicat de risc.

(44a) Atunci când se aplică principiile menționate la articolul 5 alineatul (1) litera (c) din Regulamentul 2016/679 și la articolul 4 alineatul (1) litera (c) din Regulamentul 2018/1725, în special principiul reducerii la minimum a datelor, în ceea ce privește seturile de date de antrenament, de validare și de testare în temeiul prezentului regulament, ar trebui să se acorde atenția cuvenită întregului ciclu de viață al sistemului de IA.

(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. În plus, furnizorii sau utilizatorii ar trebui să păstreze înregistrările generate automat de sistemul de IA cu grad ridicat de risc, inclusiv, de exemplu, datele de ieșire, data și ora de începere etc., în măsura în care un astfel de sistem și înregistrările aferente se află sub controlul lor, pentru o perioadă adecvată care să le permită să își îndeplinească obligațiile.

(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 persoanelor care pot fi afectate de sistem având în vedere obiectivul preconizat al acestuia, după caz. Pentru a putea fi înțelese mai ușor de către utilizatori, instrucțiunile de utilizare ar trebui să conțină exemple ilustrative, 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. Având în vedere consecințele semnificative pentru persoane în cazul unor concordanțe incorecte ale anumitor sisteme de identificare biometrică, este oportun să se prevadă o cerință de supraveghere umană mai strictă pentru sistemele respective, astfel încât utilizatorul să nu poată lua nicio măsură sau decizie pe baza identificării rezultate din sistem, decât dacă acest lucru a fost verificat și confirmat separat de cel puțin două persoane fizice. Aceste persoane ar putea proveni de la una sau mai multe entități și ar putea include persoana care operează sau utilizează sistemul. Această cerință nu ar trebui să reprezinte o povară inutilă sau să genereze întârzieri inutile și ar putea fi suficient ca verificările separate efectuate de diferite persoane să fie înregistrate automat în jurnalele generate de sistem.

(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 reziliente în raport cu comportamentul dăunător sau nedorit în alt mod, care poate rezulta din limitările din cadrul sistemelor sau al mediului în care funcționează sistemele (de exemplu, erori, defecțiuni, inconsecvențe, situații neprevăzute). Prin urmare, sistemele de IA cu grad ridicat de risc ar trebui să fie proiectate și dezvoltate utilizând soluții tehnice adecvate, pentru a preveni sau a reduce la minimum comportamentul dăunător sau nedorit în alt mod, printre soluțiile respective numărându-se, de exemplu, mecanismele care permit sistemului să își întrerupă funcționarea în condiții de siguranță (planuri de autoprotecție) în prezența anumitor anomalii sau atunci când funcționarea are loc în afara anumitor limite prestabilite. 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 [22]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[23] privind un cadru comun pentru comercializarea produselor și cu Regulamentul (UE) 2019/1020 al Parlamentului European și al Consiliului[24] privind supravegherea pieței și conformitatea produselor („Noul cadru legislativ pentru comercializarea produselor”).

(52a) În conformitate cu principiile noului cadru legislativ, ar trebui stabilite obligații specifice pentru operatorii relevanți din cadrul lanțului valoric al IA, pentru a asigura securitatea juridică și a facilita respectarea prezentului regulament. În anumite situații, operatorii respectivi ar putea acționa în mai multe roluri în același timp și, prin urmare, ar trebui să îndeplinească în mod cumulativ toate obligațiile relevante asociate rolurilor respective. De exemplu, un operator ar putea acționa în același timp ca distribuitor și importator.

(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.

---

22 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).

23 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).

24 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.

(54a) Pentru a asigura securitatea juridică, este necesar să se clarifice faptul că, în anumite condiții specifice, orice persoană fizică sau juridică ar trebui să fie considerată drept furnizoare a unui nou sistem de IA cu grad ridicat de risc și, prin urmare, să își asume toate obligațiile relevante. De exemplu, acest lucru ar fi valabil dacă persoana respectivă își pune numele sau marca comercială pe un sistem de IA cu grad ridicat de risc deja introdus pe piață sau pus în funcțiune, sau dacă persoana respectivă modifică scopul preconizat al unui sistem de IA care nu prezintă un grad ridicat de risc și care este deja introdus pe piață sau pus în funcțiune, astfel încât sistemul modificat să devină un sistem de IA cu grad ridicat de risc. Aceste dispoziții ar trebui să se aplice fără a aduce atingere dispozițiilor mai specifice stabilite în anumite acte legislative sectoriale din noul cadru legislativ, cu care prezentul regulament ar trebui să se aplice prin coroborare. De exemplu, articolul 16 alineatul (2) din Regulamentul (UE) 745/2017, care stabilește că anumite modificări nu ar trebui să fie considerate modificări ale unui dispozitiv care ar putea afecta conformitatea acestuia cu cerințele aplicabile, ar trebui să se aplice în continuare sistemelor de IA cu grad ridicat de risc care sunt dispozitive medicale în sensul regulamentului respectiv.

(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, fabricantul produsului, 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.

(56a) Pentru furnizorii care nu sunt stabiliți în Uniune, reprezentantul autorizat joacă un rol central în asigurarea conformității sistemelor de IA cu grad ridicat de risc introduse pe piață sau puse în funcțiune în Uniune de producătorii respectivi și în îndeplinirea rolului de persoană de contact stabilită în Uniune al acestora. Având în vedere acest rol esențial și pentru a se asigura asumarea responsabilității în scopul asigurării respectării prezentului regulament, este oportun ca reprezentantul autorizat să răspundă în solidar cu furnizorul pentru sistemele de IA cu grad ridicat de risc defecte. Răspunderea reprezentantului autorizat prevăzută în prezentul regulament nu aduce atingere dispozițiilor Directivei 85/374/CEE cu privire la răspunderea pentru produsele cu defect.

(57) [eliminat]

(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. Aceste obligații nu ar trebui să aducă atingere altor obligații ale utilizatorilor în ceea ce privește sistemele de IA cu grad ridicat de risc în temeiul dreptului Uniunii sau al dreptului intern și nu ar trebui să se aplice în cazul în care sistemele respective sunt utilizate în cursul unei activități personale neprofesionale.

(58a) Este oportun să se clarifice faptul că prezentul regulament nu aduce atingere obligațiilor furnizorilor și utilizatorilor de sisteme de IA în rolul lor de operatori de date sau de persoane împuternicite de operatori care decurg din dreptul Uniunii privind protecția datelor cu caracter personal, în măsura în care proiectarea, dezvoltarea sau utilizarea sistemelor de IA implică prelucrarea de date cu caracter personal. De asemenea, este oportun să se clarifice faptul că persoanele vizate continuă să beneficieze de toate drepturile și garanțiile care le sunt acordate de dreptul Uniunii, inclusiv de drepturile legate de procesul decizional individual exclusiv automatizat, inclusiv de crearea de profiluri. Normele armonizate pentru introducerea pe piață, punerea în funcțiune și utilizarea sistemelor de IA instituite în temeiul prezentului regulament ar trebui să faciliteze punerea în aplicare eficace și să permită exercitarea drepturilor persoanelor vizate și a altor căi de atac garantate în temeiul dreptului Uniunii privind protecția datelor cu caracter personal și a altor drepturi fundamentale.

(59) [eliminat]

(60) [eliminat]

(61) Standardizarea ar trebui să joace un rol esențial în furnizarea de soluții tehnice furnizorilor pentru a asigura conformitatea cu prezentul regulament, în conformitate cu stadiul actual al tehnologiei. Conformitatea cu normele armonizate, astfel cum se prevede în Regulamentul (UE) nr. 1025/2012 al Parlamentului European și al Consiliului[25], care ar trebui, în mod normal, să respecte stadiul actual al tehnologiei, ar trebui să fie un mijloc prin care furnizorii să demonstreze conformitatea cu cerințele prezentului regulament. Cu toate acestea, în absența unor trimiteri relevante la standardele armonizate, Comisia ar trebui să poată stabili, prin intermediul unor acte de punere în aplicare, specificații comune pentru anumite cerințe în temeiul prezentului regulament ca soluție excepțională de rezervă pentru a facilita obligația furnizorului de a respecta cerințele prezentului regulament, atunci când procesul de standardizare este blocat sau atunci când există întârzieri în stabilirea unui standard armonizat adecvat. În cazul în care o astfel de întârziere se datorează complexității tehnice a standardului în cauză, acest lucru ar trebui luat în considerare de către Comisie înainte de a avea în vedere stabilirea unor specificații comune. O implicare adecvată a întreprinderilor mici și mijlocii în elaborarea standardelor care sprijină punerea în aplicare a prezentului regulament este esențială pentru promovarea inovării și a competitivității în domeniul inteligenței artificiale în cadrul Uniunii. O astfel de implicare ar trebui asigurată în mod corespunzător, în conformitate cu articolele 5 și 6 din Regulamentul 1025/2012.

[25] 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).

(61a) Este oportun ca, fără a aduce atingere utilizării standardelor armonizate și a specificațiilor comune, furnizorii să beneficieze de o prezumție de conformitate cu cerința relevantă privind datele, atunci când sistemul lor de IA cu grad ridicat de risc a fost antrenat și testat pe baza unor date care reflectă cadrul geografic, comportamental sau funcțional specific în care se intenționează utilizarea sistemului de IA. În mod similar, în conformitate cu articolul 54 alineatul (3) din Regulamentul (UE) 2019/881 al Parlamentului European și al Consiliului, 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 respectiv și ale căror referințe au fost publicate în Jurnalul Oficial al Uniunii Europene ar trebui să fie considerate a fi în conformitate cu cerința de securitate cibernetică menționată în prezentul regulament. Acest lucru nu aduce atingere caracterului voluntar al respectivului sistem de securitate cibernetică.

(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. În ceea ce privește sistemele de IA cu grad ridicat de risc legate de produsele care intră sub incidența Regulamentelor (UE) 745/2017 și (UE) 746/2017 privind dispozitivele medicale, aplicabilitatea cerințelor prezentului regulament nu ar trebui să aducă atingere și să țină seama de logica gestionării riscurilor și de evaluarea beneficiu-risc efectuată în temeiul cadrului privind dispozitivele medicale.

(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. Lista acestor organisme notificate ar trebui trimisă de autoritățile naționale competente Comisiei și celorlalte state membre prin intermediul instrumentului de notificare electronică dezvoltat și gestionat de Comisie în temeiul articolului R23 din Decizia 768/2008.

(66) În conformitate cu noțiunea stabilită de comun acord de modificare substanțială pentru produsele reglementate de legislația de armonizare a Uniunii, este oportun ca, ori de câte ori se produce o modificare care poate afecta respectarea prezentului regulament de către un sistem de IA cu grad ridicat de risc (de exemplu, modificarea sistemului de operare sau a arhitecturii software) sau atunci când scopul preconizat al sistemului se modifică, respectivul sistem de IA să fie considerat un sistem de IA nou care ar trebui să facă obiectul unei noi evaluări a conformității. Cu toate acestea, modificările care afectează algoritmul și performanța sistemelor de IA care continuă să „învețe” după ce au fost introduse pe piață sau puse în funcțiune (și anume, adaptarea automată a modului în care sunt îndeplinite funcțiile) nu ar trebui să constituie o modificare substanțială, cu condiția ca modificările respective să fi fost prestabilite de furnizor și evaluate în momentul evaluării conformității.

(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 se înregistra, precum și de a înregistra informații despre 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. Înainte de a utiliza un sistem de IA cu grad ridicat de risc menționat în anexa III, utilizatorii sistemelor de IA cu grad ridicat de risc care sunt autorități, agenții sau organisme publice, cu excepția autorităților responsabile în materie de aplicare a legii, de control la frontiere, de imigrație sau de azil, precum și autoritățile care sunt utilizatori ai sistemelor de IA cu grad ridicat de risc în domeniul infrastructurii critice se înregistrează, de asemenea, într-o astfel de bază de date și selectează sistemul pe care intenționează să îl utilizeze. Comisia ar trebui să fie operatorul bazei de date respective, în conformitate cu Regulamentul (UE) 2018/1725 al Parlamentului European și al Consiliului[26]. 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.

[26] 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).

(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 punctul de vedere al unei persoane fizice normal informate, suficient de atente și de avizate, ținând seama de circumstanțele și contextul de utilizare. La punerea în aplicare a unei astfel de obligații, caracteristicile persoanelor care aparțin unor grupuri vulnerabile din motive de vârstă sau handicap ar trebui să fie luate în considerare în măsura în care sistemul de IA are rolul de a interacționa și cu aceste grupuri. În plus, persoanele fizice ar trebui să fie informate atunci când sunt expuse la sisteme care, prin prelucrarea datelor lor biometrice, le pot identifica sau deduce emoțiile sau intențiile persoanelor respective sau le pot include în categorii specifice. Astfel de categorii specifice se pot referi la aspecte precum sexul, vârsta, culoarea părului, culoarea ochilor, tatuajele, trăsăturile personale, originea etnică, preferințele și interesele personale sau la alte aspecte, cum ar fi orientarea sexuală sau politică. Astfel de informații 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. Respectarea obligațiilor de informare menționate anterior nu ar trebui interpretată ca indicând faptul că utilizarea sistemului sau a rezultatelor sale este legală în temeiul prezentului regulament sau al altor acte legislative ale Uniunii și ale statelor membre și nu ar trebui să aducă atingere altor obligații de transparență pentru utilizatorii sistemelor de IA prevăzute în dreptul Uniunii sau în cel intern. În plus, aceasta nu ar trebui interpretată în sensul de a indica faptul că utilizarea sistemului sau a rezultatelor sale împiedică dreptul la libertatea de exprimare și dreptul la libertatea artelor și științelor garantate de Carta drepturilor fundamentale a UE, în special atunci când conținutul face parte dintr-o lucrare sau dintr-un program în mod evident creativ, satiric, artistic sau fictiv, sub rezerva unor garanții adecvate pentru drepturile și libertățile terților.

(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 a IA 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), inclusiv a întreprinderilor nou-înființate. Participarea la spațiul de testare în materie de reglementare a IA ar trebui să se concentreze pe aspecte care determină lipsa securității juridice pentru furnizori și potențiali furnizori cu privire la capacitatea acestora de a inova, a experimenta cu IA în Uniune și a contribui la învățarea bazată pe dovezi în materie de reglementare. Supravegherea sistemelor de IA în spațiul de testare în materie de reglementare a IA ar trebui, prin urmare, să acopere dezvoltarea, antrenarea, testarea și validarea lor înainte ca sistemele să fie introduse pe piață sau puse în funcțiune, precum și noțiunea și apariția unei modificări substanțiale care ar putea necesita o nouă procedură de evaluare a conformității. După caz, autoritățile naționale competente care instituie spații de testare în materie de reglementare a IA ar trebui să coopereze cu alte autorități relevante, inclusiv cu cele care supraveghează protecția drepturilor fundamentale, și ar putea permite implicarea altor actori din ecosistemul IA, cum ar fi organizațiile de standardizare naționale sau europene, organismele notificate, instalațiile de testare și experimentare, laboratoarele de cercetare și experimentare, centrele de inovare și organizațiile relevante ale părților interesate și ale societății civile. 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. Spațiile de testare în materie de reglementare a IA instituite în temeiul prezentului regulament nu ar trebui să aducă atingere altor acte legislative care permit instituirea altor spații de testare cu scopul de a asigura conformitatea cu alte acte legislative decât prezentul regulament. După caz, autoritățile competente relevante responsabile de aceste alte spații de testare în materie de reglementare ar trebui să ia în considerare beneficiile utilizării acestor spații de testare și în scopul asigurării conformității sistemelor de IA cu prezentul regulament. Pe baza unui acord între autoritățile naționale competente și participanții la spațiul de testare în materie de reglementare a IA, testarea în condiții reale poate fi, de asemenea, efectuată și supravegheată în cadrul spațiului de testare în materie de reglementare a IA.

(-72a) Prezentul regulament ar trebui să ofere temeiul juridic pentru participanții la spațiul de testare în materie de reglementare a IA de a utiliza datele cu caracter personal colectate în alte scopuri pentru dezvoltarea anumitor sisteme de IA de interes public în cadrul spațiului de testare în materie de reglementare a IA, în conformitate cu articolul 6 alineatul (4) și cu articolul 9 alineatul (2) litera (g) din Regulamentul (UE) 2016/679, precum și cu articolele 5 și 10 din Regulamentul (UE) 2018/1725 și fără a aduce atingere articolului 4 alineatul (2) și articolului 10 din Directiva (UE) 2016/680. Toate celelalte obligații ale operatorilor de date și drepturile persoanelor vizate în temeiul Regulamentului (UE) 2016/679, al Regulamentului (UE) 2018/1725 și al Directivei (UE) 2016/680 rămân aplicabile. În special, prezentul regulament nu ar trebui să ofere un temei juridic în sensul articolului 22 alineatul (2) litera (b) din Regulamentul (UE) 2016/679 și al articolului 24 alineatul (2) litera (b) din Regulamentul (UE) 2018/1725. 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.

(-72a) Pentru a accelera procesul de dezvoltare și introducere pe piață a sistemelor de IA cu grad ridicat de risc enumerate în anexa III, este important ca furnizorii sau potențialii furnizori ai acestor sisteme să poată beneficia, la rândul lor, de un regim specific pentru testarea acestor sisteme în condiții reale, fără a participa la un spațiu de testare în materie de reglementare a IA. Cu toate acestea, în astfel de cazuri și ținând seama de posibilele consecințe ale unor astfel de teste asupra persoanelor fizice, ar trebui să se garanteze faptul că regulamentul introduce garanții și condiții adecvate și suficiente pentru furnizori sau potențiali furnizori. Astfel de garanții ar trebui să includă, printre altele, solicitarea consimțământului în cunoștință de cauză al persoanelor fizice de a participa la teste în condiții reale, cu excepția asigurării respectării legii în cazurile în care solicitarea consimțământului în cunoștință de cauză ar împiedica testarea sistemului de IA. Consimțământul subiecților de a participa la astfel de teste în temeiul prezentului regulament este distinct de consimțământului persoanelor vizate pentru prelucrarea datelor lor cu caracter personal în temeiul legislației relevante privind protecția datelor și nu aduce atingere acestuia.

(73) Pentru a promova și proteja inovarea, este important ca interesele IMM-urilor furnizoare și ale utilizatorilor 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 IMM-urilor furnizoare 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.

(73a) Pentru a promova și a proteja inovarea, platforma de IA la cerere, toate programele și proiectele de finanțare relevante ale UE, cum ar fi programul Europa digitală, Orizont Europa, puse în aplicare de Comisie și de statele membre la nivel național sau la nivelul UE, ar trebui să contribuie la îndeplinirea obiectivelor prezentului regulament.

(74) În special, 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, în special de către IMM-uri, precum și de către 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.

(74a) În plus, pentru a asigura proporționalitatea, având în vedere dimensiunea foarte mică a unor operatori în ceea ce privește costurile inovării, este oportun ca microîntreprinderile să fie exceptate de obligațiile cele mai costisitoare, cum ar fi instituirea unui sistem de management al calității care ar reduce sarcina administrativă și costurile pentru întreprinderile respective, fără a afecta nivelul de protecție și necesitatea de a respecta cerințele pentru sistemele de IA cu grad ridicat de risc.

(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 reflecte diferitele interese ale ecosistemului IA și să fie alcătuit din reprezentanți ai statelor membre. Pentru a asigura implicarea părților interesate relevante, ar trebui creat un subgrup permanent al comitetului. 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 aspecte de asigurare a respectării legii, specificații tehnice sau standarde existente referitoare la cerințele stabilite în prezentul regulament, precum și furnizarea de consiliere și asistență Comisiei și statelor lor membre și autorităților naționale competente ale acestora cu privire la chestiuni specifice legate de inteligența artificială. Pentru a oferi o anumită flexibilitate statelor membre în ceea ce privește desemnarea reprezentanților lor în cadrul Comitetului pentru IA, astfel de reprezentanți pot fi persoane care aparțin unor entități publice care ar trebui să aibă competențele și prerogativele relevante pentru a facilita coordonarea la nivel național și pentru a contribui la îndeplinirea sarcinilor comitetului. Comitetul ar trebui să instituie două subgrupuri permanente pentru a oferi o platformă de cooperare și de schimb între autoritățile de supraveghere a pieței și autoritățile de notificare cu privire la aspecte legate de supravegherea pieței și, respectiv, de organismele notificate. Subgrupul permanent pentru supravegherea pieței ar trebui să acționeze în calitate de grup de cooperare administrativă (ADCO) pentru prezentul regulament în sensul articolului 30 din Regulamentul (UE) 2019/1020. În conformitate cu rolul și sarcinile Comisiei în temeiul articolului 33 din Regulamentul (UE) 2019/1020, Comisia ar trebui să sprijine activitățile subgrupului permanent pentru supravegherea pieței prin efectuarea de evaluări sau studii de piață, în special în vederea identificării aspectelor prezentului regulament care necesită o coordonare specifică și urgentă între autoritățile de supraveghere a pieței. Comitetul poate înființa alte subgrupuri permanente sau temporare, după caz, în scopul examinării unor chestiuni specifice. Comitetul ar trebui, de asemenea, să coopereze, după caz, cu organismele, grupurile de experți și rețelele relevante ale UE care își desfășoară activitatea în contextul legislației relevante a UE, inclusiv, în special, cu cele care își desfășoară activitatea în temeiul normelor relevante ale UE privind datele, produsele și serviciile digitale.

(76a) Comisia ar trebui să sprijine în mod activ statele membre și operatorii în punerea în aplicare și asigurarea respectării prezentului regulament. În acest sens, Comisia ar trebui să elaboreze orientări cu privire la subiecte specifice menite să faciliteze aplicarea prezentului regulament, acordând în același timp o atenție deosebită nevoilor IMM-urilor și întreprinderilor nou-înființate din sectoarele cele mai susceptibile de a fi afectate. Pentru a sprijini punerea în aplicare adecvată și capacitățile statelor membre, la nivelul Uniunii ar trebui create și puse la dispoziția statelor membre instalații de testare a IA, precum și un grup de experți competenți.

(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. Statele membre pot decide să numească orice tip de entitate publică pentru a îndeplini sarcinile autorităților naționale competente în sensul prezentului regulament, în conformitate cu caracteristicile și nevoile organizaționale naționale specifice ale acestora.

(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 care decurge din utilizarea 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. Autoritățile de supraveghere a pieței desemnate în temeiul prezentului regulament ar trebui să dispună de toate competențele de asigurare a respectării legii în temeiul prezentului regulament și al Regulamentului (UE) 2019/1020 și ar trebui să își exercite competențele și să își îndeplinească atribuțiile în mod independent, imparțial și nepărtinitor. Deși majoritatea sistemelor de IA nu fac obiectul unor cerințe și obligații specifice în temeiul prezentului regulament, autoritățile de supraveghere a pieței pot lua măsuri în legătură cu toate sistemele de IA atunci când acestea prezintă un risc în conformitate cu prezentul regulament. Având în vedere natura specifică a instituțiilor, agențiilor și organismelor Uniunii care intră în domeniul de aplicare al prezentului regulament, este oportun ca Autoritatea Europeană pentru Protecția Datelor să fie desemnată drept autoritatea competentă de supraveghere a pieței pentru acestea. Acest lucru nu ar trebui să aducă atingere desemnării autorităților naționale competente de către statele membre. Activitățile de supraveghere a pieței nu ar trebui să afecteze capacitatea entităților supravegheate de a-și îndeplini sarcinile în mod independent, atunci când independența lor este impusă de dreptul Uniunii.

(79a) Prezentul regulament nu aduce atingere competențelor, sarcinilor, prerogativelor și independenței autorităților publice naționale relevante sau ale organismelor care supraveghează aplicarea dreptului Uniunii care protejează drepturile fundamentale, inclusiv ale organismelor de promovare a egalității și ale autorităților de protecție a datelor. În cazul în care acest lucru este necesar pentru îndeplinirea mandatului lor, autoritățile sau organismele publice naționale respective ar trebui să aibă, de asemenea, acces la orice documentație creată în temeiul prezentului regulament. Ar trebui stabilită o procedură de salvgardare specifică pentru a asigura respectarea legii, în mod adecvat și în timp util, împotriva sistemelor de IA care prezintă un risc pentru sănătate, siguranță și drepturile fundamentale. Procedura pentru astfel de sisteme de IA care prezintă un risc ar trebui să se aplice sistemelor de IA cu grad ridicat de risc care prezintă un risc, sistemelor interzise care au fost introduse pe piață, puse în funcțiune sau utilizate cu încălcarea practicilor interzise prevăzute în prezentul regulament, precum și sistemelor de IA care au fost puse la dispoziție cu încălcarea cerințelor de transparență prevăzute în prezentul regulament și care prezintă un risc.

(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 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, cu excepția cazului în care statele membre decid să desemneze o altă autoritate pentru a îndeplini aceste sarcini de supraveghere a pieței. Autoritățile competente respective ar trebui să dețină toate competențele privind supravegherea pieței în temeiul prezentului regulament și al Regulamentului (UE) 2019/1020 pentru a asigura respectarea cerințelor și a obligațiilor prevăzute în prezentul regulament, inclusiv competențele de a desfășura activități ex post de supraveghere a pieței care pot fi integrate, după caz, în mecanismele și procedurile lor de supraveghere existente în temeiul legislației relevante a Uniunii privind serviciile financiare. Este oportun să se considere că, atunci când acționează în calitate de autorități de supraveghere a pieței în temeiul prezentului regulament, autoritățile naționale responsabile de supravegherea instituțiilor de credit reglementate în temeiul Directivei 2013/36/UE, care participă la mecanismul unic de supraveghere (MUS) instituit prin Regulamentul nr. 1024/2013 al Consiliului, ar trebui să raporteze fără întârziere Băncii Centrale Europene orice informații identificate în cursul activităților lor de supraveghere a pieței care ar putea prezenta un interes pentru sarcinile de supraveghere prudențială ale Băncii Centrale Europene, astfel cum se specifică în regulamentul respectiv. 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[27], este, de asemenea, oportun să se integreze 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

[27] 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).

risc, în măsura în care acestea se aplică instituțiilor de credit reglementate de Directiva 2013/36/UE. Același regim ar trebui să se aplice întreprinderilor de asigurare și reasigurare și holdingurilor de asigurare în temeiul Directivei 2009/138/CE (Solvabilitate II), intermediarilor de asigurări în temeiul Directivei (UE) 2016/97, precum și altor tipuri de instituții financiare care fac obiectul cerințelor privind guvernanța internă, mecanismelor sau proceselor instituite în temeiul legislației relevante a Uniunii privind serviciile financiare pentru a asigura coerența și egalitatea de tratament în sectorul financiar.

(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 aplicabile sistemelor de IA cu grad ridicat de risc, adaptate în funcție de scopul preconizat al sistemelor și de riscul mai redus implicat. 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.

(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[28] 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, în conformitate cu dreptul Uniunii sau cu dreptul intern.

[28] 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).

(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, și cu respectarea principiului *ne bis in idem*. 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 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 adecvate, inclusiv la nivel de experți, și ca respectivele consultări să se desfășoare în conformitate cu principiile stabilite în Acordul interinstituțional din 13 aprilie 2016 privind o mai bună legiferare[29]. 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. Astfel de consultări și sprijinul consultativ ar trebui, de asemenea, să se desfășoare în cadrul activităților Comitetului pentru IA și al subgrupurilor sale.

[29] JO L 123, 12.5.2016, p. 1.

(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[30]. Este deosebit de important ca, în conformitate cu principiile stabilite în Acordul interinstituțional din 13 aprilie 2016 privind o mai bună legiferare, ori de câte ori este necesară o expertiză mai amplă în pregătirea timpurie a proiectelor de acte de punere în aplicare, Comisia să recurgă la grupuri de experți, să consulte părțile interesate vizate sau să organizeze consultări publice, după caz. Astfel de consultări și sprijinul consultativ ar trebui să se desfășoare, de asemenea, în cadrul activităților Comitetului pentru IA și al subgrupurilor sale, inclusiv pregătirea actelor de punere în aplicare în legătură cu articolele 4, 4b și 6.

(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 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.

(87a) Pentru a asigura securitatea juridică, a asigura o perioadă de adaptare adecvată pentru operatori și a evita perturbarea pieței, inclusiv prin asigurarea continuității utilizării sistemelor de IA, este oportun ca prezentul regulament să se aplice sistemelor de IA cu grad ridicat de risc care au fost introduse pe piață sau puse în funcțiune înainte de data generală de aplicare a acestora, numai dacă, de la data respectivă, sistemele respective fac obiectul unor modificări semnificative în ceea ce privește proiectarea sau scopul lor preconizat. Este oportun să se clarifice faptul că, în acest sens, conceptul de modificare semnificativă ar trebui înțeles ca fiind echivalent în esență cu noțiunea de modificare substanțială, care este utilizată numai în ceea ce privește sistemele de IA cu grad ridicat de risc, astfel cum sunt definite în prezentul regulament.

[30] 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).

(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 anumite sisteme de IA;

(d) norme privind monitorizarea și supravegherea pieței și guvernanța;

(e) măsuri de sprijinire a inovării.

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 prezenți fizic sau stabiliți în Uniune sau într-o țară terță;

(b) utilizatorii sistemelor de IA care sunt prezenți fizic sau stabiliți pe teritoriul Uniunii;

(c) furnizorii și utilizatorii de sisteme de IA care sunt prezenți fizic sau stabiliți într-o țară terță, în cazul în care rezultatele produse de sistem sunt utilizate în Uniune;

(d) importatorii și distribuitorii de sisteme de IA;

(e) fabricanții de produse care introduc pe piață sau pun în funcțiune un sistem de IA împreună cu produsul lor și sub numele sau marca lor comercială;

(f) reprezentanții autorizați ai furnizorilor, stabiliți în Uniune;

(2) În cazul sistemelor de IA clasificate ca prezentând un grad ridicat de risc în conformitate cu articolul 6 alineatele (1) și (2) legate de produse care fac obiectul legislației de armonizare a Uniunii enumerate în anexa II secțiunea B, se aplică numai articolul 84 din prezentul regulament. Articolul 53 se aplică numai în măsura în care cerințele pentru sistemele de IA cu grad ridicat de risc menționate în prezentul regulament au fost integrate în respectiva legislație de armonizare a Uniunii.

(3) Prezentul regulament nu se aplică sistemelor de IA în cazul și în măsura în care sunt introduse pe piață, puse în funcțiune sau utilizate cu sau fără a fi modificate în scopul unor activități care nu intră în domeniul de aplicare al dreptului Uniunii și, în orice caz, pentru activități militare, de apărare sau de securitate națională, indiferent de tipul de entitate care desfășoară activitățile respective.

În plus, prezentul regulament nu se aplică sistemelor de IA care nu sunt introduse pe piață ori puse în funcțiune în Uniune, în cazul în care rezultatul este utilizat în Uniune în scopul unor activități care nu intră în domeniul de aplicare al dreptului Uniunii și, în orice caz, pentru activități militare, de apărare sau de securitate națională, indiferent de tipul de entitate care desfășoară activitățile respective.

(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 4 din Directiva 2000/31/CE a Parlamentului European și a Consiliului[31] [*astfel cum urmează să fie înlocuite cu dispozițiile corespunzătoare din Actul privind serviciile digitale*].

(6) Prezentul regulament nu se aplică sistemelor de IA, inclusiv rezultatelor acestora, dezvoltate și puse în funcțiune special și exclusiv pentru cercetare și dezvoltare științifică.

(7) Prezentul regulament nu se aplică niciunei activități de cercetare și dezvoltare privind sistemele de IA.

(8) Prezentul regulament nu se aplică obligațiilor utilizatorilor persoane fizice care utilizează sisteme de IA în cursul unei activități neprofesionale pur personale, cu excepția articolului 52.

---

[31] 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).

Articolul 3

Definiții

În sensul prezentului regulament, se aplică următoarele definiții:

1. „sistem de inteligență artificială” (sistem de IA) înseamnă un sistem conceput să funcționeze cu elemente de autonomie și care, pe baza datelor și a datelor de intrare furnizate automat și/sau de factorul uman, deduce o modalitate prin care să atingă o serie de obiective utilizând abordări bazate pe învățarea automată și/sau pe logică și pe cunoaștere și produce rezultate generate de sistem de tip conținut (sisteme de IA generative), previziuni, recomandări sau decizii, influențând mediul cu care interacționează sistemul de IA;

1a. „ciclul de viață al unui sistem de IA” înseamnă durata unui sistem de IA, de la proiectare până la scoaterea din uz. Fără a aduce atingere competențelor autorităților de supraveghere a pieței, scoaterea din uz poate avea loc în orice moment al etapei de monitorizare ulterioară introducerii pe piață pe baza deciziei furnizorului și implică faptul că sistemul nu mai poate fi utilizat. Ciclul de viață al unui sistem de IA se încheie, de asemenea, printr-o modificare substanțială adusă sistemului respectiv, efectuată de către furnizor sau de către orice altă persoană fizică sau juridică, caz în care sistemul de IA modificat substanțial este considerat un nou sistem de IA.

1b. „sistem de IA de uz general” înseamnă un sistem de IA care, indiferent de modul în care este introdus pe piață sau pus în funcțiune, inclusiv ca software cu sursă deschisă, urmează, conform intenției furnizorului, să realizeze funcții general aplicabile, cum ar fi recunoașterea imaginilor sau a vorbirii, generarea de fișiere audio sau video, detectarea de modele, răspunsul la întrebări, traducere sau altele; un sistem de IA de uz general poate fi folosit într-o gamă variată de contexte și poate fi integrat în numeroase alte sisteme de IA;

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 și introduce respectivul sistem pe piață sau îl pune în funcțiune sub propriul nume sau propria marcă comercială, contra cost sau gratuit;

3. [eliminat]

3a. întreprindere mică și mijlocie (IMM) înseamnă o întreprindere astfel cum este definită în anexa la Recomandarea 2003/361/CE a Comisiei privind definirea microîntreprinderilor și a întreprinderilor mici și mijlocii;

4. „utilizator” înseamnă orice persoană fizică sau juridică, inclusiv o autoritate publică, o agenție sau un alt organism sub autoritatea căruia este utilizat un sistem de IA;

5. „reprezentant autorizat” înseamnă orice persoană fizică sau juridică prezentă fizic sau stabilită în Uniune care a primit și a acceptat 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;

5a. „fabricantul produsului” înseamnă un producător în sensul oricăruia dintre actele legislative în materie de armonizare ale Uniunii menționate în anexa II;

6. „importator” înseamnă orice persoană fizică sau juridică prezentă fizic sau stabilită în Uniune care introduce pe piață 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;

8. „operator” înseamnă furnizorul, fabricantul produsului, utilizatorul, reprezentantul autorizat, importatorul sau 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 în Uniune, 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;

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;

16. „rechemare a unui sistem de IA” înseamnă orice măsură care are drept scop returnarea către furnizor, scoaterea din funcțiune sau dezactivarea utilizării unui sistem de IA deja pus la dispoziția utilizatorilor;

17. „retragerea unui sistem de IA” înseamnă orice măsură cu scopul de a împiedica punerea la dispoziție pe piață a unui sistem de IA din lanțul de aprovizionare;

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

19. „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 cu grad ridicat de risc;

20. „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;

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 o modificare a scopului preconizat pentru care a fost evaluat sistemul de IA; 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.

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 sau la articolul 4b 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. „sistem de monitorizare ulterioară introducerii pe piață” înseamnă toate activitățile desfășurate de furnizorii de sisteme de IA pentru a colecta și a revizui 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. „specificație comună” înseamnă un set de specificații tehnice, astfel cum sunt definite la articolul 2 punctul 4 din Regulamentul (UE) nr. 1025/2012, care oferă mijloacele de a respecta anumite cerințe 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;

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, 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 stările psihologice, 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 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, de obicei la distanță, fără implicarea activă a acestora, prin compararea datelor biometrice ale unei persoane cu datele biometrice conținute într-o bază de date de referință;

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 împreună, în mod instantaneu sau aproape instantaneu;

38. [eliminat]

39. „spațiu accesibil publicului” înseamnă orice loc fizic aflat în proprietate publică sau privată, accesibil unui număr nedeterminat de persoane fizice, indiferent dacă anumite condiții sau circumstanțe de acces au fost prestabilite și indiferent de potențiale restricții de capacitate;

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 sau în numele acestora 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. [eliminat]

43. „autoritate națională competentă” înseamnă oricare dintre următoarele: autoritatea de notificare și autoritatea de supraveghere a pieței. În ceea ce privește sistemele de IA puse în funcțiune sau utilizate de instituțiile, agențiile, oficiile și organele UE, Autoritatea Europeană pentru Protecția Datelor îndeplinește responsabilitățile care, în statele membre, sunt încredințate autorității naționale competente și, după caz, orice trimitere la autoritățile naționale competente sau la autoritățile de supraveghere a pieței din prezentul regulament se interpretează ca trimitere la Autoritatea Europeană pentru Protecția Datelor;

44. „incident grav” înseamnă orice incident sau funcționare necorespunzătoare a unui sistem de IA care, direct sau indirect, conduce la oricare dintre următoarele:

(a) decesul unei persoane sau afectarea gravă a sănătății unei persoane;

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

(c) încălcarea obligațiilor care decurg din dreptul Uniunii menit să protejeze drepturile fundamentale;

(d) daune grave aduse bunurilor sau mediului.

45. „infrastructură critică” înseamnă un activ, un sistem sau o componentă a acestuia care este necesar(ă) pentru furnizarea unui serviciu esențial pentru menținerea funcțiilor societale sau a activităților economice vitale în sensul articolului 2 alineatele (4) și (5) din Directiva ... privind reziliența entităților critice;

46. „date cu caracter personal” înseamnă date astfel cum sunt definite la articolul 4 punctul 1 din Regulamentul (UE) 2016/679;

47. „date fără caracter personal” înseamnă date, altele decât datele cu caracter personal definite la articolul 4 punctul 1 din Regulamentul (UE) 2016/679;

48. „testare în condiții reale” înseamnă testarea temporară a unui sistem de IA în scopul său preconizat, în condiții reale, în afara unui laborator sau a unui mediu simulat în alt mod, în vederea colectării de date fiabile și solide și a evaluării și verificării conformității sistemului de IA cu cerințele prezentului regulament; testarea în condiții reale nu este considerată ca echivalentă cu introducerea sistemul de IA pe piață sau punerea în funcțiune a acestuia în sensul prezentului regulament, dacă sunt îndeplinite toate condițiile prevăzute la articolul 53 sau la articolul 54a;

49. „plan de testare în condiții reale” înseamnă un document care descrie obiectivele, metodologia, domeniul de aplicare geografic, demografic și temporal, monitorizarea, organizarea și efectuarea testelor în condiții reale;

50. „subiect” în scopul testării în condiții reale înseamnă o persoană fizică care participă la testarea în condiții reale;

51. „consimțământ în cunoștință de cauză” înseamnă exprimarea liberă și voluntară de către un subiect a dorinței sale de a participa la o anumită testare în condiții reale, după ce a fost informat cu privire la toate aspectele testării care sunt relevante pentru decizia sa de a participa; în cazul minorilor și al subiecților aflați în incapacitate, consimțământul în cunoștință de cauză este acordat de reprezentantul desemnat legal al acestora;

52. „spațiu de testare în materie de reglementare a IA” înseamnă un cadru concret instituit de o autoritate națională competentă care oferă furnizorilor sau potențialilor furnizori de sisteme de IA posibilitatea de a dezvolta, de a antrena, de a valida și de a testa, după caz în condiții reale, un sistem de IA inovator, pe baza unui plan specific, pentru o perioadă limitată de timp, sub supraveghere reglementară.

Articolul 4

Acte de punere în aplicare

În vederea asigurării unor condiții uniforme pentru punerea în aplicare a prezentului regulament în ceea ce privește abordările bazate pe învățarea automată și abordările bazate pe conectare și pe cunoaștere menționate la articolul 3 alineatul (1), Comisia poate adopta acte de punere în aplicare pentru a specifica elementele tehnice ale abordărilor respective, ținând seama de evoluțiile tehnologice și ale pieței. Actele de punere în aplicare respective se adoptă în conformitate cu procedura de examinare menționată la articolul 74 alineatul (2).

TITLUL IA

SISTEME DE IA DE UZ GENERAL

Articolul 4a

Conformitatea sistemelor de IA de uz general cu prezentul regulament

1. Fără a aduce atingere articolelor 5, 52, 53 și 69 din prezentul regulament, sistemele de IA de uz general respectă numai cerințele și obligațiile prevăzute la articolul 4b.

2. Astfel de cerințe și obligații se aplică indiferent dacă sistemul de IA de uz general este introdus pe piață sau pus în funcțiune ca model preantrenat și dacă modelul urmează să fie calibrat în continuare de către utilizatorul sistemului de IA de uz general.

Articolul 4b

Cerințe pentru sistemele de IA de uz general și obligații pentru furnizorii unor astfel de sisteme

1. Sistemele de IA de uz general care pot fi utilizate drept sisteme de IA cu grad ridicat de risc sau drept componente ale sistemelor de IA cu grad ridicat de risc în sensul articolului 6 respectă cerințele stabilite în titlul III capitolul 2 din prezentul regulament de la data aplicării actelor de punere în aplicare adoptate de Comisie în conformitate cu procedura de examinare menționată la articolul 74 alineatul (2) și în termen de cel mult 18 luni de la intrarea în vigoare a prezentului regulament. Respectivele acte de punere în aplicare specifică și adaptează aplicarea cerințelor stabilite în titlul III capitolul 2 la sistemele de IA de uz general, având în vedere caracteristicile lor, fezabilitatea tehnică, particularitățile lanțului valoric al IA și evoluțiile pieței și ale tehnologiei. La îndeplinirea acestor cerințe, se ține seama de stadiul actual general recunoscut al tehnologiei.

2. Furnizorii de sisteme de IA de uz general menționați la alineatul (1) respectă, de la data aplicării actelor de punere în aplicare menționate la alineatul (1), obligațiile prevăzute la articolele 16aa, 16e, 16f, 16 g, 16i, 16j, 25, 48 și 61.

3. Pentru a respecta obligațiile prevăzute la articolul 16e, furnizorii urmează procedura de evaluare a conformității bazată pe controlul intern, menționată în anexa VI, punctele 3 și 4.

4. De asemenea, furnizorii acestor sisteme păstrează documentația tehnică menționată la articolul 11 la dispoziția autorităților naționale competente pentru o perioadă de zece ani de la introducerea pe piața Uniunii sau punerea în funcțiune în Uniune a sistemului de IA de uz general.

5. Furnizorii de sisteme de IA de uz general cooperează cu alți furnizori care intenționează să pună în funcțiune sau să introducă astfel de sisteme pe piața Uniunii drept sisteme de IA cu grad ridicat de risc, sau drept componente ale sistemelor de IA cu grad ridicat de risc, și furnizează informațiile necesare furnizorilor respectivi, pentru a le permite să își respecte obligațiile care le revin în temeiul prezentului regulament. În cadrul acestei cooperări între furnizori se păstrează, după caz, drepturile de proprietate intelectuală și informațiile comerciale confidențiale sau secretele comerciale, în conformitate cu articolul 70. Pentru a asigura condiții uniforme pentru punerea în aplicare a prezentului regulament în ceea ce privește informațiile care trebuie comunicate de furnizorii de sisteme de IA de uz general, Comisia poate adopta acte de punere în aplicare în conformitate cu procedura de examinare menționată la articolul 74 alineatul (2).

6. În vederea respectării cerințelor și obligațiilor menționate la alineatele (1), (2) și (3):

- orice trimitere la scopul preconizat este interpretată ca referindu-se la posibila utilizare a sistemelor de IA de uz general drept sisteme de IA cu grad ridicat de risc sau drept componente ale sistemelor de IA cu grad ridicat de risc în sensul articolului 6;

- orice trimitere la cerințele pentru sistemele de IA cu grad ridicat de risc menționate la capitolul II titlul III se interpretează ca referindu-se numai la cerințele prevăzute în prezentul articol.

Articolul 4c

Excepții la articolul 4b

1. Articolul 4b nu se aplică atunci când furnizorul a exclus în mod explicit orice uz cu grad ridicat de risc din instrucțiunile de utilizare sau din informațiile care însoțesc sistemul de IA de uz general.

2. Excluderea se face cu bună-credință și nu este considerată justificată în cazul în care furnizorul are motive suficiente să considere că sistemul poate fi utilizat în mod abuziv.

3. Atunci când detectează sau este informat cu privire la utilizarea abuzivă pe piață, furnizorul ia toate măsurile necesare și proporționale pentru a împiedica continuarea utilizării abuzive, în special ținând seama de amploarea utilizării abuzive și de gravitatea riscurilor asociate.

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, ceea ce are drept obiectiv sau efect denaturarea în mod semnificativ a comportamentului unei persoane într-un mod care aduce sau este susceptibil în mod rezonabil de a 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, sau a unei situații sociale sau economice specifice, ceea ce are drept obiectiv sau efect denaturarea în mod semnificativ a comportamentului unei persoane care aparține grupului respectiv într-un mod care aduce sau este susceptibil în mod rezonabil de a aduce prejudicii fizice sau psihologice persoanei respective sau altei persoane;

(c) introducerea pe piață, punerea în funcțiune sau utilizarea sistemelor de IA pentru evaluarea sau clasificarea 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 aplicat anumitor persoane fizice sau unor grupuri 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 aplicat anumitor persoane fizice sau unor grupuri 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 de către autoritățile de aplicare a legii sau în numele acestora 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;

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

(iii) localizarea sau identificarea unei persoane fizice în scopul desfășurării unei investigații penale, al urmăririi penale sau al executării unor sancțiuni penale menționate la articolul 2 alineatul (2) din Decizia-cadru 2002/584/JAI a Consiliului[32], pasibile de pedepse sau de măsuri de siguranță privative de libertate în statul membru în cauză pentru o perioadă maximă de cel puțin trei ani, sau pentru alte infracțiuni specifice pasibile de pedepse sau de măsuri de siguranță privative de libertate în statul membru în cauză pentru o perioadă maximă de cel puțin cinci 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;

[32] 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).

(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 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 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, cu condiția ca autorizația respectivă să fie solicitată fără întârzieri nejustificate în timpul utilizării sistemului de IA și, în cazul în care autorizația respectivă este respinsă, utilizarea sistemului să înceteze cu efect imediat.

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), precum și pentru raportarea cu privire la acestea. 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) Un sistem de IA care este el însuși un produs vizat de legislația de armonizare a Uniunii menționată în anexa II este considerat ca prezentând un grad ridicat de risc dacă 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 menționate mai sus.

(2) Un sistem de IA destinat a fi utilizat ca o componentă de siguranță a unui produs vizat de legislația menționată la alineatul (1) este considerat a fi un sistem cu grad ridicat de risc dacă 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 menționate mai sus. Această dispoziție se aplică indiferent dacă sistemul de IA este introdus pe piață sau pus în funcțiune independent de produs.

(3) Sistemele de IA menționate în anexa III sunt considerate ca prezentând un grad ridicat de risc, cu excepția cazului în care rezultatul sistemului este pur accesoriu în raport cu acțiunea relevantă sau cu decizia care urmează să fie luată și, prin urmare, nu este susceptibil să genereze un risc semnificativ pentru sănătate, siguranță sau drepturile fundamentale.

În vederea asigurării unor condiții uniforme pentru punerea în aplicare a prezentului regulament, Comisia adoptă, în termen de cel mult un an de la intrarea în vigoare a prezentului regulament, acte de punere în aplicare pentru a preciza circumstanțele în care rezultatul sistemelor de IA menționate în anexa III ar fi pur accesoriu în raport cu acțiunea relevantă sau cu decizia care urmează să fie luată. Actele de punere în aplicare respective se adoptă în conformitate cu procedura de examinare menționată la articolul 74 alineatul (2).

Articolul 7

Modificări ale anexei III

(1) Comisia este împuternicită să adopte acte delegate în conformitate cu articolul 73 pentru a modifica 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 nu 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;

(i) amploarea și probabilitatea beneficiilor utilizării IA pentru persoane, grupuri sau societate în general.

(3) Comisia este împuternicită să adopte acte delegate în conformitate cu articolul 73 pentru a modifica lista din anexa III prin eliminarea sistemelor de IA cu grad ridicat de risc în cazul în care sunt îndeplinite cumulativ următoarele două condiții:

(a) sistemul (sistemele) de IA cu grad ridicat de risc în cauză nu mai prezintă riscuri semnificative pentru drepturile fundamentale, sănătate sau siguranță, ținând seama de criteriile enumerate la alineatul (2);

(b) eliminarea nu reduce nivelul general de protecție a sănătății, siguranței și drepturilor fundamentale în temeiul dreptului Uniunii.

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, ținând cont de stadiul actual general recunoscut al tehnologiei.

(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 este înțeles ca un proces iterativ continuu planificat și 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 la adresa sănătății, siguranței și drepturilor fundamentale, având în vedere scopul preconizat al sistemului de IA cu grad ridicat de risc;

(b) [eliminat]

(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.

Riscurile menționate la prezentul alineat se referă numai la riscurile care pot fi atenuate sau eliminate în mod rezonabil prin dezvoltarea sau proiectarea sistemului de IA cu grad ridicat de risc sau prin furnizarea de informații tehnice adecvate.

(3) Măsurile de gestionare a riscurilor menționate la alineatul (2) litera (d) țin seama în mod corespunzător de efectele și interacțiunea posibilă care rezultă din aplicarea combinată a cerințelor prevăzute în prezentul capitol 2, în vederea reducerii la minimum a riscurilor într-un mod mai eficace, obținându-se totodată un echilibru adecvat în punerea în aplicare a măsurilor de îndeplinire a cerințelor respective.

(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.

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

(a) eliminarea sau reducerea riscurilor identificate și evaluate în temeiul alineatului (2), pe cât posibil prin proiectarea și dezvoltarea adecvată a sistemului de IA cu grad ridicat de risc;

(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.

În vederea eliminării sau reducerii 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 pentru a asigura faptul că sistemele de IA cu grad ridicat de risc funcționează într-un mod coerent cu scopul preconizat și sunt conforme cu cerințele stabilite în prezentul capitol.

(6) Procedurile de testare pot include testarea în condiții reale, în conformitate cu articolul 54a.

(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) Sistemul de gestionare a riscurilor descris la alineatele (1)-(7) evaluează în mod concret posibilitatea ca sistemul de IA cu grad ridicat de risc să fie accesat de persoane cu vârsta sub 18 ani sau să aibă un impact asupra acestora.

(9) Pentru furnizorii de sisteme de IA cu grad ridicat de risc care fac obiectul unor cerințe privind procesele interne de gestionare a riscurilor în temeiul dreptului sectorial relevant al Uniunii, aspectele descrise la alineatele (1)-(8) pot face parte din procedurile de gestionare a riscurilor stabilite în temeiul legislației respective.

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) procesele de colectare a 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 care sunt susceptibile să afecteze sănătatea și siguranța persoanelor fizice sau să ducă la o discriminare interzisă de dreptul Uniunii;

(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 sunt relevante, reprezentative, și pe cât posibil, 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 sistemelor de IA cu grad ridicat de risc care nu utilizează tehnici care implică antrenarea de modele, alineatele (2)-(5) se aplică numai seturilor de date de testare.

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 într-un mod clar și cuprinzător, pentru a evalua conformitatea sistemului de IA cu cerințele respective. Aceasta conține cel puțin elementele prevăzute în anexa IV sau, în cazul IMM-urilor, inclusiv al întreprinderilor nou-înființate, orice documentație echivalentă care îndeplinește aceleași obiective, cu excepția cazului în care autoritatea competentă o consideră necorespunzătoare.

(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 permit din punct de vedere tehnic înregistrarea automată a evenimentelor („fișiere de jurnalizare”) pe durata ciclului de viață al sistemului.

(2) Pentru a asigura un nivel de trasabilitate a funcționării sistemului de IA care să fie adecvat scopului preconizat al sistemului, capacitățile de jurnalizare permit înregistrarea evenimentelor relevante pentru

(i) identificarea 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;

facilitarea monitorizării ulterioare introducerii pe piață menționate la articolul 61 și

monitorizarea funcționării sistemelor de IA cu grad ridicat de risc menționate la articolul 29 alineatul (4).

(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 asigura respectarea obligațiilor relevante ale utilizatorului și ale furnizorului prevăzute în capitolul 3 din prezentul titlu și pentru a le permite utilizatorilor să înțeleagă și să utilizeze sistemul în mod corespunzător.

(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, inclusiv cu privire la mediul geografic, comportamental sau funcțional specific în care sistemul de IA cu grad ridicat de risc urmează să fie utilizat;

(ii) nivelul de acuratețe, inclusiv indicatorii săi, de robustețe și de 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, care poate conduce la riscurile pentru sănătate și siguranță sau pentru drepturile fundamentale menționate la articolul 9 alineatul (2);

(iv) după caz, comportamentul său privind anumite persoane sau grupuri 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;

(vi) după caz, descrierea rezultatelor preconizate ale sistemului.

(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) resursele de calcul și resursele hardware necesare, durata de viață preconizată a sistemului de IA cu grad ridicat de risc și orice măsuri de întreținere și de îngrijire, inclusiv frecvența lor, necesare pentru a asigura funcționarea corespunzătoare a sistemului de IA respectiv, inclusiv în ceea ce privește actualizările software-ului.

(f) o descriere a mecanismului inclus în sistemul de IA care să permită utilizatorilor să colecteze, să stocheze și să interpreteze în mod corespunzător fișierele de jurnalizare după caz.

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 tipuri de măsuri:

(a) măsuri 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) măsuri 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) În scopul punerii în aplicare a alineatelor (1)-(3), sistemul de IA cu grad ridicat de risc este pus la dispoziția utilizatorului astfel încât persoanelor fizice cărora li se încredințează supravegherea umană să li se permită, în funcție de circumstanțe și proporțional cu acestea, următoarele:

(a) să înțeleagă capacitățile și limitările sistemului de IA cu grad ridicat de risc și să fie în măsură să monitorizeze în mod corespunzător funcționarea acestuia;

(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”);

(c) să interpreteze corect rezultatele sistemului de IA cu grad ridicat de risc, ținând seama, de exemplu, de instrumentele și metodele de interpretare disponibile;

(d) 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 intervină 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 separat și confirmat de cel puțin două persoane fizice. Cerința unei verificări separate de către cel puțin două persoane fizice nu se aplică sistemelor de IA cu grad ridicat de risc utilizate în scopul asigurării respectării legii, al imigrației, al controlului la frontiere sau al azilului, în cazurile în care dreptul Uniunii sau dreptul intern consideră că aplicarea acestei cerințe este disproporționată.

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 acurateță 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 elimine sau să reducă pe cât posibil riscul unor eventuale rezultate părtinitoare care să influențeze datele 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;

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

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

(c) păstrează documentația menționată la articolul 18;

(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 menționate la articolul 20;

(e) se asigură că sistemul de IA cu grad ridicat de risc este supus procedurii relevante de evaluare a conformității menționată la articolul 43, înainte de introducerea sa pe piață sau de punerea sa în funcțiune;

(f) respectă obligațiile de înregistrare menționate la articolul 51 alineatul (1);

(g) iau măsurile corective necesare, astfel cum se menționează la articolul 21, 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 autoritatea națională competentă relevantă a 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 unui incident grav 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.

(2a) Pentru furnizorii de sisteme de IA cu grad ridicat de risc care fac obiectul unor obligații în materie de sisteme de management al calității în temeiul dreptului sectorial relevant al Uniunii, aspectele descrise la alineatul (1) pot face parte din sistemele de management al calității stabilite în temeiul legislației respective.

(3) În cazul furnizorilor care sunt instituții financiare supuse unor cerințe privind guvernanța internă, modalitățile sau procesele interne în temeiul legislației Uniunii privind serviciile financiare, se consideră că obligația de instituire a unui sistem de management al calității, cu excepția alineatului (1) literele (g), (h) și (i) este îndeplinită prin respectarea normelor privind mecanismele, sau procesele interne în temeiul legislației relevante privind serviciile financiare. În acest context, se ține seama de toate normele armonizate menționate la articolul 40 din prezentul regulament.

Articolul 18

Păstrarea evidențelor

(1) 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.

(1a) Fiecare stat membru stabilește condițiile în care documentația menționată la alineatul (1) rămâne la dispoziția autorităților naționale competente pentru perioada indicată la alineatul respectiv pentru cazurile în care un furnizor sau reprezentantul autorizat al acestuia, stabilit pe teritoriul său intră în faliment sau își încetează activitatea înainte de sfârșitul perioadei respective.

(2) Furnizorii care sunt instituții financiare supuse unor cerințe privind guvernanța internă, modalitățile sau procesele lor interne în temeiul legislației Uniunii privind serviciile financiare păstrează documentația tehnică ca parte a documentației păstrate în temeiul legislației relevante a Uniunii privind serviciile financiare.

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) [eliminat]

Articolul 20

Fișiere de jurnalizare generate automat

(1) Furnizorii de sisteme de IA cu grad ridicat de risc păstrează fișierele de jurnalizare menționate la articolul 12 alineatul (1), 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. Aceştia le păstrează pentru o perioadă de cel puțin șase luni, cu excepția cazului în care se prevede altfel în dreptul Uniunii sau în dreptul intern aplicabil, în special în dreptul Uniunii privind protecția datelor cu caracter personal.

(2) Furnizorii care sunt instituții financiare supuse unor cerințe privind guvernanța internă, modalitățile sau procesele lor interne în temeiul legislației Uniunii privind serviciile financiare păstrează fișierele de jurnalizare generate automat de sistemele lor de Ia cu grad ridicat de risc ca parte a documentației păstrate în temeiul legislației relevante privind serviciile financiare.

Articolul 21

Măsuri 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 investighează imediat, după caz, cauzele în colaborare cu utilizatorul care a raportat neconformitatea și întreprind imediat acțiunile corective necesare pentru ca sistemul să fie adus în conformitate sau să fie retras sau rechemat, după caz. Aceştia 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 care poate fi înțeleasă cu ușurință de către autoritatea statului membru în cauză. Pe baza unei cereri motivate a unei autorități naționale competente, furnizorii oferă, de asemenea, autorității respective acces la fișierele de jurnalizare menționate la articolul 12 alineatul (1) 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 23a

Condițiile în care alte persoane sunt supuse obligațiilor unui furnizor

(1) Orice persoană fizică sau juridică este considerată a fi un furnizor de sistem de IA cu grad ridicat de risc în sensul prezentului regulament și este supusă obligațiilor care revin furnizorului în temeiul articolului 16, în oricare dintre următoarele situații:

(a) își aplică numele sau marca comercială pe un sistem de IA cu grad ridicat de risc deja introdus pe piață sau pus în funcțiune, fără a aduce atingere acordurilor contractuale care prevăd o repartizare diferită a obligațiilor;

(b) [eliminat]

(c) efectuează o modificare substanțială a unui sistem de IA cu grad ridicat de risc deja introdus pe piață sau pus în funcțiune;

(d) modifică scopul preconizat al unui sistem de IA care nu prezintă un grad ridicat de risc și care este deja introdus pe piață sau pus în funcțiune, în așa fel încât sistemul modificat devine un sistem de IA cu grad ridicat de risc;

(e) introduc pe piață sau pun în funcțiune un sistem de IA de uz general drept sistem de IA cu grad ridicat de risc sau drept componentă a unui sistem de IA cu grad ridicat de risc.

(2) În cazul în care se produc circumstanțele menționate la alineatul (1) litera (a) 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.

(3) În cazul sistemelor de IA cu grad ridicat de risc care sunt componente de siguranță ale produselor cărora li se aplică actele juridice enumerate în anexa II secțiunea A, producătorul produselor respective este considerat furnizorul sistemului de IA cu grad ridicat de risc și este supus obligațiilor menționate la articolul 16 în oricare dintre următoarele situații:

(i) sistemul de IA cu grad ridicat de risc este introdus pe piață împreună cu produsul sub numele sau marca comercială a fabricantului produsului;

(ii) sistemul de IA cu grad ridicat de risc este pus în funcțiune sub numele sau marca comercială a fabricantului produsului după ce produsul a fost introdus pe piață.

Articolul 24

[eliminat]

Articolul 25

Reprezentanți autorizați

(1) Înainte de a-și pune la dispoziție sistemele pe piața Uniunii, 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. În sensul prezentului regulament, mandatul autorizează reprezentantul autorizat să îndeplinească numai următoarele sarcini:

(-a) să verifice dacă declarația de conformitate UE și documentația tehnică au fost întocmite și dacă o procedură de evaluare a conformității adecvată a fost efectuată de furnizor;

(a) să păstreze la dispoziția autorităților naționale competente și a autorităților naționale menționate la articolul 63 alineatul (7), pentru o perioadă de 10 ani de la introducerea pe piață sau punerea în funcțiune a sistemului de IA cu grad ridicat de risc, datele de contact ale furnizorului prin care a fost desemnat reprezentantul autorizat, o copie a declarației de conformitate UE, documentația tehnică și, dacă este cazul, certificatul eliberat de organismul notificat;

(b) să furnizeze unei autorități naționale competente, pe baza unei cereri motivate, toate informațiile și documentele, inclusiv cele păstrate în conformitate cu litera (b), 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 menționate la articolul 12 alineatul (1) 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.

(d) să respecte obligațiile de înregistrare menționate la articolul 51 alineatul (1) și, în cazul în care înregistrarea sistemului este efectuată chiar de către furnizor, să verifice dacă informațiile menționate în anexa VIII partea II punctele 1-11 sunt corecte.

Reprezentantul autorizat reziliază mandatul în cazul în care are motive suficiente să considere că furnizorul acționează contrar obligațiilor care îi revin în temeiul prezentului regulament. Într-un astfel de caz, el informează imediat autoritatea de supraveghere a pieței din statul membru în care este stabilit, precum și, după caz, organismul notificat relevant, cu privire la rezilierea mandatului și la motivele acesteia.

Reprezentantul autorizat este răspunzător din punct de vedere juridic pentru sistemele de IA defecte pe aceeași bază și în solidar cu furnizorul în ceea ce privește răspunderea sa potențială în temeiul Directivei 85/374/CEE a Consiliului.

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 respectivul sistem este conform prezentului regulament, verificând dacă:

(a) procedura relevantă de evaluare a conformității menționată la articolul 43 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 CE necesar și este însoțit de declarația de conformitate UE și de instrucțiunile de utilizare.

(d) reprezentantul autorizat menționat la articolul 25 a fost desemnat de furnizor.

(2) În cazul în care un importator are suficiente motive să considere că un sistem de IA cu grad ridicat de risc nu este în conformitate cu prezentul regulament, sau este falsificat, sau însoțit de o documentație falsificată, 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, reprezentanții autorizați 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.

(4a) Importatorii păstrează, timp de 10 ani de la introducerea pe piață sau punerea în funcțiune a sistemului de IA, o copie a certificatului eliberat de organismul notificat, după caz, a instrucțiunilor de utilizare și a declarației de conformitate UE.

(5) Importatorii furnizează autorităților naționale competente, pe baza unei cereri motivate, toate informațiile necesare și documentația necesară, inclusiv cea păstrată în conformitate cu alineatul (5), 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. În acest scop, statele membre se asigură, de asemenea, că documentația tehnică poate fi pusă la dispoziția autorităților respective.

(5a) Importatorii cooperează cu autoritățile naționale competente cu privire la orice acțiune întreprinsă de respectivele autorități în legătură cu un sistem de IA ai cărui importatori sunt.

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 o copie a declarației de conformitate UE și de instrucțiunile de utilizare și dacă furnizorul și importatorul sistemului, după caz, și-au respectat obligațiile prevăzute la articolul 16 litera (b) și la articolul 26 alineatul (3) din 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 privind activitățile lor, astfel cum se menționează la alineatele (1)-(4).

(5a) Distribuitorii cooperează cu autoritățile naționale competente cu privire la orice acțiune întreprinsă de respectivele autorități în legătură cu un sistem de IA ai cărui distribuitori sunt.

Articolul 28

[eliminat]

Articolul 29

Obligațiile furnizorilor 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 prezentului articol alineatele (2) și (5).

(1a) Utilizatorii încredințează supravegherea umană persoanelor fizice care au competența, formarea și autoritatea necesare.

(2) Obligațiile de la alineatele (1) și (1a) 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 pun în aplicare supravegherea umană și 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 și întrerup utilizarea sistemului de IA. În cazul în care utilizatorul nu poate comunica cu furnizorul, articolul 62 se aplică *mutatis mutandis*. Această obligație nu acoperă datele operaționale sensibile ale utilizatorilor sistemelor de IA care sunt autorități de aplicare a legii.

În cazul utilizatorilor care sunt instituții financiare supuse unor cerințe privind guvernanța internă, măsurile sau procesele interne în temeiul legislației Uniunii privind serviciile financiare, 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 legislației relevante privind serviciile financiare.

(5) Utilizatorii sistemelor de IA cu grad ridicat de risc păstrează fișierele de jurnalizare menționate la articolul 12 alineatul (1), 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. Aceștia le păstrează pentru o perioadă de cel puțin șase luni, cu excepția cazului în care se prevede altfel în dreptul Uniunii sau în dreptul intern aplicabil, în special în dreptul Uniunii privind protecția datelor cu caracter personal.

Utilizatorii care sunt instituții financiare supuse unor cerințe privind guvernanța internă, măsurile sau procesele interne în temeiul legislației Uniunii privind serviciile financiare păstrează fișierele de jurnalizare ca parte a documentației păstrate în temeiul legislației relevante a Uniunii privind serviciile financiare.

(5a) Utilizatorii sistemelor de IA cu grad ridicat de risc care sunt autorități, agenții sau organisme publice, cu excepția autorităților responsabile în materie de aplicare a legii, de control la frontiere, de imigrație sau de azil, respectă obligațiile de înregistrare menționate la articolul 51. În cazul în care constată că sistemul pe care intenționează să îl utilizeze nu a fost înregistrat în baza de date a UE menționată la articolul 60, aceștia nu utilizează sistemul respectiv și informează furnizorul sau distribuitorul.

(6) 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.

(6a) Utilizatorii cooperează cu autoritățile naționale competente cu privire la orice acțiune întreprinsă de respectivele autorități în legătură cu un sistem de IA ai cărui utilizatori sunt.

CAPITOLUL 4

AUTORITĂȚILE DE NOTIFICARE ȘI ORGANISMELE NOTIFICATE

Articolul 30

Autoritățile de notificare

(1) Fiecare stat membru desemnează sau instituie cel puțin 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 decide ca evaluarea și monitorizarea menționate la alineatul (1) să fie efectuate de un organism național de acreditare în sensul Regulamentului (CE) nr. 765/2008 și în conformitate cu acesta.

(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 în conformitate cu articolul 70.

(7) Autoritățile de notificare au la dispoziție un număr adecvat de membri competenți ai personalului în vederea îndeplinirii corespunzătoare a sarcinilor lor.

(8) [eliminat]

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 sistemelor de IA 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 toate 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. Organismul notificat actualizează documentația menționată la alineatele (2) și (3) ori de câte ori au loc modificări relevante, pentru a oferi autorității naționale responsabile de organismele notificate posibilitatea de a monitoriza și de a verifica respectarea continuă a tuturor cerințelor prevăzute la articolul 33.

Articolul 32

Procedura de notificare

(1) Autoritățile de notificare pot notifica numai organismele de evaluare a conformității care îndeplinesc cerințele prevăzute la articolul 33.

(2) Autoritățile de notificare înștiințează Comisia și celelalte state membre cu privire la aceste organisme folosind instrumentul de notificare electronică dezvoltat și administrat de Comisie.

(3) Notificarea menționată la alineatul (2) include detalii complete ale activităților de evaluare a conformității, ale modulului sau modulelor de evaluare a conformității și ale sistemelor de IA în cauză și atestarea relevantă a competenței. În cazul în care notificarea nu se bazează pe un certificat de acreditare menționat la articolul 31 alineatul (2), autoritatea de notificare prezintă Comisiei și celorlalte state membre documentele justificative care atestă competența organismului de evaluare a conformității și măsurile adoptate pentru a se asigura că organismul respectiv va fi monitorizat periodic și că va îndeplini în continuare cerințele prevăzute la articolul 33.

(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 două săptămâni de la o notificare din partea unei autorități de notificare, în cazul în care se include un certificat de acreditare menționat la articolul 31 alineatul (2), sau în termen de două luni de la o notificare din partea unei autorități de notificare, în cazul în care se includ documentele justificative menționate la articolul 31 alineatul (3).

(5) [eliminat]

Articolul 33

Cerințe cu privire la organismele notificate

(1) Un organism notificat este instituit în temeiul legislației naționale și are personalitate juridică.

(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, în conformitate cu articolul 70, 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 pe teritoriul căruia sunt situate, în conformitate cu dreptul intern, sau în care însuși 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. Organismul notificat dispune în permanență de suficient personal administrativ, tehnic, juridic 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) [eliminat]

Articolul 33a

Prezumția de conformitate cu cerințele referitoare la organismele notificate

În cazul în care un organism de evaluare a conformității își demonstrează conformitatea cu criteriile prevăzute în standardele armonizate relevante sau în părți din acestea, ale căror referințe au fost publicate în Jurnalul Oficial al Uniunii Europene, se consideră că acesta este în conformitate cu cerințele prevăzute la articolul 33, în măsura în care standardele armonizate aplicabile vizează aceste cerințe.

Articolul 34

Filiale și subcontractanți ai organismelor 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) Documentele relevante privind evaluarea calificărilor subcontractantului sau ale filialei și activitatea desfășurată de aceștia în temeiul prezentului regulament sunt puse la dispoziția autorității de notificare pentru o perioadă de 5 ani de la data încetării activității de subcontractare.

Articolul 34a

Obligații operaționale ale organismelor 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 își desfășoară activitățile evitând sarcinile inutile pentru furnizori și ținând 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 cu grad ridicat de risc în cauză. Procedând astfel, organismul notificat respectă totuși gradul de precizie și nivelul de protecție necesare pentru conformitatea sistemului de IA cu grad ridicat de risc cu cerințele prezentului regulament.

(3) 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 acestei autorități să își desfășoare activitățile de evaluare, desemnare, notificare și monitorizare și pentru a facilita evaluarea descrisă în prezentul capitol.

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) Autoritatea de notificare înștiințează Comisia și celelalte state membre cu privire la orice modificare relevantă adusă notificării unui organism notificat prin intermediul instrumentului de notificare electronică menționat la articolul 32 alineatul (2).

(2) Procedurile descrise la articolele 31 și 32 se aplică extinderilor domeniului de aplicare al notificării. În ceea ce privește modificările aduse notificării, altele decât extinderile domeniului său de aplicare, se aplică procedurile prevăzute la alineatele de mai jos.

În cazul în care un organism notificat decide să își înceteze activitățile de evaluare a conformității, acesta informează autoritatea de notificare și furnizorii vizați cât mai curând posibil și, în cazul unei încetări planificate, cu un an înainte de încetarea activităților. Certificatele pot rămâne valabile pentru o perioadă temporară de nouă luni de la încetarea activității organismului notificat, cu condiția ca un alt organism notificat să fi confirmat în scris că își va asuma responsabilitățile pentru sistemele de IA reglementate de respectivele certificate. Noul organism notificat efectuează o evaluare completă a sistemelor de IA afectate până la finalul perioadei respective, înainte de emiterea de noi certificate pentru aceste sisteme. În cazul în care organismul notificat și-a încetat activitatea, autoritatea de notificare retrage desemnarea.

(3) În cazul în care o autoritate de notificare are motive suficiente să considere că un organism notificat nu mai îndeplinește cerințele prevăzute la articolul 33 sau că acesta nu își îndeplinește obligațiile, autoritatea de notificare, cu condiția ca organismul notificat să aibă posibilitatea de a-și face cunoscute punctele de vedere, restricționează, suspendă sau retrage notificarea, după caz, în funcție de gravitatea încălcării cerințelor sau a neîndeplinirii obligațiilor. Autoritatea de notificare informează de îndată Comisia și celelalte state membre în consecință.

(4) În cazul în care desemnarea sa a fost suspendată, restricționată sau retrasă integral sau parțial, organismul notificat informează fabricanții în cauză în termen de maximum 10 zile.

(5) În caz de restricționare, suspendare sau retragere a unei notificări, autoritatea de notificare ia măsurile necesare pentru a se asigura că dosarele organismului notificat în cauză sunt păstrate și le pun la dispoziția autorităților de notificare din alte state membre și a autorităților responsabile de supravegherea pieței, la cererea acestora.

(6) În caz de restricționare, suspendare sau retragere a unei desemnări, autoritatea de notificare:

(a) evaluează impactul asupra certificatelor eliberate de organismul notificat;

(b) prezintă Comisiei și celorlalte state membre un raport conținând constatările sale în termen de trei luni de la data la care a notificat modificările la notificare;

(c) solicită organismului notificat să suspende sau să retragă, într-un interval rezonabil de timp stabilit de către autoritate, orice certificat care a fost eliberat în mod necorespunzător pentru a asigura conformitatea sistemelor de IA pe piață;

(d) informează Comisia și statele membre cu privire la certificatele pentru care a solicitat suspendarea sau retragerea;

(e) furnizează autorităților naționale competente din statul membru în care furnizorul își are sediul social toate informațiile relevante cu privire la certificatele pentru care a solicitat suspendarea sau retragerea. Respectiva autoritate competentă ia măsurile corespunzătoare, acolo unde este necesar, pentru evitarea unui risc potențial pentru sănătate, siguranță sau drepturile fundamentale.

(7) Cu excepția certificatelor eliberate în mod necorespunzător și în cazul în care o notificare a fost suspendată sau restricționată, certificatele rămân valabile în următoarele circumstanțe:

(a) autoritatea de notificare a confirmat, în termen de o lună de la suspendare sau restricționare, că nu există niciun risc pentru sănătate, siguranță sau drepturile fundamentale în legătură cu certificatele afectate de suspendare sau de restricționare, și a prezentat un calendar și acțiuni anticipate pentru remedierea suspendării sau a restricționării; sau

(b) autoritatea de notificare a confirmat că, pe durata suspendării sau restricționării nu se va emite, modifica sau emite din nou niciun certificat relevant pentru suspendare și declară dacă organismul notificat are capacitatea de a continua să monitorizeze și să rămână responsabil de certificatele existente pe care le-a emis pe perioada suspendării sau a restricției. În cazul în care autoritatea responsabilă de organismele notificate stabilește că organismul notificat nu are capacitatea de a susține certificatele existente emise, furnizorul furnizează autorităților naționale competente ale statului membru în care furnizorul sistemului reglementat de certificat își are sediul social, în termen de trei luni de la suspendare sau restricționare, o confirmare scrisă a faptului că un alt organism notificat calificat își asumă temporar funcțiile organismului notificat de a monitoriza și de a rămâne responsabil de certificate pe perioada suspendării sau a restricției.

(8) Cu excepția certificatelor eliberate în mod necorespunzător și, în cazul în care desemnarea a fost retrasă, certificatele rămân valabile pe o perioadă de nouă luni în următoarele circumstanțe:

(a) în cazul în care autoritatea națională competentă din statul membru în care furnizorul sistemului de IA reglementat de certificat își are sediul social a confirmat că nu există niciun risc pentru sănătate, siguranță și drepturile fundamentale asociat sistemelor în cauză; și

(b) un alt organism notificat a confirmat în scris că își va asuma responsabilitățile imediate pentru respectivele sisteme și va fi încheiat evaluarea acestora în termen de 12 luni de la retragerea desemnării.

În condițiile menționate la primul paragraf, autoritatea națională competentă din statul membru în care își are sediul social furnizorul sistemului reglementat de certificat poate prelungi valabilitatea provizorie a certificatelor cu perioade suplimentare de trei luni, care în total nu depășesc 12 luni.

Autoritatea națională competentă sau organismul notificat care își asumă funcțiile organismului notificat afectat de modificarea notificării informează imediat Comisia, celelalte state membre și celelalte organisme notificate în acest sens.

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 în conformitate cu articolul 70.

(4) În cazul în care Comisia constată că un organism notificat nu îndeplinește sau nu mai îndeplinește cerințele prevăzute la articolul 33, Comisia informează autoritatea de notificare cu privire la motivele unei astfel de constatări și îi solicită acesteia să ia măsurile corective necesare, inclusiv suspendarea, restricționarea sau retragerea desemnării, dacă este necesar. În cazul în care autoritatea de notificare nu ia măsurile corective necesare, Comisia poate, prin intermediul unor acte de punere în aplicare, să suspende, să restricționeze sau să retragă notificarea. 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 sistemele de IA cu grad ridicat de risc, 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 în temeiul prezentului regulament, sub forma unui grup sectorial al organismelor notificate.

(2) Autoritatea de notificare se asigură că organismele notificate de aceasta 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, cu condiția ca aceste organisme să îndeplinească cerințele prevăzute la articolul 33.

CAPITOLUL 5

STANDARDE, EVALUAREA CONFORMITĂȚII, CERTIFICATE, ÎNREGISTRARE

Articolul 40

Standarde armonizate

(1) Sistemele de IA cu grad ridicat de risc sau sistemele de IA de uz general care sunt în conformitate cu standardele 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 sau, după caz, cu cerințele stabilite în articolul 4a și în articolul 4b, în măsura în care standardele respective acoperă cerințele respective.

(2) Atunci când adresează o cerere de standardizare organizațiilor europene de standardizare în conformitate cu articolul 10 din Regulamentul nr. 1025/2012, Comisia precizează că standardele trebuie să fie coerente, clare și elaborate astfel încât să urmărească îndeplinirea în special a următoarelor obiective:

(a) să asigure faptul că sistemele de IA introduse pe piață sau puse în funcțiune în Uniune sunt sigure și respectă valorile Uniunii și consolidează autonomia strategică deschisă a Uniunii;

(b) să promoveze investițiile și inovarea în domeniul IA, inclusiv prin sporirea securității juridice, precum și competitivitatea și creșterea pieței Uniunii;

(c) să consolideze guvernanța multipartită, astfel încât toate părțile interesate europene relevante (de exemplu, industrie, IMM-uri, societatea civilă, cercetători) să fie reprezentate;

(d) să contribuie la consolidarea cooperării globale în materie de standardizare în domeniul IA care să respecte valorile și interesele Uniunii.

Comisia solicită organizațiilor europene de standardizare să furnizeze dovezi ale tuturor eforturilor pe care le-au depus pentru a îndeplini obiectivele de mai sus.

Articolul 41

Specificații comune

(1) Comisia este împuternicită să adopte, după consultarea Comitetului pentru IA menționat la articolul 56, acte de punere în aplicare în conformitate cu procedura de examinare menționată la articolul 74 alineatul (2), de stabilire a specificațiilor tehnice comune pentru cerințele prevăzute în capitolul 2 din prezentul titlu sau, după caz, în conformitate cu cerințele prevăzute la articolul 4a și la articolul 4b, în cazul în care sunt îndeplinite următoarele condiții:

(a) nu a fost publicată în *Jurnalul Oficial al Uniunii Europene* nicio trimitere la standardele armonizate care acoperă preocupările esențiale relevante privind siguranța sau drepturile fundamentale, în conformitate cu Regulamentul (UE) nr. 1025/2012;

(b) Comisia a solicitat, în temeiul articolului 10 alineatul (1) din Regulamentul 1025/2012, uneia sau mai multor organizații de standardizare europene să elaboreze un standard armonizat pentru cerințele prevăzute în capitolul 2 din prezentul titlu;

(c) cererea menționată la litera (b) nu a fost acceptată de niciuna dintre organizațiile de standardizare europene sau standardele armonizate care răspund cererii respective nu sunt prezentate în termenul stabilit în conformitate cu articolul 10 alineatul (1) din Regulamentul 1025/2012 sau standardele respective nu sunt conforme cu cererea.

(1a) Înainte de a pregăti un proiect de act de punere în aplicare, Comisia informează comitetul menționat la articolul 22 din Regulamentul (UE) nr. 1025/2012 că, în opinia sa, condițiile de la alineatul (1) sunt îndeplinite.

(2) În pregătirea timpurie a proiectului de act de punere în aplicare de stabilire a specificației comune, Comisia îndeplinește obiectivele menționate la articolul 40 alineatul (2) și colectează opiniile organismelor sau ale grupurilor de experți relevante instituite în temeiul legislației sectoriale relevante a Uniunii. Pe baza acestei consultări, Comisia pregătește proiectul de act de punere în aplicare.

(3) Sistemele de IA cu grad ridicat de risc sau sistemele de IA de uz general 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 sau, după caz, cu cerințele stabilite la articolul 4a și la articolul 4b, în măsura în care acele specificații comune acoperă cerințele respective.

(4) Atunci când referințele unui standard armonizat sunt publicate în *Jurnalul Oficial al Uniunii Europene*, actele de punere în aplicare menționate la alineatul (1), care vizează cerințele prevăzute în capitolul 2 din prezentul titlu sau cerințele prevăzute la articolul 4a și la articolul 4b, se abrogă, după caz.

(5) În cazul în care un stat membru consideră că o specificație comună nu îndeplinește în totalitate cerințele prevăzute în capitolul 2 din prezentul titlu sau cerințele prevăzute la articolul 4a și la articolul 4b, după caz, acesta informează Comisia în acest sens, furnizând o explicație detaliată, iar Comisia evaluează informațiile respective și, dacă este cazul, modifică actul de punere în aplicare prin care se stabilește specificația comună în cauză.

Articolul 42

Prezumția de conformitate cu anumite cerințe

(1) Sistemele de IA cu grad ridicat de risc care au fost antrenate și testate pe baza datelor care reflectă mediul geografic, comportamental sau funcțional specific în care sunt destinate să fie utilizate sunt considerate a fi în conformitate cu cerințele respective prevăzute la articolul 10 alineatul (4).

(2) Sistemele de IA cu grad ridicat de risc sau sistemele de IA de uz general 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[33] 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 optează pentru una dintre următoarele proceduri:

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

(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.

[33] 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).

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 responsabile în materie de aplicare a legii, de imigrație sau de azil, 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.

(2) În cazul sistemelor de IA cu grad ridicat de risc menționate la punctele 2-8 din anexa III și al sistemelor de IA de uz general menționate în titlul 1a, 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.

(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) [eliminat]

(5) Comisia este împuternicită să adopte acte delegate în conformitate cu articolul 73 în scopul actualizării anexelor VI și VII 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 care poate fi ușor înțeleasă de autoritățile competente din statul membru în care este stabilit 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. Orice supliment la un certificat rămâne valabil atât timp cât este valabil certificatul pe care îl completează.

(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

Este pusă 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 sisteme de IA informații relevante privind aspecte legate de rezultatele negative ale evaluărilor conformității și, la cerere, de rezultatele pozitive ale evaluărilor conformității.

(4) Obligațiile menționate la alineatele (1)-(3) sunt îndeplinite în conformitate cu articolul 70.

Articolul 47

Derogare de la procedura de evaluare a conformității

(1) Prin derogare de la articolul 43 și pe baza unei cereri justificate în mod corespunzător, 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, ținând seama de motivele excepționale care justifică derogarea. Finalizarea procedurilor respective se efectuează fără întârzieri nejustificate.

(1a) Într-o situație de urgență justificată în mod corespunzător din motive excepționale de securitate publică sau în cazul unei amenințări specifice, substanțiale și iminente la adresa vieții sau a siguranței fizice a persoanelor fizice, autoritățile de aplicare a legii sau autoritățile de protecție civilă pot pune în funcțiune un anumit sistem de IA cu grad ridicat de risc fără autorizația menționată la alineatul (1), cu condiția ca o astfel de autorizație să fie solicitată în timpul utilizării sau după aceasta, fără întârzieri nejustificate, iar în cazul în care această autorizație este refuzată, utilizarea sistemului respectiv este oprită imediat și toate realizările și rezultatele acestei utilizări sunt eliminate imediat.

(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). Această obligație nu acoperă datele operaționale sensibile legate de activitățile autorităților de aplicare a legii.

(3) [eliminat]

(4) [eliminat]

(5) [eliminat]

(6) Pentru sistemele de IA cu grad ridicat de risc legate de produsele care fac obiectul legislației de armonizare a Uniunii menționate în anexa II secțiunea A, se aplică numai procedurile de derogare de la evaluarea conformității stabilite în legislația respectivă.

Articolul 48

Declarația de conformitate UE

(1) Furnizorul întocmește o declarație de conformitate UE scrisă sau semnată electronic 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 transmisă 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 care poate fi ușor înțeleasă de autoritățile naționale competente din 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 de conformitate face obiectul principiilor generale prevăzute la articolul 30 din Regulamentul (CE) nr. 765/2008.

(2) 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.

(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

[eliminat]

Articolul 51

Înregistrarea operatorilor relevanți și a sistemelor de IA cu grad ridicat de risc enumerate în anexa III

(1) Înainte de a introduce pe piață sau de a pune în funcțiune un sistem de IA cu grad ridicat de risc enumerat în anexa III, cu excepția sistemelor de IA cu grad ridicat de risc menționate la punctele 1, 6 și 7 din anexa III din domeniul asigurării respectării legii, al migrației, al azilului și al gestionării controlului frontierelor și a sistemelor de IA cu grad ridicat de risc menționate în anexa III punctul 2, furnizorul și, după caz, reprezentantul autorizat se înregistrează în baza de date a UE menționată la articolul 60. Furnizorul sau, după caz, reprezentantul autorizat, își înregistrează, de asemenea, sistemele în baza de date respectivă.

(2) Înainte de a utiliza un sistem de IA cu grad ridicat de risc enumerat în anexa III, utilizatorii sistemelor de IA cu grad ridicat de risc care sunt autorități, agenții sau organisme publice sau entitățile care acționează în numele lor se înregistrează în baza de date a UE menționată la articolul 60 și selectează sistemul pe care intenționează să îl utilizeze.

Obligațiile prevăzute la alineatul anterior nu se aplică autorităților, agențiilor sau organismelor responsabile în materie de aplicare a legii, de control la frontiere, de imigrație sau de azil, agențiilor sau organismelor și autorităților, agențiilor sau organismelor care utilizează sisteme de IA cu grad ridicat de risc menționate la punctul 2 din anexa III, precum și entităților care acționează în numele acestora.

TITLUL IV

OBLIGAȚII DE TRANSPARENȚĂ PENTRU FURNIZORII ȘI UTILIZATORII ANUMITOR SISTEME DE IA

Articolul 52

Obligații de transparență pentru furnizorii și utilizatorii anumitor 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 punctul de vedere al unei persoane fizice normal informate, suficient de atente și de avizate, ținând seama de 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, sub rezerva unor garanții adecvate pentru drepturile și libertățile terților, cu excepția cazului în care aceste sisteme sunt disponibile publicului pentru a denunța o infracțiune.

(2) Utilizatorii 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, sub rezerva unor garanții adecvate pentru drepturile și libertățile terților.

(2a) Utilizatorii unui sistem de recunoaștere a emoțiilor informează persoanele fizice expuse la sistem cu privire la funcționarea acestuia. Această obligație nu se aplică sistemelor de IA utilizate pentru recunoașterea emoțiilor, care sunt autorizate prin lege să detecteze, să prevină și să investigheze infracțiunile, sub rezerva unor garanții adecvate pentru drepturile și libertățile terților.

(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 în cazul în care conținutul face parte dintr-o activitate sau un program în mod evident creativ, satiric, artistic sau fictiv, sub rezerva unor garanții adecvate pentru drepturile și libertățile terților.

(3a) Informațiile menționate la alineatele (1)-(3) sunt furnizate persoanelor fizice într-un mod clar și distinct, cel târziu în momentul primei interacțiuni sau al primei expuneri.

(4) Alineatele (1), (2), (2a), (3) și (3a) nu aduc atingere cerințelor și obligațiilor prevăzute în titlul III din prezentul regulament și nu aduc atingere altor obligații de transparență pentru utilizatorii sistemelor de IA prevăzute în dreptul Uniunii sau în dreptul intern.

TITLUL V

MĂSURI DE SPRIJINIRE A INOVĂRII

Articolul 53

Spațiile de testare în materie de reglementare a IA

(-1a) Autoritățile naționale competente pot institui spații de testare în materie de reglementare a IA pentru dezvoltarea, antrenarea, testarea și validarea sistemelor de IA inovatoare, sub supravegherea, îndrumarea și sprijinul direct al autorității naționale competente, înainte ca aceste sisteme să fie introduse pe piață sau puse în funcțiune. Astfel de spații de testare în materie de reglementare pot include testarea în condiții reale supravegheată de autoritățile naționale competente.

(-1b) [eliminat]

(-1c) După caz, autoritățile naționale competente cooperează cu alte autorități relevante și pot permite implicarea altor actori din ecosistemul de IA.

(-1d) Prezentul articol nu aduce atingere altor spații de testare în materie de reglementare instituite în temeiul dreptului intern sau al dreptului Uniunii, inclusiv în cazurile în care produsele sau serviciile care sunt testate în cadrul acestora sunt legate de utilizarea sistemelor de IA inovatoare. Statele membre asigură un nivel adecvat de cooperare între autoritățile care supraveghează aceste alte spații de testare și autoritățile naționale competente.

(1) [eliminat]

(1a) [eliminat]

(1b) Instituirea spațiilor de testare în materie de reglementare a IA în temeiul prezentului regulament urmărește să contribuie la unul sau mai multe dintre următoarele obiective:

a) stimularea inovării și a competitivității și facilitarea dezvoltării unui ecosistem de IA;
b) facilitarea și accelerarea accesului la piața Uniunii pentru sistemele de IA, în special atunci când sunt furnizate de întreprinderi mici și mijlocii (IMM-uri), inclusiv de întreprinderi nou-înființate;
c) îmbunătățirea securității juridice și contribuția la schimbul de bune practici prin cooperarea cu autoritățile implicate în spațiul de testare în materie de reglementare a IA, cu scopul de a asigura conformitatea viitoare cu prezentul regulament și, după caz, cu alte acte legislative ale Uniunii și ale statelor membre;
d) contribuția la învățarea bazată pe dovezi în materie de reglementare.

(2) [eliminat]

(2a) Accesul la spațiile de testare în materie de reglementare a IA este deschis oricărui furnizor sau potențial furnizor al unui sistem de IA care îndeplinește criteriile de eligibilitate și de selecție menționate la alineatul (6) litera (a) și care a fost selectat de autoritățile naționale competente în urma procedurii de selecție menționate la alineatul (6) litera (b). Furnizorii sau potențialii furnizori pot, de asemenea, depune cereri în parteneriat cu utilizatorii sau cu orice alte părți terțe relevante.

Participarea la spațiul de testare în materie de reglementare a IA este limitată la o perioadă adecvată complexității și amplorii proiectului. Această perioadă poate fi prelungită de autoritatea națională competentă.

Participarea la spațiul de testare în materie de reglementare a IA se bazează pe un plan specific menționat la alineatul (6) din prezentul articol, care este convenit între participant (participanți) și autoritatea (autoritățile) națională (naționale) competentă (competente), după caz.

(3) Participarea la spațiile de testare în materie de reglementare a IA nu afectează competențele de supraveghere și atribuțiile corective ale autorităților care supraveghează spațiul de testare. Autoritățile respective își exercită competențele de supraveghere într-un mod flexibil, în limitele legislației relevante, utilizând competențele lor discreționare atunci când pun în aplicare dispoziții juridice pentru un anumit proiect de spațiu de testare în materie de IA, cu obiectivul de a sprijini inovarea în domeniul IA în Uniune.

Cu condiția ca participantul (participanții) să respecte planul privind spațiul de testare și termenii și condițiile de participare menționate la alineatul (6) litera (c) și să urmeze cu bună-credință orientările oferite de autorități, autoritățile nu impun amenzi administrative pentru încălcarea legislației aplicabile a Uniunii sau a statului membru referitoare la sistemul de IA supravegheat în spațiul de testare, inclusiv a dispozițiilor prezentului regulament.

(4) Participanții rămân responsabili, în temeiul legislației aplicabile a Uniunii și a statelor membre în materie de răspundere, pentru orice prejudiciu cauzat în cursul participării lor la un spațiu de testare în materie de reglementare a IA.

(4a) La cererea furnizorului sau a potențialului furnizor al sistemului de IA, autoritatea națională competentă furnizează, după caz, o dovadă scrisă a activităților desfășurate cu succes în spațiul de testare. Autoritatea națională competentă furnizează, de asemenea, un raport de ieșire care detaliază activitățile desfășurate în spațiul de testare, precum și realizările și rezultatele învățării aferente. Astfel de dovezi scrise și rapoarte de ieșire ar putea fi luate în considerare de autoritățile de supraveghere a pieței sau de organismele notificate, după caz, în contextul procedurilor de evaluare a conformității sau al controalelor de supraveghere a pieței.

Sub rezerva dispozițiilor privind confidențialitatea de la articolul 70 și cu acordul participanților la spațiul de testare, Comisia Europeană și Comitetul pentru IA sunt autorizate să acceseze rapoartele de ieșire și le iau în considerare, după caz, atunci când își exercită atribuțiile în temeiul prezentului regulament. Dacă atât participantul, cât și autoritatea națională competentă sunt de acord în mod explicit cu acest lucru, raportul de ieșire poate fi pus la dispoziția publicului prin intermediul platformei unice de informare menționate la articolul 55 alineatul (3) litera (b).

(4b) Spațiile de testare în materie de reglementare a IA sunt concepute și puse în aplicare astfel încât, după caz, să faciliteze cooperarea transfrontalieră între autoritățile naționale competente.

(5) Autoritățile naționale competente pun la dispoziția publicului rapoarte anuale cu privire la punerea în aplicare a spațiilor de testare în materie de reglementare a IA, 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. Rapoartele anuale respective sunt prezentate Comitetului pentru IA, care pune la dispoziția publicului un rezumat al tuturor bunelor practici, lecțiilor învățate și recomandărilor. Această obligație de a face publice rapoartele anuale nu acoperă datele operaționale sensibile legate de activitățile autorităților responsabile în materie de aplicare a legii, de control la frontiere, de imigrație sau de azil. Comisia și Comitetul pentru IA țin seama, după caz, de rapoartele anuale atunci când își exercită atribuțiile în temeiul prezentului regulament.

(5b) Comisia se asigură că informațiile privind spațiile de testare în materie de reglementare a IA, inclusiv cele instituite în temeiul prezentului articol, sunt disponibile prin intermediul platformei unice de informare menționate la articolul 55 alineatul (3) litera (b).

(6) Modalitățile și condițiile de instituire și funcționare a spațiilor de testare în materie de reglementare a IA în temeiul prezentului regulament se adoptă prin acte de punere în aplicare în conformitate cu procedura de examinare menționată la articolul 74 alineatul (2).

Modalitățile și condițiile sprijină, în cea mai mare măsură posibilă, flexibilitatea pentru ca autoritățile naționale competente să instituie și să opereze spațiile lor de testare în materie de reglementare a IA, promovează inovarea și învățarea în materie de reglementare și țin seama în special de circumstanțele și capacitățile speciale ale IMM-urilor participante, inclusiv ale întreprinderilor nou-înființate.

Respectivele acte de punere în aplicare includ principii de bază comune cu privire la următoarele aspecte:

a) eligibilitatea și selecția pentru participarea la spațiul de testare în materie de reglementare a IA;
b) procedura de depunere a cererii, participare, monitorizare, ieșire și încetare a spațiului de testare în materie de reglementare a IA, inclusiv planul privind spațiul de testare și raportul de ieșire;
c) termenii și condițiile aplicabile participanților.

(7) Atunci când autoritățile naționale competente iau în considerare autorizarea testării în condiții reale supravegheate în cadrul unui spațiu de testare în materie de reglementare a IA instituit în temeiul prezentului articol, acestea convin în mod specific cu participanții asupra termenilor și condițiilor unei astfel de testări și, în special, asupra garanțiilor adecvate în vederea protejării drepturilor fundamentale, a sănătății și a siguranței. După caz, acestea cooperează cu alte autorități naționale competente în vederea asigurării unor practici coerente în întreaga Uniune.

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 pot fi prelucrate în scopul dezvoltării, testării și antrenării anumitor sisteme de IA inovatoare în spațiul de testare, în următoarele condiții cumulative:

(a) sistemele de IA inovatoare sunt dezvoltate pentru a proteja un interes public substanțial de către o autoritate publică sau de către o altă persoană fizică sau juridică de drept public sau de drept privat și în unul sau mai multe dintre următoarele domenii:

(i) [eliminat]

(ii) siguranța și sănătatea publică, inclusiv prevenirea, controlul și tratarea bolilor și îmbunătățirea sistemelor de sănătate;

(iii) protejarea și îmbunătățirea calității mediului, inclusiv tranziția verde, atenuarea schimbărilor climatice și adaptarea la acestea;

(iv) durabilitatea energetică, transporturile și mobilitatea;

(v) eficiența și calitatea administrației publice și a serviciilor publice;

(vi) securitatea cibernetică și reziliența infrastructurii critice.

(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 și libertăților persoanelor vizate în timpul experimentării în spațiul de testare, astfel cum se menționează la articolul 35 din Regulamentul (UE) 2016/679 și la articolul 39 din Regulamentul (UE) 2018/1725, 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 trebuie transmise, transferate sau accesate în alt mod de către alte părți care nu sunt participante la spațiul de testare, cu excepția cazului în care o astfel de divulgare are loc în conformitate cu Regulamentul (UE) 2016/679 sau, după caz, cu Regulamentul (UE) 2018/1725 și toți participanții au fost de acord cu acest lucru;

(f) nicio prelucrare a datelor cu caracter personal în contextul spațiului de testare nu aduce atingere aplicării drepturilor persoanelor vizate, astfel cum se prevede în dreptul Uniunii privind protecția datelor cu caracter personal, în special la articolul 22 din Regulamentul (UE) 2016/679 și la articolul 24 din Regulamentul (UE) 2018/1725;

(g) toate datele cu caracter personal prelucrate în contextul spațiului de testare sunt protejate prin măsuri tehnice și organizaționale adecvate și 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, în afara cazului în care există dispoziții diferite în dreptul Uniunii sau în dreptul intern;

(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, sunt publicate pe site-ul web al autorităților competente. Această obligație nu acoperă datele operaționale sensibile legate de activitățile autorităților responsabile în materie de aplicare a legii, de control la frontiere, de imigrație sau de azil.

(1a) 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, sub controlul și responsabilitatea autorităților de aplicare a legii, prelucrarea datelor cu caracter personal în spațiile de testare în materie de reglementare a IA se bazează pe o legislație specifică a statelor membre sau a Uniunii și face obiectul acelorași condiții cumulative ca cele menționate la alineatul (1).

(2) Alineatul (1) nu aduce atingere legislației Uniunii sau a statelor membre care stabilește baza pentru prelucrarea datelor cu caracter personal care este necesară în scopul dezvoltării, testării și antrenării sistemelor de IA inovatoare sau oricărui alt temei juridic, în conformitate cu dreptul Uniunii privind protecția datelor cu caracter personal.

Articolul 54a

Testarea sistemelor de IA cu grad ridicat de risc în condiții reale în afara spațiilor de testare în materie de reglementare a IA

(1) Testarea sistemelor de IA în condiții reale în afara spațiilor de testare în materie de reglementare a IA poate fi efectuată de către furnizorii sau potențialii furnizori de sisteme de IA cu grad ridicat de risc enumerați în anexa III, în conformitate cu dispozițiile prezentului articol și cu planul de testare în condiții reale menționat la prezentul articol.

Elementele detaliate ale planului de testare în condiții reale sunt specificate în actele de punere în aplicare adoptate de Comisie în conformitate cu procedura de examinare menționată la articolul 74 alineatul (2).

Această dispoziție nu aduce atingere legislației Uniunii sau a statelor membre privind testarea în condiții reale a sistemelor de IA cu grad ridicat de risc legate de produsele care fac obiectul legislației enumerate în anexa II.

(2) Furnizorii sau potențialii furnizori pot efectua teste ale sistemelor de IA cu grad ridicat de risc menționate în anexa III în condiții reale în orice moment înainte de introducerea pe piață sau de punerea în funcțiune a sistemului de IA pe cont propriu sau în parteneriat cu unul sau mai mulți utilizatori potențiali.

(3) Testarea sistemelor de IA cu grad ridicat de risc în condiții reale în temeiul prezentului articol nu aduce atingere evaluării etice care poate fi impusă de dreptul național sau de dreptul Uniunii.

(4) Furnizorii sau potențialii furnizori pot efectua testarea în condiții reale numai dacă sunt îndeplinite toate condițiile următoare:

(a) furnizorul sau potențialul furnizor a elaborat un plan de testare în condiții reale și l-a prezentat autorității de supraveghere a pieței din statul membru (statele) membru (membre) în care urmează să se efectueze testarea în condiții reale;

(b) autoritatea de supraveghere a pieței din statul (statele) membru (membre) în care urmează să fie efectuată testarea în condiții reale nu a formulat obiecții cu privire la testare în termen de 30 de zile de la transmiterea acesteia;

(c) furnizorul sau potențialul furnizor, cu excepția sistemelor de IA cu grad ridicat de risc menționate la punctele 1, 6 și 7 din anexa III în domeniul asigurării respectării legii, al migrației, al azilului și al gestionării controlului frontierelor și a sistemelor de IA cu grad ridicat de risc menționate la punctul 2 din anexa III, a înregistrat testarea în condiții reale în baza de date a UE menționată la articolul 60 alineatul (5a) cu un număr unic de identificare la nivelul întregii Uniuni și informațiile specificate în anexa VIIIa;

(d) furnizorul sau potențialul furnizor care efectuează testarea în condiții reale este stabilit în Uniune sau a desemnat un reprezentant legal în scopul testării în condiții reale care este stabilit în Uniune;

(e) datele colectate și prelucrate în scopul testării în condiții reale nu se transferă către țări din afara Uniunii, cu excepția cazului în care transferul și prelucrarea oferă garanții echivalente cu cele prevăzute de dreptul Uniunii;

(f) testarea în condiții reale nu durează mai mult decât este necesar pentru atingerea obiectivelor sale și, în orice caz, nu depășește 12 luni;

(g) persoanele care aparțin unor grupuri vulnerabile din cauza vârstei, a dizabilității fizice sau mintale sunt protejate în mod corespunzător;

(h) [eliminat]

(i) în cazul în care un furnizor sau un potențial furnizor organizează testarea în condiții reale în cooperare cu unul sau mai mulți utilizatori potențiali, aceştia din urmă au fost informați cu privire la toate aspectele testării care sunt relevante pentru decizia lor de a participa și au primit instrucțiunile relevante privind modul de utilizare a sistemului de IA menționat la articolul 13; furnizorul sau potențialul furnizor și utilizatorul (utilizatorii) încheie un acord în care precizează rolurile și responsabilitățile lor, în vederea asigurării conformității cu dispozițiile privind testarea în condiții reale în temeiul prezentului regulament și al altor acte legislative aplicabile ale Uniunii și ale statelor membre;

(j) subiecții testării în condiții reale și-au dat consimțământul în cunoștință de cauză în conformitate cu articolul 54b sau, în cazul autorităților de aplicare a legii, în cazul în care solicitarea consimțământului în cunoștință de cauză ar împiedica testarea sistemului de IA, testarea în sine și rezultatul testării în condițiile reale nu au un efect negativ asupra subiectului;

(k) testarea în condiții reale este supravegheată efectiv de furnizor sau de potențialul furnizor și de utilizator (utilizatori) prin intermediul unor persoane care sunt calificate corespunzător în domeniul relevant și care au capacitatea, formarea și autoritatea necesare pentru a-și îndeplini sarcinile;

(l) previziunile, recomandările sau deciziile sistemului de IA pot fi efectiv inversate sau ignorate.

(5) Orice subiect al testării în condiții reale sau reprezentantul său desemnat legal, după caz, se poate retrage din testare în orice moment, fără vreun prejudiciu și fără a trebui să prezinte vreo justificare, prin revocarea consimțământului său în cunoștință de cauză. Retragerea consimțământului în cunoștință de cauză nu afectează activitățile deja desfășurate și utilizarea datelor obținute pe baza consimțământului în cunoștință de cauză înainte de retragerea acestuia.

(6) Orice incident grav identificat în cursul testării în condiții reale se raportează autorității naționale de supraveghere a pieței în conformitate cu articolul 62 din prezentul regulament. Furnizorul sau potențialul furnizor adoptă măsuri imediate de atenuare sau, în caz contrar, suspendă testarea în condiții reale până când are loc o astfel de atenuare sau îi pune capăt în alt mod. Furnizorul sau potențialul furnizor instituie o procedură pentru rechemarea promptă a sistemului de IA în cazul unei astfel de încetări a testării în condiții reale.

(7) Furnizorii sau potențialii furnizori informează autoritatea națională de supraveghere a pieței din statul (statele) membru (membre) în care urmează să se efectueze testarea în condiții reale cu privire la suspendarea sau încetarea testării în condiții reale și cu privire la rezultatele finale.

(8) Furnizorul sau potențialul furnizor este responsabil, în temeiul legislației aplicabile a Uniunii și a statelor membre în materie de răspundere, pentru orice prejudiciu cauzat în cursul participării lor la testarea în condiții reale.

Articolul 54b

Consimțământul în cunoștință de cauză la participarea la testarea în condiții reale în afara spațiilor de testare în materie de reglementare a IA

(1) În scopul testării în condiții reale în conformitate cu articolul 54a, consimțământul în cunoștință de cauză este acordat în mod liber de către subiectul testării înainte de participarea sa la o astfel de testare și după ce a fost informat în mod corespunzător cu informații concise, clare, relevante și inteligibile cu privire la:

(i) natura și obiectivele testării în condiții reale și posibilele inconveniente care ar putea fi legate de participarea sa;

(ii) condițiile în care se desfășoară testarea în condiții reale, inclusiv durata preconizată a participării subiectului;

(iii) drepturile și garanțiile subiectului cu privire la participarea sa, în special dreptul său de a refuza să participe la testarea în condiții reale și dreptul de a se retrage din aceasta în orice moment, fără angajarea vreunui prejudiciu și fără a fi nevoit să prezinte vreo justificare;

(iv) modalitățile de solicitare a inversării sau a ignorării previziunilor, recomandărilor sau deciziilor sistemului de IA;

(v) numărul unic de identificare la nivelul întregii Uniuni al testării în condiții reale în conformitate cu articolul 54a alineatul (4c) și datele de contact ale furnizorului sau ale reprezentantului său legal de la care se pot obține informații suplimentare.

(2) Consimțământul în cunoștință de cauză este datat și documentat, iar o copie se înmânează subiectului sau reprezentantului său legal.

Articolul 55

Măsuri de sprijinire pentru operatori, în special IMM-uri, inclusiv întreprinderi nou-înființate

(1) Statele membre întreprind următoarele acțiuni:

(a) oferă IMM-urilor, inclusiv întreprinderilor nou-înființate, acces prioritar la spațiile de testare în materie de reglementare a IA, în măsura în care îndeplinesc criteriile de eligibilitate și de selecție;

(b) organizează activități specifice de sensibilizare și formare cu privire la aplicarea prezentului regulament, adaptate la nevoile IMM-urilor, inclusiv ale întreprinderilor nou-înființate și, după caz, ale autorităților publice locale;

(c) după caz, stabilesc un canal specific de comunicare cu IMM-urile, inclusiv cu întreprinderile nou-înființate și, după caz, cu autoritățile publice locale pentru a oferi consiliere și a răspunde la întrebări cu privire la aplicarea prezentului regulament, inclusiv în ceea ce privește participarea la spațiile de testare în materie de reglementare a IA.

(2) Interesele și nevoile specifice ale IMM-urilor furnizoare, inclusiv ale întreprinderilor nou-înființate, sunt luate în considerare la stabilirea taxelor pentru evaluarea conformității în temeiul articolului 43, taxele respective fiind reduse proporțional cu dimensiunea lor, cu dimensiunea pieței și cu alți indicatori relevanți.

(3) Comisia întreprinde următoarele acțiuni:

(a) la cererea Comitetului pentru IA, furnizează modele standardizate pentru domeniile vizate de prezentul regulament;

(b) dezvoltă și menține o platformă unică de informații care să ofere informații ușor de utilizat în legătură cu prezentul regulament pentru toți operatorii din întreaga Uniune;

(c) organizează campanii de comunicare adecvate pentru a sensibiliza publicul cu privire la obligațiile care decurg din prezentul regulament;

(d) evaluează și promovează convergența celor mai bune practici în procedurile de achiziții publice în ceea ce privește sistemele de IA.

Articolul 55a

Derogări pentru operatori specifici

(1) Obligațiile prevăzute la articolul 17 din prezentul regulament nu se aplică microîntreprinderilor, astfel cum sunt definite la articolul 2 alineatul (3) din anexa la Recomandarea 2003/361/CE a Comisiei privind definiția microîntreprinderilor și a întreprinderilor mici și mijlocii, cu condiția ca aceste întreprinderi să nu aibă întreprinderi partenere sau întreprinderi afiliate, astfel cum sunt definite la articolul 3 din aceeași anexă.

(2) Alineatul (1) nu se interpretează ca o exceptare a operatorilor respectivi de la îndeplinirea oricăror alte cerințe și obligații prevăzute în prezentul regulament, inclusiv cele stabilite la articolele 9, 61 și 62.

(3) Cerințele și obligațiile pentru sistemele de IA de uz general prevăzute la articolul 4b nu se aplică microîntreprinderilor și întreprinderilor mici și mijlocii, cu condiția ca aceste întreprinderi să nu aibă întreprinderi partenere sau întreprinderi afiliate, astfel cum sunt definite la articolul 3 din anexa la Recomandarea 2003/361/CE a Comisiei privind definiția microîntreprinderilor și a întreprinderilor mici și mijlocii.

TITLUL VI

GUVERNANȚA

CAPITOLUL 1

COMITETUL EUROPEAN PENTRU INTELIGENȚA ARTIFICIALĂ

Articolul 56

Instituirea și structura Comitetului european pentru inteligența artificială

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

(2) Comitetul este alcătuit dintr-un reprezentant pentru fiecare stat membru. Autoritatea Europeană pentru Protecția Datelor participă ca observator. Comisia participă, de asemenea, la reuniunile comitetului fără a lua parte la vot.

De la caz la caz, comitetul poate invita la reuniuni și alte autorități, organisme sau experți de la nivel național și de la nivelul Uniunii, în cazul în care chestiunile discutate le privesc.

(2a) Fiecare reprezentant este desemnat de statul său membru pentru o perioadă de trei ani, care poate fi reînnoită o singură dată.

(2aa) Statele membre se asigură că reprezentanții lor în comitet:

(i) dețin competențele și prerogativele relevante în statul lor membru, astfel încât să contribuie în mod activ la îndeplinirea sarcinilor comitetului menționate la articolul 58;

(ii) sunt desemnați ca punct unic de contact pentru comitet și, după caz, ținând seama de nevoile statelor membre, ca punct unic de contact pentru părțile interesate;

(iii) sunt împuterniciți să faciliteze coerența și coordonarea între autoritățile naționale competente din statul lor membru în ceea ce privește punerea în aplicare a prezentului regulament, inclusiv prin colectarea de date și informații relevante în scopul îndeplinirii sarcinilor care le revin în cadrul comitetului.

(3) Reprezentanții desemnați ai statelor membre adoptă regulamentul de procedură al comitetului cu o majoritate de două treimi.

Regulamentul de procedură stabilește, în special, procedurile pentru procesul de selecție, durata mandatului și specificațiile sarcinilor președintelui, modalitățile de vot și organizarea activităților comitetului și a subgrupurilor acestuia.

Comitetul instituie un subgrup permanent care să servească drept platformă pentru ca părțile interesate să consilieze comitetul cu privire la toate aspectele legate de punerea în aplicare a prezentului regulament, inclusiv cu privire la pregătirea actelor de punere în aplicare și a actelor delegate. În acest scop, organizațiile care reprezintă interesele furnizorilor și utilizatorilor de sisteme de IA, inclusiv IMM-urile și întreprinderile nou-înființate, precum și organizațiile societății civile, reprezentanții persoanelor afectate, cercetătorii, organizațiile de standardizare, organismele notificate, laboratoarele și instalațiile de testare și experimentare sunt invitate să participe la acest subgrup. Comitetul instituie două subgrupuri permanente pentru a oferi o platformă de cooperare și de schimb între autoritățile de supraveghere a pieței și autoritățile de notificare cu privire la aspecte legate de supravegherea pieței și, respectiv, de organismele notificate.

Comitetul poate înființa alte subgrupuri permanente sau temporare, după caz, în scopul examinării unor chestiuni specifice. După caz, părțile interesate menționate la paragraful anterior pot fi invitate la astfel de subgrupuri sau la reuniuni specifice ale subgrupurilor respective în calitate de observatori.

(3a) Comitetul este organizat și funcționează astfel încât să garanteze obiectivitatea și imparțialitatea activităților sale.

(4) Comitetul este prezidat de către unul dintre reprezentanții statelor membre. La solicitarea președintelui, 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.

Articolul 57

[eliminat]

Articolul 58

Sarcinile comitetului

Comitetul oferă consiliere și asistență Comisiei și statelor membre pentru a facilita aplicarea coerentă și eficace a prezentului regulament. În acest scop, comitetul poate, în special:

(a) asigura colectarea și schimbul de expertiză tehnică și în materie de reglementare și de bune practici între statele membre;

(b) contribui la armonizarea practicilor administrative din statele membre, inclusiv în ceea ce privește derogarea de la procedurile de evaluare a conformității menționate la articolul 47, funcționarea spațiilor de testare în materie de reglementare și testarea în condiții reale menționate la articolele 53, 54 și 54a;

(c) la cererea Comisiei sau din proprie inițiativă, emite recomandări și avize scrise cu privire la orice aspecte relevante legate de punerea în aplicare a prezentului regulament și de aplicarea coerentă și eficace a acestuia, inclusiv:

(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;

(d) consilia Comisia cu privire la eventuala necesitate de modificare a anexei III în conformitate cu articolele 4 și 7, ținând seama de dovezile relevante disponibile și de cele mai recente evoluții tehnologice;

(e) consilia Comisia în cursul pregătirii actelor delegate sau de punere în aplicare în temeiul prezentului regulament;

(f) coopera, după caz, cu organismele, grupurile de experți și rețelele relevante ale UE, în special în domeniul siguranței produselor, al securității cibernetice, al concurenței, al serviciilor digitale și media, al serviciilor financiare, al criptomonedelor, al protecției consumatorilor, al protecției datelor și a drepturilor fundamentale;

(g) contribui și oferi consultanță relevantă Comisiei în elaborarea orientărilor menționate la articolul 58a sau solicita elaborarea unor astfel de orientări;

(h) sprijini activitatea autorităților de supraveghere a pieței și, în cooperare și sub rezerva acordului autorităților de supraveghere a pieței în cauză, promova și sprijini investigațiile transfrontaliere în materie de supraveghere a pieței, inclusiv în ceea ce privește apariția riscurilor de natură sistemică care pot proveni din sistemele de IA;

(i) contribui la evaluarea nevoilor de formare pentru personalul statelor membre implicat în punerea în aplicare a prezentului regulament;

(j) consilia Comisia în legătură cu chestiunile internaționale privind inteligența artificială.

CAPITOLUL 1A

ORIENTĂRI DIN PARTEA COMISIEI

Articolul 58a

Orientări din partea Comisiei cu privire la punerea în aplicare a prezentului regulament

(1) La solicitarea statelor membre sau a comitetului sau din proprie inițiativă, Comisia emite orientări cu privire la punerea în practică a prezentului regulament și, în special, cu privire la

(i) aplicarea cerințelor menționate la articolele 8 - 15;

(ii) practicile interzise menționate la articolul 5;

(iii) punerea în practică a dispozițiilor referitoare la modificarea substanțială;

(iv) punerea în practică a condițiilor uniforme menționate la articolul 6 alineatul (3), inclusiv exemple în ceea ce privește sistemele de IA cu risc ridicat menționate în anexa III;

(v) punerea în practică a obligațiilor de transparență prevăzute la articolul 52;

(vi) relația dintre prezentul regulament și alte acte legislative relevante ale Uniunii, inclusiv cu privire la coerența în ceea ce privește asigurarea respectării acestora.

Atunci când emite astfel de orientări, Comisia acordă o atenție deosebită nevoilor IMM-urilor, inclusiv ale întreprinderilor nou-înființate, ale autorităților publice locale și ale sectoarelor celor mai susceptibile de a fi afectate de prezentul regulament.

CAPITOLUL 2

AUTORITĂȚILE NAȚIONALE COMPETENTE

Articolul 59

Desemnarea autorităților naționale competente

(1) [eliminat]

(2) Fiecare stat membru stabilește sau desemnează cel puțin o autoritate de notificare și cel puțin o autoritate de supraveghere a pieței în sensul prezentului regulament în calitate de autorități naționale competente. Aceste autorități naționale competente sunt organizate astfel încât să garanteze principiile obiectivității și imparțialității activităților și sarcinilor lor. Cu condiția ca aceste principii să fie respectate, astfel de activități și sarcini pot fi efectuate de una sau mai multe autorități desemnate, în conformitate cu nevoile organizaționale ale statului membru.

(3) Statele membre informează Comisia în legătură cu desemnarea sau desemnările lor.

(4) Statele membre se asigură că autoritățile naționale competente dispun de resurse financiare, echipamente tehnice și resurse umane competente adecvate pentru a-și îndeplini cu eficacitate sarcinile care le revin în temeiul prezentului regulament.

(5) Până la *[un an de la intrarea în vigoare a prezentului regulament]* și ulterior cu șase luni înainte de termenul menționat la articolul 84 alineatul (2), statele membre informează Comisia cu privire la situația resurselor financiare, a echipamentelor tehnice și a resurselor umane ale autorităților naționale competente, evaluând caracterul adecvat al acestora. 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 consiliere cu privire la punerea în aplicare a prezentului regulament, adaptată inclusiv IMM-urilor furnizoare, inclusiv întreprinderilor nou-înființate. 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 SISTEMELE DE IA CU GRAD RIDICAT DE RISC ENUMERATE ÎN ANEXA III

Articolul 60

Baza de date a UE pentru sistemele de IA cu grad ridicat de risc enumerate în anexa III

(1) Comisia, în colaborare cu statele membre, creează și întreține o bază de date a UE care conține informațiile menționate la alineatul (2) privind operatorii relevanți și sistemele de IA cu grad ridicat de risc enumerate în anexa III care sunt înregistrate în conformitate cu articolele 51 și 54a. Atunci când stabilește specificațiile funcționale ale unei astfel de baze de date, Comisia consultă Comitetul pentru IA.

(2) Datele enumerate în anexa VIII partea I se introduc în baza de date a UE de către furnizori, reprezentanții autorizați și utilizatorii relevanți, după caz, la înregistrarea lor. Datele enumerate în anexa VIII partea II punctele 1-11 se introduc în baza de date a UE de către furnizori sau, după caz, de către reprezentantul autorizat, în conformitate cu articolul 51. Datele menționate în anexa VIII partea II punctul 12 sunt generate automat de baza de date pe baza informațiilor furnizate de utilizatorii relevanți în temeiul articolului 51 alineatul (2). Datele enumerate în anexa VIIIa sunt introduse în baza de date de către potențialii furnizori sau de către furnizori în conformitate cu articolul 54a.

(3) [eliminat]

(4) Baza de date a UE nu conține date cu caracter personal, cu excepția informațiilor enumerate în anexa VIII, și nu aduce atingere articolului 70.

(5) Comisia este operatorul bazei de date a UE. Aceasta pune la dispoziția furnizorilor, a potențialilor furnizori și a utilizatorilor sprijin tehnic și administrativ adecvat.

(5a) Informațiile conținute în baza de date a UE, înregistrate în conformitate cu articolul 51, sunt accesibile publicului. Informațiile înregistrate în conformitate cu articolul 54a sunt accesibile numai autorităților de supraveghere a pieței și Comisiei, cu excepția cazului în care potențialul furnizor sau furnizorul și-a dat consimțământul pentru ca aceste informații să fie, de asemenea, accesibile publicului.

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 riscurile sistemului de IA cu grad ridicat de risc.

(2) Pentru a permite furnizorului să evalueze conformitatea sistemelor de IA cu cerințele prevăzute în titlul III capitolul 2 pe parcursul întregului lor ciclu de viață, sistemul de monitorizare ulterioară introducerii pe piață colectează, documentează și analizează datele relevante care pot fi furnizate de utilizatori sau care pot fi colectate din alte surse cu privire la performanța sistemelor de IA cu grad ridicat de risc. Această obligație nu acoperă datele operaționale sensibile ale utilizatorilor sistemelor de IA care sunt autorități de aplicare a legii.

(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 secțiunea A, în cazul în care s-au instituit deja un sistem și un plan de monitorizare ulterioară introducerii pe piață în temeiul legislației respective, documentația de monitorizare ulterioară introducerii pe piață pregătită în temeiul legislației respective este considerată suficientă, cu condiția utilizării modelului menționat la alineatul (3).

Primul paragraf se aplică, de asemenea, sistemelor de IA cu grad ridicat de risc menționate la punctul 5 din anexa III introduse pe piață sau puse în funcțiune de instituții financiare care fac obiectul unor cerințe privind guvernanța lor internă, măsurile sau procesele lor interne în temeiul legislației Uniunii privind serviciile financiare.

CAPITOLUL 2

SCHIMBUL DE INFORMAȚII PRIVIND INCIDENTELE GRAVE

Articolul 62

Raportarea incidentelor grave

(1) Furnizorii de sisteme de IA cu grad ridicat de risc introduse pe piața Uniunii raportează orice incident grav autorităților de supraveghere a pieței din statele membre în care s-a produs incidentul respectiv.

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

(2) La primirea unei notificări referitoare la un incident grav menționat la articolul 3 alineatul (44) litera (c), autoritatea relevantă 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 din anexa III care sunt introduse pe piață sau puse în funcțiune de instituții financiare care fac obiectul unor cerințe privind guvernanța lor internă, măsurile sau procesele lor interne în temeiul legislației Uniunii privind serviciile financiare, notificarea incidentelor grave se limitează la cele menționate la articolul 3 alineatul (44) litera (c).

(4) În cazul sistemelor 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 se limitează la cele menționate la articolul 3 alineatul (44) litera (c) și se efectuează către autoritatea națională competentă aleasă în acest scop de statele membre în care s-a produs incidentul respectiv.

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 la articolul 2 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) Ca parte a obligațiilor de raportare care le revin în temeiul articolului 34 alineatul (4) din Regulamentul (UE) 2019/1020, autoritățile de supraveghere a pieței raportează Comisiei cu privire la rezultatele activităților relevante de supraveghere a pieței în temeiul prezentului regulament.

(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 sau, în circumstanțe justificate și cu condiția asigurării coordonării, o altă autoritate relevantă identificată de statul membru.

Procedurile menționate la articolele 65 - 68 din prezentul regulament nu se aplică sistemelor de IA legate de produse cărora li se aplică actele juridice enumerate în anexa II secțiunea A, atunci când astfel de acte juridice prevăd deja proceduri care au același obiectiv. În acest caz, se aplică în schimb aceste proceduri sectoriale.

(4) Pentru sistemele de IA cu grad ridicat de risc 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 națională relevantă responsabilă cu supravegherea financiară a instituțiilor respective în temeiul legislației respective, în măsura în care introducerea pe piață, punerea în funcțiune sau utilizarea sistemului de IA este în legătură directă cu furnizarea serviciilor financiare respective.

Prin derogare de la paragraful anterior, în circumstanțe justificate și cu condiția asigurării coordonării, o altă autoritate relevantă poate fi identificată de statul membru drept autoritate de supraveghere a pieței în sensul prezentului regulament.

Autoritățile naționale de supraveghere a pieței care supraveghează instituțiile de credit reglementate în temeiul Directivei 2013/36/UE, care participă la mecanismul unic de supraveghere (MUS) instituit prin Regulamentul nr. 1024/2013 al Consiliului, ar trebui să raporteze fără întârziere Băncii Centrale Europene orice informații identificate în cursul activităților lor de supraveghere a pieței care ar putea prezenta un interes potențial pentru sarcinile de supraveghere prudențială ale Băncii Centrale Europene, astfel cum se specifică în regulamentul respectiv.

(5) Pentru sistemele de IA cu grad ridicat de risc enumerate la punctul 1 litera (a), în măsura în care sistemele sunt utilizate în scopul asigurării respectării legii, la punctele 6, 7 și 8 din anexa III, statele membre desemnează drept autorități de supraveghere a pieței în sensul prezentului regulament fie autoritățile naționale care supraveghează activitățile autorităților responsabile în materie de aplicare a legii, de control la frontiere, de imigrație, de azil sau ale autorităților judiciare, fie autoritățile de supraveghere în materie de protecție a datelor competente în temeiul Directivei (UE) 2016/680 sau al Regulamentului 2016/679. Activitățile de supraveghere a pieței nu afectează în niciun fel independența autorităților judiciare și nici nu interferează în alt mod cu activitățile acestora atunci când acționează în exercițiul funcției lor judiciare.

(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.

(8) Fără a aduce atingere competențelor prevăzute în Regulamentul (UE) 2019/1020 și dacă este relevant și limitat la ceea ce este necesar pentru a-și îndeplini sarcinile, furnizorul acordă acces deplin autorităților de supraveghere a pieței la documentație, precum și la seturile de date de antrenament, de validare și de testare utilizate pentru dezvoltarea sistemului de IA cu grad ridicat de risc, inclusiv, dacă este cazul și sub rezerva unor garanții de securitate, prin interfețe de programare a aplicațiilor („IPA”) sau prin alte mijloace și instrumente tehnice relevante care permit accesul de la distanță.

(9) Autorităților de supraveghere a pieței li se acordă acces la codul sursă al sistemului de IA cu grad ridicat de risc pe baza unei cereri motivate și numai atunci când sunt îndeplinite următoarele condiții cumulative:

(a) accesul la codul sursă este necesar pentru a evalua conformitatea unui sistem de IA cu grad ridicat de risc cu cerințele prevăzute în titlul III capitolul 2 și

(b) procedurile de testare/audit și verificările bazate pe datele și documentația furnizate de furnizor au fost epuizate sau s-au dovedit insuficiente.

(10) Toate informațiile și documentația obținute de autoritățile de supraveghere a pieței în temeiul prezentului articol sunt tratate în conformitate cu obligațiile de confidențialitate prevăzute la articolul 70.

(11) Plângerile adresate autorității relevante de supraveghere a pieței pot fi depuse de orice persoană fizică sau juridică care are motive să considere că a avut loc o încălcare a dispozițiilor prezentului regulament.

În conformitate cu articolul 11 alineatul (3) litera (e) și alineatul (7) litera (a) din Regulamentul (UE) 2019/1020, plângerile sunt luate în considerare în scopul desfășurării activităților de supraveghere a pieței și sunt tratate în conformitate cu procedurile specifice stabilite prin urmare de autoritățile de supraveghere a pieței.

Articolul 63a

Supravegherea testării în condiții reale de către autoritățile de supraveghere a pieței

(1) Autoritățile de supraveghere a pieței dețin competența și prerogativele necesare pentru a se asigura că testarea în condiții reale este conformă cu prezentul regulament.

(2) În cazul în care se efectuează testarea în condiții reale pentru sistemele de IA care sunt supravegheate într-un spațiu de testare în materie de reglementare a IA în temeiul articolului 54, autoritățile de supraveghere a pieței verifică conformitatea cu dispozițiile articolului 54a ca parte a rolului lor de supraveghere pentru spațiul de testare în materie de reglementare a IA. Autoritățile respective pot permite, după caz, ca testarea în condiții reale să fie efectuată de furnizor sau de potențialul furnizor, prin derogare de la condițiile prevăzute la articolul 54a alineatul (4) literele (f) și (g).

(3) În cazul în care o autoritate de supraveghere a pieței a fost informată de către furnizorul potențial, de către furnizor sau de către orice parte terță cu privire la un incident grav sau are alte motive pentru a considera că nu sunt îndeplinite condițiile prevăzute la articolele 54a și 54b, aceasta poate lua oricare dintre următoarele decizii pe teritoriul său, după caz:

(a) suspendarea sau încetarea testării în condiții reale;

(b) solicitarea furnizorului sau potențialului furnizor și utilizatorului (utilizatorilor) să modifice orice aspect al testării în condiții reale.

(4) În cazul în care o autoritate de supraveghere a pieței a luat o decizie menționată la alineatul (3) din prezentul articol sau a emis o obiecție în sensul articolului 54a alineatul (4) litera (b), decizia sau obiecția indică motivele acesteia, precum și modalitățile și condițiile în care furnizorul sau potențialul furnizor poate contesta decizia sau obiecția.

(5) După caz, în cazul în care o autoritate de supraveghere a pieței a luat o decizie menționată la alineatul (3) din prezentul articol, aceasta comunică motivele care stau la baza deciziei respective autorităților de supraveghere a pieței din celelalte state membre în care sistemul de IA a fost testat în conformitate cu planul de testare.

Articolul 64

Competențele autorităților care protejează drepturile fundamentale

(1) [eliminat]

(2) [eliminat]

(3) Autoritățile sau organismele publice naționale care supraveghează sau asigură respectarea obligațiilor în temeiul dreptului Uniunii care protejează drepturile fundamentale, inclusiv dreptul la nediscriminare, 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 lista la dispoziția publicului. 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 drepturile 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 sunt identificate riscuri pentru drepturile 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, fără întârzieri nejustificate, 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 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, fără întârzieri nejustificate, 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 notifică aceste măsuri Comisiei și celorlalte state membre, fără întârzieri nejustificate.

(6) Notificarea menționată la alineatul (5) include toate detaliile disponibile, în special informațiile 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 interdicției privind practicile în domeniul inteligenței artificiale menționate la articolul 5;

(a) nerespectarea de către sistemul de IA cu grad ridicat de risc 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.

(c) nerespectarea dispozițiilor prevăzute la articolul 52;

(d) nerespectarea de către sistemele de IA de uz general a cerințelor și obligațiilor menționate la articolul 4a;

(7) Autoritățile de supraveghere a pieței din statele membre, altele decât autoritatea de supraveghere a pieței din statul membru care a inițiat procedura, informează, fără întârzieri nejustificate, 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 notificării 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. Termenul menționat în prima teză a prezentului alineat se reduce la 30 de zile în cazul nerespectării interdicției privind practicile în domeniul inteligenței artificiale menționate la articolul 5.

(9) Autoritățile de supraveghere a pieței din toate statele membre se asigură apoi că se iau măsuri restrictive adecvate în ceea ce privește sistemul de IA în cauză, cum ar fi retragerea fără întârzieri nejustificate 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) sau în termen de 30 de zile în cazul nerespectării interdicției privind practicile în domeniul inteligenței artificiale menționate la articolul 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 întârzieri nejustificate, consultări cu autoritatea de supraveghere a pieței din 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 nouă luni sau de 60 de zile în cazul nerespectării interdicției privind practicile în domeniul inteligenței artificiale menționate la articolul 5, începând cu notificarea menționată la articolul 65 alineatul (5). Comisia notifică respectiva decizie statului membru în cauză. Comisia informează de asemenea toate celelalte state membre cu privire la această decizie.

(2) În cazul în care măsura luată de autoritatea de supraveghere a pieței din statul membru în cauză este considerată justificată de către Comisie, autoritățile de supraveghere a pieței din toate statele membre se asigură că se iau măsuri restrictive adecvate în ceea ce privește sistemul de IA în cauză, cum ar fi retragerea fără întârzieri nejustificate a sistemului de IA de pe piața lor, și informează Comisia în consecință. În cazul în care măsura națională este considerată nejustificată de către Comisie, autoritatea de supraveghere a pieței din statul membru în cauză retrage măsura și informează Comisia în consecință.

(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 cu grad ridicat de risc sau de uz general 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 cu grad ridicat de risc sau de uz general este în conformitate cu prezentul regulament, acesta prezintă un risc pentru sănătatea sau siguranța persoanelor sau pentru drepturile fundamentale, autoritatea de supraveghere respectivă 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, să retragă de pe piață sau să recheme sistemul de IA fără întârzieri nejustificate, într-un termen 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 întârzieri nejustificate consultări cu statele membre în cauză 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 statului membru în cauză și informează toate celelalte 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, într-un termen indicat de aceasta, 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.

Articolul 68a

Instalațiile de testare ale Uniunii în domeniul inteligenței artificiale

(1) Comisia desemnează una sau mai multe instalații de testare ale Uniunii în domeniul inteligenței artificiale în temeiul articolului 21 din Regulamentul (UE) nr. 1020/2019.

(2) Fără a aduce atingere activităților instalațiilor de testare ale Uniunii menționate la articolul 21 alineatul (6) din Regulamentul (UE) nr. 1020/2019, instalațiile de testare ale Uniunii menționate la alineatul (1) furnizează, de asemenea, consiliere tehnică sau științifică independentă la cererea comitetului sau a autorităților de supraveghere a pieței.

Articolul 68b

Grupul central de experți independenți

(1) La cererea Comitetului pentru IA, Comisia, prin intermediul unui act de punere în aplicare, adoptă dispoziții privind crearea, menținerea și finanțarea unui grup central de experți independenți care să sprijine activitățile de asigurare a respectării legislației în temeiul prezentului regulament.

(2) Experții sunt selectați de Comisie și incluși în grupul central pe baza unei expertize științifice sau tehnice actualizate în domeniul inteligenței artificiale, ținând seama în mod corespunzător de domeniile tehnice vizate de cerințele și obligațiile prevăzute în prezentul regulament și de activitățile autorităților de supraveghere a pieței în temeiul articolului 11 din Regulamentul (UE) 1020/2019. Comisia stabilește numărul de experți din grup în funcție de necesități.

(3) Experții pot avea următoarele sarcini:

(a) oferă consiliere și sprijin autorităților de supraveghere a pieței, la cererea acestora;

(b) sprijină investigațiile transfrontaliere în materie de supraveghere a pieței menționate la articolul 58 litera (h), fără a aduce atingere competențelor autorităților de supraveghere a pieței;

(c) consiliază și sprijină Comisia în îndeplinirea sarcinilor sale în contextul clauzei de salvgardare în temeiul articolului 66.

(4) Experții își îndeplinesc sarcinile cu imparțialitate și obiectivitate și asigură confidențialitatea informațiilor și a datelor obținute în cursul îndeplinirii sarcinilor și activităților lor. Fiecare expert întocmește o declarație de interese, care este pusă la dispoziția publicului. Comisia instituie sisteme și proceduri pentru a gestiona în mod activ și pentru a preveni potențialele conflicte de interese.

(5) Statele membre pot fi obligate să plătească onorarii pentru consilierea și sprijinul din partea experților. Structura și nivelul taxelor, precum și amploarea și structura costurilor recuperabile sunt adoptate de Comisie prin intermediul actului de punere în aplicare menționat la alineatul (1), ținând seama de obiectivele punerii în aplicare adecvate a prezentului regulament, de raportul cost-eficacitate și de necesitatea de a asigura accesul efectiv al tuturor statelor membre la experți.

(6) Comisia facilitează accesul în timp util al statelor membre la experți, după caz, și se asigură că combinarea activităților de sprijin desfășurate de instalațiile de testare ale Uniunii în temeiul articolului 68a și de experți în temeiul prezentului articol este organizată în mod eficient și oferă cea mai bună valoare adăugată posibilă.

TITLUL IX

CODURI DE CONDUITĂ

Articolul 69

Coduri de conduită pentru aplicarea voluntară a cerințelor specifice

(1) Comisia și statele membre facilitează elaborarea de coduri de conduită menite să încurajeze aplicarea voluntară în cazul altor sisteme de IA decât sistemele de IA cu grad ridicat de risc a uneia sau mai multora dintre cerințele prevăzute în titlul III capitolul 2 din prezentul regulament, în cea mai mare măsură posibilă, ținând seama de soluțiile tehnice disponibile care permit aplicarea unor astfel de cerințe.

(2) Comisia și statele membre facilitează elaborarea de coduri de conduită menite să încurajeze aplicarea voluntară, pentru toate sistemele de IA, a cerințelor specifice legate, de exemplu, de durabilitatea mediului, inclusiv în ceea ce privește programarea eficientă din punct de vedere energetic, de accesibilitatea pentru persoanele cu dizabilități, 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. Comisia și statele membre facilitează, de asemenea, după caz, elaborarea unor coduri de conduită aplicabile în mod voluntar în ceea ce privește obligațiile utilizatorilor în ceea ce privește sistemele de IA.

(3) Codurile de conduită aplicabile în mod voluntar 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 sau, după caz, de utilizatori în ceea ce privește obligațiile care le revin. Codurile de conduită pot acoperi unul sau mai multe sisteme de IA, ținând seama de similaritatea scopului preconizat al sistemelor relevante.

(4) Comisia și statele membre țin seama de interesele și nevoile specifice ale IMM-urilor furnizoare, inclusiv ale întreprinderilor nou-înființate, atunci când încurajează și facilitează elaborarea codurilor de conduită menționate în prezentul articol.

TITLUL X

CONFIDENȚIALITATE ȘI SANCȚIUNI

Articolul 70

Confidențialitate

(1) Autoritățile naționale competente, organismele notificate, Comisia, comitetul și orice altă persoană fizică sau juridică implicată în aplicarea prezentului regulament instituie, în conformitate cu dreptul Uniunii sau cu dreptul intern, măsuri tehnice și organizatorice adecvate pentru a asigura 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 și auditurilor;

(c) interesele de securitate publică și națională;

(d) integritatea procedurilor penale sau administrative;

(e) integritatea informațiilor clasificate în conformitate cu dreptul Uniunii sau cu dreptul intern.

(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 responsabile în materie de aplicare a legii, de control la frontiere, de imigrație sau de azil, în cazul în care o astfel de divulgare ar pune în pericol interesele publice și de securitate națională. Această obligație de a face schimb de informații nu acoperă datele operaționale sensibile legate de activitățile autorităților responsabile în materie de aplicare a legii, de control la frontiere, de imigrație sau de azil.

În cazul în care autoritățile responsabile în materie de aplicare a legii, de imigrație sau de azil 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 autorităților relevante ale acestora, precum și organismelor notificate cu privire la schimbul de informații și difuzarea avertizărilor, inclusiv în contextul cooperării transfrontaliere, și nici obligațiilor părților în cauză de a furniza informații în temeiul dreptului penal al statelor membre.

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 dimensiunea și interesele IMM-urilor furnizoare, inclusiv ale întreprinderilor nou-înființate, precum și de viabilitatea lor economică. De asemenea, statele membre iau în considerare cazul în care sistemul de IA este utilizat în contextul unei activități neprofesionale, personale.

(2) Statele membre notifică normele și măsurile respective Comisiei și îi comunică acesteia, fără întârziere, orice modificare ulterioară care le afectează.

(3) Nerespectarea oricăreia dintre interdicțiile privind practicile în domeniul inteligenței artificiale menționate la articolul 5 face 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 dintre acestea. În cazul IMM-urilor, inclusiv al întreprinderilor nou-înființate, aceste amenzi sunt de până la 3 % din cifra lor de afaceri anuală mondială pentru exercițiul financiar precedent.

(4) Încălcările următoarelor dispoziții privind operatorii sau organismele notificate fac 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:

(-a) obligațiile furnizorilor în temeiul articolelor 4b și 4c;

(a) obligațiile furnizorilor în temeiul articolului 16;

(b) obligațiile pentru anumite alte persoane în temeiul articolului 23a;

(c) obligațiile reprezentanților autorizați în temeiul articolului 25;

(d) obligațiile importatorilor în temeiul articolului 26;

(e) obligațiile distribuitorilor în temeiul articolului 27;

(f) obligațiile utilizatorilor în temeiul articolului 29 alineatele (1) - (6a);

(g) cerințele și obligațiile organismelor notificate în temeiul articolului 33, al articolului 34 alineatul (1), al articolului 34 alineatul (3), al articolului 34 alineatul (4) și al articolului 34a;

(h) obligațiile de transparență pentru furnizori și utilizatori în temeiul articolului 52.

În cazul IMM-urilor, inclusiv al întreprinderilor nou-înființate, aceste amenzi sunt de până la 2 % din cifra lor de afaceri anuală mondială pentru exercițiul financiar precedent.

(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. În cazul IMM-urilor, inclusiv al întreprinderilor nou-înființate, aceste amenzi sunt de până la 1 % din cifra lor de afaceri anuală mondială pentru exercițiul financiar precedent.

(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;

(aa) dacă încălcarea a fost comisă intenționat sau din neglijență;

(ab) orice măsură luată de operator pentru a remedia încălcarea și a atenua posibilele efecte negative ale încălcării;

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

(ba) dacă alte autorități au aplicat deja amenzi administrative aceluiași operator pentru încălcări ale altor acte legislative ale Uniunii sau ale legislației naționale, în cazul în care astfel de încălcări rezultă din aceeași activitate sau omisiune care constituie o încălcare relevantă a prezentului act;

(c) dimensiunea, cifra de afaceri anuală și cota de piață ale operatorului care a săvârșit încălcarea;

(d) orice alt factor agravant sau atenuant aplicabil circumstanțelor cazului, cum ar fi beneficiile financiare dobândite sau pierderile evitate în mod direct sau indirect de pe urma încălcării.

(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 sau de alte organisme, astfel cum sunt aplicabile în statele membre respective. Aplicarea unor astfel de norme în statele membre respective are un efect echivalent.

(9) Exercitarea de către autoritatea de supraveghere a pieței a competențelor sale în temeiul prezentului articol are loc cu condiția existenței unor garanții procedurale adecvate în conformitate cu dreptul Uniunii și cu dreptul intern, inclusiv căi de atac judiciare eficiente și dreptul la un proces echitabil.

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) Nerespectarea oricăreia dintre interdicțiile privind practicile de inteligență artificială menționate la articolul 5 face obiectul unor amenzi administrative de până la 500 000 EUR.

(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 7 alineatul (1), la articolul 7 alineatul (3), la articolul 11 alineatul (3), la articolul 43 alineatele (5) și (6) și la articolul 48 alineatul (5) se conferă Comisiei pentru o perioadă de cinci ani de la [*intrarea în vigoare a regulamentului*].

Comisia elaborează un raport privind delegarea de competențe cu cel puțin nouă luni înainte de încheierea perioadei de cinci ani. Delegarea de competențe se prelungește tacit cu perioade de timp identice, cu excepția cazului în care Parlamentul European sau Consiliul se opune prelungirii respective cu cel puțin trei luni înainte de încheierea fiecărei perioade.

(3) Delegarea de competențe menționată la articolul 7 alineatul (1), la articolul 7 alineatul (3), 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 7 alineatul (1), al articolului 7 alineatul (3), 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

Modificare adusă 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) [eliminat]

(1b) Comisia evaluează necesitatea modificării listei din anexa III o dată la 24 de luni după intrarea în vigoare a prezentului regulament și până la sfârșitul perioadei de delegare a competențelor. Rezultatele evaluării respective sunt prezentate Parlamentului European și Consiliului.

(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, a echipamentelor tehnice și a resurselor 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, după caz, Comisia evaluează impactul și eficacitatea codurilor de conduită voluntare pentru a încuraja aplicarea cerințelor prevăzute în titlul III capitolul 2 pentru sistemele de IA, altele decât sistemele de IA cu grad ridicat de risc și, eventual, a altor cerințe suplimentare pentru sistemele de IA, inclusiv în ceea ce privește durabilitatea mediului.

(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 (1a)-(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 [36 de 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 [12 luni de la intrarea în vigoare a prezentului regulament];

(b) articolul 71 se aplică de la [12 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*

ANEXA I

[eliminat]

ANEXA II

LISTA LEGISLAȚIEI DE ARMONIZARE A UNIUNII

Secțiunea A – Lista legislației de armonizare a Uniunii pe baza noului cadru legislativ

1. Directiva 2006/42/CE a Parlamentului European și a Consiliului din 17 mai 2006 privind echipamentele tehnice și de modificare a Directivei 95/16/CE (JO L 157, 9.6.2006, p. 24) (astfel cum a fost abrogată de Regulamentul privind echipamentele tehnice);

2. Directiva 2009/48/CE a Parlamentului European și a Consiliului din 18 iunie 2009 privind siguranța jucăriilor (JO L 170, 30.6.2009, p. 1);

3. Directiva 2013/53/UE a Parlamentului European și a Consiliului din 20 noiembrie 2013 privind ambarcațiunile de agrement și motovehiculele nautice și de abrogare a Directivei 94/25/CE (JO L 354, 28.12.2013, p. 90);

4. Directiva 2014/33/UE a Parlamentului European și a Consiliului din 26 februarie 2014 de armonizare a legislațiilor statelor membre referitoare la ascensoare și la componentele de siguranță pentru ascensoare (JO L 96, 29.3.2014, p. 251);

5. Directiva 2014/34/UE a Parlamentului European și a Consiliului din 26 februarie 2014 privind armonizarea legislațiilor statelor membre referitoare la echipamentele și sistemele de protecție destinate utilizării în atmosfere potențial explozive (JO L 96, 29.3.2014, p. 309);

6. Directiva 2014/53/UE a Parlamentului European și a Consiliului din 16 aprilie 2014 privind armonizarea legislației statelor membre referitoare la punerea la dispoziție pe piață a echipamentelor radio și de abrogare a Directivei 1999/5/CE (JO L 153, 22.5.2014, p. 62);

7. Directiva 2014/68/UE a Parlamentului European și a Consiliului din 15 mai 2014 privind armonizarea legislației statelor membre referitoare la punerea la dispoziție pe piață a echipamentelor sub presiune (JO L 189, 27.6.2014, p. 164);

8. Regulamentul (UE) 2016/424 al Parlamentului European și al Consiliului din 9 martie 2016 privind instalațiile pe cablu și de abrogare a Directivei 2000/9/CE (JO L 81, 31.3.2016, p. 1);

9. Regulamentul (UE) 2016/425 al Parlamentului European și al Consiliului din 9 martie 2016 privind echipamentele individuale de protecție și de abrogare a Directivei 89/686/CEE a Consiliului (JO L 81, 31.3.2016, p. 51);

10. Regulamentul (UE) 2016/426 al Parlamentului European și al Consiliului din 9 martie 2016 privind aparatele consumatoare de combustibili gazoși și de abrogare a Directivei 2009/142/CE (JO L 81, 31.3.2016, p. 99);

11. 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);

12. 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).

Secțiunea B. Lista altor acte legislative de armonizare ale Uniunii

1. 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).

2. 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);

3. 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);

4. 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);

5. 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).

6. 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);

7. 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);

8. 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), în ceea ce privește proiectarea, producerea și introducerea pe piață a aeronavelor menționate la articolul 2 alineatul (1) literele (a) și (b), în cazul aeronavelor fără pilot la bord și al motoarelor, elicelor, pieselor și echipamentelor acestora de control de la distanță.

ANEXA III

SISTEMELE DE IA CU GRAD RIDICAT DE RISC MENȚIONATE LA ARTICOLUL 6 ALINEATUL (3)

În fiecare dintre domeniile enumerate la punctele 1-8, sistemele de IA menționate în mod specific la fiecare literă sunt considerate sisteme de IA cu grad ridicat de risc în temeiul articolului 6 alineatul (3):

1. biometrie:

   (a) sisteme de identificare biometrică la distanță;

2. infrastructură critică:

   (a) sisteme de IA destinate a fi utilizate drept componente de siguranță în gestionarea și operarea infrastructurii digitale critice, a traficului rutier și în aprovizionarea cu apă, gaz, încălzire și energie electrică;

3. educație și formare profesională:

   (a) sisteme de IA destinate a fi utilizate pentru a stabili accesul, admisia sau pentru a repartiza persoane fizice la instituțiile de învățământ și formare profesională sau în programele de formare profesională la toate nivelurile;

   (b) sisteme de IA destinate a fi utilizate pentru a evalua rezultatele învățării, inclusiv atunci când acestea sunt utilizate pentru a orienta procesul de învățare al persoanelor fizice în instituțiile de învățământ și formare profesională sau în programele de formare profesională la toate nivelurile;

4. ocuparea forței de muncă, gestionarea lucrătorilor și accesul la activități independente:

   (a) sisteme de IA destinate a fi utilizate pentru recrutarea sau selectarea persoanelor fizice, în special pentru a plasa anunțuri de angajare specifice, pentru a analiza și a filtra candidaturile pentru locuri de muncă și pentru a evalua candidații;

(b) inteligență artificială destinată a fi utilizată pentru a lua decizii privind promovarea și încetarea relațiilor contractuale legate de muncă, pentru a aloca sarcini pe baza comportamentului individual sau a trăsăturilor ori caracteristicilor personale și pentru a monitoriza și evalua performanța și comportamentul persoanelor aflate în astfel de relații;

5. accesul la servicii esențiale private și la servicii și beneficii publice esențiale, precum și posibilitatea de a beneficia de acestea:

(a) sisteme de IA destinate a fi utilizate de autoritățile publice sau în numele autorităților publice pentru a evalua eligibilitatea persoanelor fizice pentru prestații și servicii esențiale de asistență publică, precum și pentru a acorda, a reduce, a revoca sau a recupera astfel de prestații și servicii;

(b) sisteme de IA destinate a fi utilizate pentru a evalua bonitatea persoanelor fizice sau pentru a stabili punctajul lor de credit, cu excepția sistemelor de IA puse în funcțiune pentru uz propriu de furnizori care sunt microîntreprinderi și întreprinderi mici, astfel cum sunt definite în anexa la Recomandarea 2003/361/CE a Comisiei;

(c) sisteme de IA destinate a fi utilizate pentru dispecerizare sau pentru a stabili prioritatea în dispecerizarea serviciilor de primă intervenție de urgență, inclusiv de către pompieri și de asistență medicală;

(d) sisteme de IA destinate a fi utilizate pentru evaluarea riscurilor și stabilirea prețurilor în ceea ce privește persoanele fizice în cazul asigurărilor de viață și de sănătate, cu excepția sistemelor de IA puse în funcțiune pentru uz propriu de furnizori care sunt microîntreprinderi și întreprinderi mici, astfel cum sunt definite în anexa la Recomandarea 2003/361/CE a Comisiei;

6. aplicarea legii:

(a) sisteme de IA destinate a fi utilizate de autoritățile de aplicare a legii sau în numele acestora pentru a evalua riscul ca o persoană fizică să comită infracțiuni sau să recidiveze sau riscul ca o persoană fizică să devină o potențială victimă a unor infracțiuni;

(b) sisteme de IA destinate a fi utilizate de autoritățile de aplicare a legii sau în numele acestora drept poligrafe și instrumente similare sau pentru a detecta starea emoțională a unei persoane fizice;

(c) [eliminat]

(d) sisteme de IA destinate a fi utilizate de autoritățile de aplicare a legii sau în numele acestora pentru a evalua fiabilitatea probelor în cursul investigării sau al urmăririi penale a infracțiunilor;

(e) sisteme de IA destinate a fi utilizate de autoritățile de aplicare a legii sau în numele acestora pentru a prevedea apariția sau repetarea unei infracțiuni reale sau potențiale pe baza creării de profiluri ale persoanelor fizice, astfel cum se menționează la articolul 3 alineatul (4) din Directiva (UE) 2016/680, sau pentru a evalua trăsături și caracteristici de personalitate sau comportamentul infracțional anterior al unor persoane fizice sau grupuri;

(f) sisteme de IA destinate a fi utilizate de autoritățile de aplicare a legii sau în numele acestora pentru crearea de profiluri ale persoanelor fizice, astfel cum se menționează la articolul 3 alineatul (4) din Directiva (UE) 2016/680, în cursul depistării, investigării sau al urmăririi penale a infracțiunilor;

(g) [eliminat]

7. gestionarea migrației, a azilului și a controlului la frontiere:

(a) sisteme de IA destinate a fi utilizate de autoritățile publice competente sau în numele acestora drept poligrafe și instrumente similare sau pentru a detecta starea emoțională a unei persoane fizice;

(b) sisteme de IA destinate a fi utilizate de autoritățile publice competente sau în numele acestora pentru a evalua un risc, inclusiv un risc de securitate, un risc de migrație clandestină sau un risc pentru sănătate din partea unei persoane fizice care intenționează să intre sau care a intrat pe teritoriul unui stat membru;

(c) [eliminat]

(d) sisteme de IA destinate să fie utilizate de către autoritățile publice competente sau în numele acestora pentru a examina cererile de azil, de viză și de permise de ședere și plângerile aferente cu privire la eligibilitatea persoanelor fizice care solicită un statut;

8. administrarea justiției și procesele democratice:

(a) sisteme de IA menite să fie utilizate de către o autoritate judiciară sau în numele acesteia pentru a interpreta faptele sau legea, precum și pentru a aplica legea la un set concret de fapte.

ANEXA IV

DOCUMENTAȚIA TEHNICĂ menționată la articolul 11 alineatul (1)

Documentația tehnică menționată la articolul 11 alineatul (1) conține cel puțin următoarele informații, aplicabile sistemului de IA relevant:

1. o descriere generală a sistemului de IA, inclusiv:

   (a) scopul preconizat, persoana/persoanele care dezvoltă sistemul, data și versiunea sistemului;

   (b) modul în care sistemul de IA interacționează sau poate fi utilizat pentru a interacționa cu hardware-ul sau cu software-ul care nu face parte din sistemul de IA în sine, după caz;

   (c) versiunile software-ului sau ale firmware-ului relevant și orice cerință legată de actualizarea versiunilor;

   (d) descrierea tuturor formelor sub care sistemul de IA este introdus pe piață sau este pus în funcțiune [de exemplu, pachet software integrat în hardware, sistem care poate fi descărcat, interfață de programare a aplicațiilor („IPA”) etc.];

   (e) descrierea hardware-ului pe care urmează să funcționeze sistemul de IA;

   (f) în cazul în care sistemul de IA este o componentă a unor produse, fotografii sau ilustrații care prezintă caracteristici externe, marcajele și dispunerea internă a produselor respective;

   (g) instrucțiuni de utilizare pentru utilizator și, după caz, instrucțiuni de instalare;

2. o descriere detaliată a elementelor sistemului de IA și a procesului de dezvoltare a acestuia, inclusiv:

   (a) metodele și etapele parcurse pentru dezvoltarea sistemului de IA, inclusiv, dacă este cazul, recurgerea la sisteme sau instrumente antrenate anterior furnizate de terți și modul în care acestea au fost utilizate, integrate sau modificate de către furnizor;

(b) specificațiile de proiectare ale sistemului, și anume logica generală a sistemului de IA și a algoritmilor; principalele opțiuni de proiectare, inclusiv justificarea și ipotezele asumate, inclusiv în ceea ce privește persoanele sau grupurile de persoane pentru care se intenționează să fie utilizat sistemul, principalele opțiuni de clasificare; pentru ce anume este proiectat să fie optimizat sistemul și relevanța diverșilor parametri; descrierea rezultatelor preconizate ale sistemului; deciziile cu privire la orice posibil compromis făcut în ceea ce privește soluțiile tehnice adoptate în vederea conformării la cerințele prevăzute în titlul III capitolul 2;

(c) descrierea arhitecturii sistemului, care explică modul în care componentele de software se bazează una pe alta sau se alimentează reciproc și se integrează în prelucrarea generală; precum și resursele de calcul utilizate pentru dezvoltarea, antrenarea, testarea și validarea sistemului de IA;

(d) după caz, cerințele în materie de date în ceea ce privește fișele tehnice care descriu metodologiile și tehnicile de antrenare și seturile de date de antrenare utilizate, inclusiv o descriere generală a acestor seturi de date, informații privind proveniența, domeniul de aplicare și principalele caracteristici ale acestora; modul în care au fost obținute și selectate datele, proceduri de etichetare (de exemplu, pentru învățarea supervizată), metodologii de curățare a datelor (de exemplu, detectarea valorilor aberante);

(e) evaluarea măsurilor de supraveghere umană necesare în conformitate cu articolul 14, inclusiv o evaluare a măsurilor tehnice necesare pentru a facilita interpretarea rezultatelor sistemelor de IA de către utilizatori, în conformitate cu articolul 13 alineatul (3) litera (d);

(f) dacă este cazul, o descriere detaliată a modificărilor prestabilite ale sistemului de IA și ale performanței acestuia, împreună cu toate informațiile relevante referitoare la soluțiile tehnice adoptate pentru a asigura conformitatea continuă a sistemului de IA cu cerințele relevante prevăzute în titlul III capitolul 2;

(g) procedurile de validare și testare utilizate, inclusiv informații cu privire la datele de validare și testare utilizate și la principalele caracteristici ale acestora; indicatorii utilizați pentru a măsura precizia, robustețea, securitatea cibernetică și conformitatea cu alte cerințe relevante prevăzute în titlul III capitolul 2, precum și impactul potențial discriminatoriu; jurnale de testare și toate rapoartele de testare datate și semnate de persoanele responsabile, inclusiv în ceea ce privește modificările prestabilite menționate la litera (f);

3. informații detaliate privind monitorizarea, funcționarea și controlul sistemului de IA, în special în ceea ce privește: capacitățile și limitările sale legate de performanță, inclusiv gradele de acuratețe pentru anumite persoane sau grupuri de persoane pentru care se intenționează să se utilizeze sistemul respectiv, precum și nivelul general preconizat de acuratețe în raport cu scopul preconizat; rezultatele neintenționate previzibile și sursele de riscuri pentru sănătate, siguranță, drepturile fundamentale și pentru discriminare, având în vedere scopul preconizat al sistemului de IA; măsurile de supraveghere umană necesare în conformitate cu articolul 14, inclusiv măsurile tehnice necesare pentru a facilita interpretarea rezultatelor sistemelor de IA de către utilizatori; specificații privind datele de intrare, după caz;

4. o descriere detaliată a sistemului de gestionare a riscurilor în conformitate cu articolul 9;

5. o descriere a modificărilor relevante aduse de furnizor sistemului de-a lungul ciclului său de viață;

6. o listă a standardelor armonizate aplicate integral sau parțial, ale căror referințe au fost publicate în Jurnalul Oficial al Uniunii Europene, iar în cazul în care nu au fost aplicate astfel de standarde armonizate, o descriere detaliată a soluțiilor adoptate pentru a se îndeplini cerințele prevăzute în titlul III capitolul 2, inclusiv o listă a altor standarde și specificații tehnice relevante aplicate;

7. o copie a declarației de conformitate UE;

8. o descriere detaliată a sistemului existent pentru evaluarea performanței sistemului de IA în etapa ulterioară introducerii pe piață în conformitate cu articolul 61, inclusiv planul de monitorizare ulterioară introducerii pe piață menționat la articolul 61 alineatul (3).

ANEXA V

DECLARAȚIA DE CONFORMITATE UE

Declarația de conformitate UE menționată la articolul 48 conține toate informațiile următoare:

1. denumirea și tipul sistemului de IA și orice referință suplimentară lipsită de ambiguitate care permite identificarea și trasabilitatea sistemului de IA;

2. numele și adresa furnizorului sau, după caz, ale reprezentantului autorizat al acestuia;

3. o declarație potrivit căreia declarația de conformitate UE este emisă pe răspunderea exclusivă a furnizorului;

4. o declarație potrivit căreia sistemul de IA în cauză este conform cu prezentul regulament și, dacă este cazul, cu orice alt act legislativ relevant al Uniunii care prevede emiterea unei declarații de conformitate UE;

5. trimiteri la toate standardele armonizate relevante utilizate sau la orice altă specificație comună în legătură cu care se declară conformitatea;

6. după caz, denumirea și numărul de identificare ale organismului notificat, o descriere a procedurii de evaluare a conformității efectuate și identificarea certificatului eliberat;

7. locul și data emiterii declarației, numele și funcția persoanei care a semnat, precum și o indicație pentru cine și în numele cui semnează, semnătura.

ANEXA VI

PROCEDURA DE EVALUARE A CONFORMITĂȚII BAZATĂ PE CONTROL INTERN

1. Procedura de evaluare a conformității bazată pe control intern este procedura de evaluare a conformității realizată pe baza punctelor 2-4.

2. Furnizorul verifică dacă sistemul de management al calității instituit respectă cerințele de la articolul 17.

3. Furnizorul examinează informațiile conținute în documentația tehnică pentru a evalua conformitatea sistemului de IA cu cerințele esențiale relevante prevăzute în titlul III capitolul 2.

4. Furnizorul verifică, de asemenea, dacă procesul de proiectare și dezvoltare a sistemului de IA și monitorizarea ulterioară introducerii pe piață a acestuia, astfel cum se menționează la articolul 61, sunt în concordanță cu documentația tehnică.

ANEXA VII

EVALUAREA CONFORMITĂȚII PE BAZA UNUI SISTEM DE MANAGEMENT AL CALITĂȚII ȘI A EXAMINĂRII DOCUMENTAȚIEI TEHNICE

1. Introducere

Evaluarea conformității pe baza unui sistem de management al calității și a examinării documentației tehnice este procedura de evaluare a conformității realizată pe baza punctelor 2-5.

2. Prezentare generală

Sistemul de management al calității aprobat pentru proiectarea, dezvoltarea și testarea sistemelor de IA în temeiul articolului 17 este examinat în conformitate cu punctul 3 și face obiectul supravegherii menționate la punctul 5. Documentația tehnică a sistemului de IA se examinează în conformitate cu punctul 4.

3. Sistemul de management al calității

3.1. Cererea furnizorului include:

(a) numele și adresa furnizorului, iar, dacă cererea este depusă de către reprezentantul autorizat, și numele și adresa acestuia;

(b) lista sistemelor de IA care fac obiectul aceluiași sistem de management al calității;

(c) documentația tehnică a fiecărui sistem de IA pentru care se aplică același sistem de management al calității;

(d) documentația privind sistemul de management al calității care acoperă toate aspectele enumerate la articolul 17;

(e) o descriere a procedurilor instituite pentru a se asigura că sistemul de management al calității continuă să fie adecvat și eficace;

(f) o declarație scrisă care să specifice că nu a fost depusă o cerere identică la un alt organism notificat.

3.2. Sistemul de management al calității este evaluat de organismul notificat, care stabilește dacă acesta satisface cerințele menționate la articolul 17.

Decizia se notifică furnizorului sau reprezentantului autorizat al acestuia.

Notificarea respectivă trebuie să cuprindă concluziile evaluării sistemului de management al calității și decizia de evaluare motivată.

3.3. Sistemul de management al calității, astfel cum a fost aprobat, continuă să fie pus în aplicare și menținut de către furnizor astfel încât să rămână adecvat și eficient.

3.4. Orice modificare preconizată a sistemului aprobat de management al calității sau a listei sistemelor de IA acoperite de acesta din urmă este adusă la cunoștința organismului notificat, de către furnizor.

Modificările propuse sunt examinate de organismul notificat care decide dacă sistemul de management al calității modificat îndeplinește în continuare cerințele menționate la punctul 3.2 sau dacă este necesară o reevaluare.

Organismul notificat înștiințează furnizorul cu privire la decizia pe care a luat-o. Notificarea respectivă trebuie să cuprindă concluziile examinării modificărilor și decizia de evaluare motivată.

4. Controlul documentației tehnice

4.1. În plus față de cererea menționată la punctul 3, furnizorul depune o cerere la un organism notificat ales de acesta pentru evaluarea documentației tehnice referitoare la sistemul de IA pe care furnizorul intenționează să îl introducă pe piață sau să îl pună în funcțiune și care este acoperit de sistemul de management al calității menționat la punctul 3.

4.2. Cererea include:

(a) numele și adresa furnizorului;

(b) o declarație scrisă care să precizeze că nu a fost depusă o cerere identică la un alt organism notificat;

(c) documentația tehnică menționată în anexa IV.

4.3. Documentația tehnică este examinată de organismul notificat. Atunci când acest lucru este relevant și limitat la ceea ce este necesar pentru a-și îndeplini sarcinile, organismului notificat i se acordă acces deplin la seturile de date de antrenament, de validare și de testare utilizate inclusiv, dacă este cazul și sub rezerva unor garanții de securitate, prin interfețe de programare a aplicațiilor („IPA”) sau prin alte mijloace și instrumente tehnice relevante care permit accesul de la distanță.

4.4. La examinarea documentației tehnice, organismul notificat poate solicita furnizorului să prezinte dovezi suplimentare sau să efectueze teste suplimentare pentru a permite o evaluare adecvată a conformității sistemului de IA cu cerințele prevăzute în titlul III capitolul 2. Ori de câte ori organismul notificat nu este satisfăcut de testele efectuate de furnizor, organismul notificat efectuează direct teste adecvate, după caz.

4.5. Organismelor notificate li se acordă acces la codul sursă al sistemului de IA pe baza unei cereri motivate și numai atunci când sunt îndeplinite următoarele condiții cumulative:

(a) accesul la codul sursă este necesar pentru a evalua conformitatea sistemului de IA cu grad ridicat de risc cu cerințele prevăzute în titlul III capitolul 2 și

(b) procedurile de testare/audit și verificările bazate pe datele și documentația furnizate de furnizor au fost epuizate sau s-au dovedit insuficiente.

4.6. Decizia se notifică furnizorului sau reprezentantului autorizat al acestuia. Notificarea respectivă trebuie să cuprindă concluziile examinării documentației tehnice și decizia de evaluare motivată.

În cazul în care sistemul de IA este în conformitate cu cerințele prevăzute în titlul III capitolul 2, organismul notificat eliberează un certificat UE de evaluare a documentației tehnice. Certificatul indică numele și adresa furnizorului, concluziile examinării, condițiile (dacă există) de valabilitate și datele necesare de identificare a sistemului de IA.

Certificatul și anexele sale conțin toate informațiile relevante care să permită evaluarea conformității sistemului de IA și controlul sistemului de IA în timpul utilizării acestuia, după caz.

În cazul în care sistemul de IA nu este conform cu cerințele prevăzute în titlul III capitolul 2, organismul notificat refuză emiterea unui certificat de evaluare UE a documentației tehnice și, în consecință, informează solicitantul, indicând motivele detaliate ale refuzului său.

În cazul în care sistemul de IA nu îndeplinește cerința referitoare la datele utilizate pentru antrenarea sa, va fi necesară reantrenarea sistemului de IA înaintea depunerii cererii pentru o nouă evaluare a conformității. În acest caz, decizia motivată de evaluare a organismului notificat prin care se refuză eliberarea certificatului UE de evaluare a documentației tehnice conține considerații specifice privind datele de calitate utilizate pentru antrenarea sistemului de IA, în special cu privire la motivele neconformității.

4.7. Orice modificare a sistemului de IA care ar putea afecta conformitatea sistemului de IA cu cerințele sau cu scopul preconizat al acestuia este aprobată de organismul notificat care a eliberat certificatul UE de evaluare a documentației tehnice. Furnizorul informează organismul notificat în cauză cu privire la intenția sa de a introduce oricare dintre modificările menționate anterior sau în cazul în care ia cunoștință de apariția unor astfel de modificări. Organismul notificat evaluează modificările planificate și decide pentru care din acestea este necesară o nouă evaluare a conformității în concordanță cu articolul 43 alineatul (4) sau dacă acestea ar putea fi abordate prin intermediul unui supliment la certificatul UE de evaluare a documentației tehnice. În acest din urmă caz, organismul notificat evaluează modificările, îi notifică furnizorului decizia sa și, în cazul în care modificările sunt aprobate, îi eliberează un supliment la certificatul UE de evaluare a documentației tehnice.

5. Supravegherea sistemului de management al calității aprobat.

5.1. Scopul supravegherii efectuate de organismul notificat menționat la punctul 3 este de a asigura faptul că furnizorul îndeplinește în mod corespunzător termenii și condițiile sistemului de management al calității aprobat.

5.2. În scopul evaluării, furnizorul permite organismului notificat să aibă acces la sediul în care are loc proiectarea, dezvoltarea sau testarea sistemelor de IA. În plus, furnizorul comunică organismului notificat toate informațiile necesare.

5.3. Organismul notificat efectuează misiuni de audit periodice, pentru a se asigura că furnizorul menține și aplică sistemul de management al calității, și prezintă furnizorului un raport de audit. În contextul acestor audituri, organismul notificat poate efectua teste suplimentare ale sistemelor de IA pentru care a fost emis un certificat UE de evaluare a documentației tehnice.

ANEXA VIII

INFORMAȚIILE CARE TREBUIE PREZENTATE ODATĂ CU ÎNREGISTRAREA OPERATORILOR ȘI A SISTEMELOR DE IA CU GRAD RIDICAT DE RISC, ÎN CONFORMITATE CU ARTICOLUL 51

Furnizorii, reprezentanții autorizați și utilizatorii care sunt autorități, agenții sau organisme publice transmit informațiile menționate în partea I. Furnizorii sau, după caz, reprezentanții autorizați se asigură că informațiile privind sistemele lor de IA cu grad ridicat de risc menționate în partea II punctele 1-11 sunt complete, corecte și actualizate. Informațiile prevăzute în partea II punctul 12 sunt generate automat de baza de date.

Partea I. Informații privind operatorii (la înregistrarea operatorilor)

(-1) tipul de operator (furnizor, reprezentant autorizat sau utilizator);

1. numele, adresa și informațiile de contact ale furnizorului;

2. în cazul în care transmiterea informațiilor este efectuată de o altă persoană în numele operatorului, numele, adresa și datele de contact ale persoanei respective;

Partea II. informații referitoare la sistemul de IA cu grad ridicat de risc;

1. numele, adresa și informațiile de contact ale furnizorului;

2. numele, adresa și datele de contact ale reprezentantului autorizat, după caz;

3. denumirea comercială a sistemului de IA și orice referință suplimentară lipsită de ambiguitate care permite identificarea și trasabilitatea sistemului de IA;

4. descrierea scopului preconizat al sistemului de IA;

5. statutul sistemului de IA (pe piață sau în funcțiune; nu mai este pe piață/în funcțiune, retras);

6. tipul, numărul și data expirării certificatului eliberat de organismul notificat și numele sau numărul de identificare al organismului notificat respectiv, după caz;

7. o copie scanată a certificatului menționat la punctul 6, dacă este cazul;

8. statele membre în care sistemul de IA este sau a fost introdus pe piață, pus în funcțiune sau pus la dispoziție în Uniune;

9. o copie a declarației de conformitate UE prevăzută la articolul 48;

10. instrucțiuni de utilizare electronice;

11. URL pentru informații suplimentare (opțional).

12. numele, adresa și informațiile de contact ale utilizatorilor.

ANEXA VIIIa

INFORMAȚIILE CARE TREBUIE PREZENTATE ODATĂ CU ÎNREGISTRAREA SISTEMELOR DE IA CU GRAD RIDICAT DE RISC ENUMERATE ÎN ANEXA III ÎN LEGĂTURĂ CU TESTAREA ÎN CONDIȚII REALE, ÎN CONFORMITATE CU ARTICOLUL 54a

Se furnizează și, ulterior, se actualizează următoarele informații referitoare la testarea în condiții reale care urmează să fie înregistrate în conformitate cu articolul 54a:

(1) numărul unic de identificare la nivelul întregii Uniuni al testării în condiții reale;

(2) numele și datele de contact ale furnizorului sau ale potențialului furnizor și ale utilizatorilor implicați în testarea în condiții reale;

(3) o scurtă descriere a sistemului de IA, a scopului său preconizat și alte informații necesare pentru identificarea sistemului;

(4) un rezumat al principalelor caracteristici ale planului de testare în condiții reale;

(5) informații privind suspendarea sau încetarea testării în condiții reale.

ANEXA IX

LEGISLAȚIA UNIUNII PRIVIND SISTEMELE INFORMATICE LA SCARĂ LARGĂ ÎN SPAȚIUL DE LIBERTATE, SECURITATE ȘI JUSTIȚIE

1. Sistemul de informații Schengen

   (a) Regulamentul (UE) 2018/1860 al Parlamentului European și al Consiliului din 28 noiembrie 2018 privind utilizarea Sistemului de informații Schengen pentru returnarea resortisanților țărilor terțe aflați în situație de ședere ilegală (JO L 312, 7.12.2018, p. 1);

   (b) Regulamentul (UE) 2018/1861 al Parlamentului European și al Consiliului din 28 noiembrie 2018 privind instituirea, funcționarea și utilizarea Sistemului de informații Schengen (SIS) în domeniul verificărilor la frontiere, de modificare a Convenției de punere în aplicare a Acordului Schengen și de modificare și abrogare a Regulamentului (CE) nr. 1987/2006 (JO L 312, 7.12.2018, p. 14);

   (c) Regulamentul (UE) 2018/1862 al Parlamentului European și al Consiliului din 28 noiembrie 2018 privind instituirea, funcționarea și utilizarea Sistemului de informații Schengen (SIS) în domeniul cooperării polițienești și al cooperării judiciare în materie penală, de modificare și de abrogare a Deciziei 2007/533/JAI a Consiliului și de abrogare a Regulamentului (CE) nr. 1986/2006 al Parlamentului European și al Consiliului și a Deciziei 2010/261/UE a Comisiei (JO L 312, 7.12.2018, p. 56).

2. Sistemul de informații privind vizele

   (a) Propunere de REGULAMENT AL PARLAMENTULUI EUROPEAN ȘI AL CONSILIULUI de modificare a Regulamentului (CE) nr. 767/2008, a Regulamentului (CE) nr. 810/2009, a Regulamentului (UE) 2017/2226, a Regulamentului (UE) 2016/399, a Regulamentului XX/2018 [Regulamentul privind interoperabilitatea] și a Deciziei 2004/512/CE și de abrogare a Deciziei 2008/633/JAI a Consiliului – COM(2018) 302 final. A se actualiza după adoptarea regulamentului de către colegiuitori (aprilie/mai 2021).

3. Eurodac

(a) Propunere modificată de REGULAMENT AL PARLAMENTULUI EUROPEAN ȘI AL CONSILIULUI privind instituirea sistemului „Eurodac” pentru compararea datelor biometrice în scopul aplicării eficiente a Regulamentului (UE) XXX/XXX [Regulamentul privind gestionarea situațiilor legate de azil și migrație] și a Regulamentului (UE) XXX/XXX [Regulamentul privind relocarea], al identificării unui resortisant al unei țări terțe sau a unui apatrid în situație neregulamentară și privind cererile de comparare cu datele Eurodac prezentate de autoritățile de aplicare a legii din statele membre și de Europol în scopul asigurării respectării legii și de modificare a Regulamentelor (UE) 2018/1240 și (UE) 2019/818 – COM(2020) 614 final.

4. Sistemul de intrare/ieșire

(a) Regulamentul (UE) 2017/2226 al Parlamentului European și al Consiliului din 30 noiembrie 2017 de instituire a Sistemului de intrare/ieșire (EES) pentru înregistrarea datelor de intrare și de ieșire și a datelor referitoare la refuzul intrării ale resortisanților țărilor terțe care trec frontierele externe ale statelor membre, de stabilire a condițiilor de acces la EES în scopul aplicării legii și de modificare a Convenției de punere în aplicare a Acordului Schengen și a Regulamentelor (CE) nr. 767/2008 și (UE) nr. 1077/2011 (JO L 327, 9.12.2017, p. 20).

5. Sistemul european de informații și de autorizare privind călătoriile

(a) Regulamentul (UE) 2018/1240 al Parlamentului European și al Consiliului din 12 septembrie 2018 de instituire a Sistemului european de informații și de autorizare privind călătoriile (ETIAS) și de modificare a Regulamentelor (UE) nr. 1077/2011, (UE) nr. 515/2014, (UE) 2016/399, (UE) 2016/1624 și (UE) 2017/2226 (JO L 236, 19.9.2018, p. 1);

(b) Regulamentul (UE) 2018/1241 al Parlamentului European și al Consiliului din 12 septembrie 2018 de modificare a Regulamentului (UE) 2016/794 în scopul instituirii Sistemului european de informații și de autorizare privind călătoriile (ETIAS) (JO L 236, 19.9.2018, p. 72).

6. Sistemul european de informații cu privire la cazierele judiciare ale resortisanților țărilor terțe și apatrizilor

(a) Regulamentul (UE) 2019/816 al Parlamentului European și al Consiliului din 17 aprilie 2019 de stabilire a unui sistem centralizat pentru determinarea statelor membre care dețin informații privind condamnările resortisanților țărilor terțe și ale apatrizilor (ECRIS-TCN), destinat să completeze sistemul european de informații cu privire la cazierele judiciare, și de modificare a Regulamentului (UE) 2018/1726 (JO L 135, 22.5.2019, p. 1).

7. Interoperabilitate

(a) Regulamentul (UE) 2019/817 al Parlamentului European și al Consiliului din 20 mai 2019 privind instituirea unui cadru pentru interoperabilitatea dintre sistemele de informații ale UE în domeniul frontierelor și al vizelor (JO L 135, 22.5.2019, p. 27);

(b) Regulamentul (UE) 2019/818 al Parlamentului European și al Consiliului din 20 mai 2019 privind instituirea unui cadru pentru interoperabilitatea dintre sistemele de informații ale UE în domeniul cooperării polițienești și judiciare, al azilului și al migrației (JO L 135, 22.5.2019, p. 85).