UNIUNEA EUROPEANĂ

PARLAMENTUL EUROPEAN **CONSILIUL**

Bruxelles, 14 mai 2024
(OR. en)

2021/0106(COD) **PE-CONS 24/24**

TELECOM 54
JAI 238
COPEN 69
CYBER 37
DATAPROTECT 76
EJUSTICE 11
COSI 16
IXIM 49
ENFOPOL 63
RELEX 180
MI 151
COMPET 154
CODEC 412

ACTE LEGISLATIVE ȘI ALTE INSTRUMENTE

Subiect:	REGULAMENT AL PARLAMENTULUI EUROPEAN ȘI AL CONSILIULUI de stabilire a unor norme armonizate privind inteligența artificială și de modificare a Regulamentelor (CE) nr. 300/2008, (UE) nr. 167/2013, (UE) nr. 168/2013, (UE) 2018/858, (UE) 2018/1139 și (UE) 2019/2144 și a Directivelor 2014/90/UE, (UE) 2016/797 și (UE) 2020/1828 (Regulamentul privind inteligența artificială)

REGULAMENTUL (UE) 2024/…
AL PARLAMENTULUI EUROPEAN ȘI AL CONSILIULUI

din …

de stabilire a unor norme armonizate privind inteligența artificială
și de modificare a Regulamentelor (CE) nr. 300/2008, (UE) nr. 167/2013, (UE) nr. 168/2013, (UE) 2018/858, (UE) 2018/1139 și (UE) 2019/2144
și a Directivelor 2014/90/UE, (UE) 2016/797 și (UE) 2020/1828
(Regulamentul privind inteligența artificială)

(Text cu relevanță pentru SEE)

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 către parlamentele naționale,

având în vedere avizul Comitetului Economic și Social European[1],

având în vedere avizul Băncii Centrale Europene[2],

având în vedere avizul Comitetului Regiunilor[3],

hotărând în conformitate cu procedura legislativă ordinară[4],

---

1 JO C 517, 22.12.2021, p. 56.
2 JO C 115, 11.3.2022, p. 5.
3 JO C 97, 28.2.2022, p. 60.
4 Poziția Parlamentului European din 13 martie 2024 (nepublicată încă în Jurnalul Oficial) și Decizia Consiliului din …

întrucât:

(1) Scopul prezentului regulament este de a îmbunătăți funcționarea pieței interne prin stabilirea unui cadru juridic uniform, în special pentru dezvoltarea, introducerea pe piață, punerea în funcțiune și utilizarea de sisteme de inteligență artificială (sisteme de IA) în Uniune, în conformitate cu valorile Uniunii, de a promova adoptarea unei inteligențe artificiale (IA) de încredere și centrate pe factorul uman, asigurând în același timp un nivel ridicat de protecție a sănătății, a siguranței, a drepturilor fundamentale consacrate în Carta drepturilor fundamentale a Uniunii Europene (denumită în continuare „Carta”), inclusiv a democrației, a statului de drept și a mediului, de a proteja împotriva efectelor dăunătoare ale sistemelor de IA în Uniune, precum și de a sprijini inovarea. Prezentul regulament 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) Prezentul regulament ar trebui să se aplice în conformitate cu valorile Uniunii consacrate în cartă, facilitând protecția persoanelor fizice, a întreprinderilor, a democrației, a statului de drept și a mediului, stimulând în același timp inovarea și ocuparea forței de muncă și asigurând Uniunii o poziție de lider în adoptarea unei IA de încredere.

(3) Sistemele de IA pot fi implementate cu ușurință într-o mare varietate de sectoare ale economiei și în multe părți ale societății, inclusiv la nivel transfrontalier, și pot circula cu ușurință în întreaga Uniune. Anumite state membre au explorat deja adoptarea unor norme naționale pentru a se asigura că IA este sigură și de încredere și că este dezvoltată și utilizată în conformitate cu obligațiile în materie de drepturi fundamentale. Divergențele dintre normele naționale 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 pentru a se obține o IA de încredere, iar divergențele care împiedică libera circulație, inovarea, implementarea și adoptarea sistemelor de IA și a produselor și serviciilor conexe în cadrul pieței interne ar trebui să fie 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 de protecție a persoanelor fizice în contextul prelucrării datelor cu caracter personal, referitoare la restricțiile de utilizare a sistemelor de IA pentru identificarea biometrică la distanță în scopul aplicării legii, la utilizarea sistemelor de IA pentru evaluarea riscurilor persoanelor fizice în scopul aplicării legii și la utilizarea sistemelor de IA de clasificare biometrică în scopul aplicării legii, este oportun ca prezentul regulament să se întemeieze, în ceea ce privește normele specifice respective, pe articolul 16 din TFUE. Având în vedere normele specifice respective și recurgerea la articolul 16 din TFUE, este oportun să se consulte Comitetul european pentru protecția datelor.

(4) IA este o familie de tehnologii cu evoluție rapidă, care contribuie la o gamă largă de beneficii economice, de mediu 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 fizice și organizații, utilizarea IA poate oferi avantaje concurențiale esențiale întreprinderilor și poate sprijini obținerea de rezultate benefice din punct de vedere social și al mediului, în domenii precum îngrijirile de sănătate, agricultura, siguranța alimentară, educația și formarea, mass-media, sportul, cultura, gestionarea infrastructurii, energia, transporturile și logistica, serviciile publice, securitatea, justiția, eficiența energetică și a utilizării resurselor, monitorizarea mediului, conservarea și refacerea biodiversității și ecosistemelor, precum și atenuarea schimbărilor climatice și adaptarea la acestea.

(5) În același timp, în funcție de circumstanțele legate de aplicarea și utilizarea sa specifică, precum și de nivelul său specific de dezvoltare tehnologică, IA poate genera riscuri și poate aduce prejudicii intereselor publice și drepturilor fundamentale care sunt protejate de dreptul Uniunii. Un astfel de prejudiciu ar putea fi material sau moral, inclusiv de natură fizică, psihologică, societală sau economică.

(6) Având în vedere impactul major pe care IA îl poate avea asupra societății și necesitatea de a genera încredere, este esențial ca IA și cadrul său de reglementare să fie dezvoltate în concordanță cu valorile Uniunii consacrate la articolul 2 din Tratatul privind Uniunea Europeană (TUE) și cu drepturile și libertățile fundamentale consacrate în tratate și, potrivit articolului 6 din TUE, în Cartă. Ca o condiție prealabilă, IA ar trebui să fie o tehnologie centrată pe factorul uman. Aceasta ar trebui să le servească oamenilor ca un instrument, cu scopul final de a le spori bunăstarea.

(7) Pentru a asigura un nivel consecvent și ridicat de protecție a intereselor publice în ceea ce privește sănătatea, siguranța și drepturile fundamentale, ar trebui să fie stabilite norme comune pentru sistemele de IA cu grad ridicat de risc. Normele respective ar trebui să fie în concordanță cu carta și ar trebui să fie nediscriminatorii și în conformitate cu angajamentele comerciale internaționale ale Uniunii. De asemenea, ele ar trebui să țină seama de Declarația europeană privind drepturile și principiile digitale pentru deceniul digital și de Orientările în materie de etică pentru o IA fiabilă ale Grupului independent de experți la nivel înalt privind inteligența artificială.

(8) Prin urmare, este necesar un cadru juridic al Uniunii care să stabilească norme armonizate privind IA pentru a încuraja dezvoltarea, utilizarea și adoptarea pe piața internă a IA și care să asigure, în același timp, un nivel ridicat de protecție a intereselor publice, cum ar fi sănătatea și siguranța, și protecția drepturilor fundamentale, inclusiv a democrației, a statului de drept și a mediului, astfel cum sunt recunoscute și protejate de dreptul Uniunii. Pentru atingerea acestui obiectiv, ar trebui să fie stabilite norme care să reglementeze introducerea pe piață, punerea în funcțiune și utilizarea anumitor sisteme de IA, asigurând astfel buna funcționare a pieței interne și permițând sistemelor respective să beneficieze de principiul liberei circulații a bunurilor și a serviciilor. Normele respective ar trebui să fie clare și solide în ceea ce privește protejarea drepturilor fundamentale, sprijinind noile soluții inovatoare, permițând unui ecosistem european de actori publici și privați să creeze sisteme de IA în conformitate cu valorile Uniunii și deblocând potențialul transformării digitale în toate regiunile Uniunii. Prin stabilirea normelor respective, precum și a unor măsuri de susținere a inovării cu un accent special pe întreprinderile mici și mijlocii (IMM), inclusiv pe întreprinderile nou-înființate, prezentul regulament sprijină obiectivul de promovare a abordării europene centrate pe factorul uman față de IA și de poziționare ca lider mondial în dezvoltarea unei IA sigure, de încredere și etice, astfel cum a afirmat Consiliul European[5], și asigură protecția principiilor etice, astfel cum a solicitat în mod expres Parlamentul European[6].

---

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

6 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).

(9) Normele armonizate 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[7], cu Decizia nr. 768/2008/CE a Parlamentului European și a Consiliului[8] și cu Regulamentul (UE) 2019/1020 al Parlamentului European și al Consiliului[9] (denumite în continuare „noul cadru legislativ”). Normele armonizate prevăzute în prezentul regulament ar trebui să se aplice în toate sectoarele și, în conformitate cu noul cadru legislativ, ar trebui să nu aducă atingere dreptului în vigoare al Uniunii, în special în ceea ce privește protecția datelor, protecția consumatorilor, drepturile fundamentale, ocuparea forței de muncă, protecția lucrătorilor 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 asupra cărora sistemele de IA ar putea avea un impact negativ, inclusiv în ceea ce privește despăgubirea pentru eventuale prejudicii prevăzută în Directiva 85/374/CEE a Consiliului[10], rămân neafectate și pe deplin aplicabile.

---

7 Regulamentul (CE) nr. 765/2008 al Parlamentului European și al Consiliului din 9 iulie 2008 de stabilire a cerințelor de acreditare și de abrogare a Regulamentului (CEE) nr. 339/93 (JO L 218, 13.8.2008, p. 30).

8 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).

9 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 (JO L 169, 25.6.2019, p. 1).

10 Directiva 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 (JO L 210, 7.8.1985, p. 29).

În plus, în contextul ocupării forței de muncă și al protecției lucrătorilor, prezentul regulament ar trebui așadar să nu aducă atingere dreptului Uniunii privind politica socială și dreptului național al muncii, în conformitate cu dreptul Uniunii, în ceea ce privește condițiile de angajare și de muncă, inclusiv securitatea și sănătatea în muncă și relația dintre angajatori și lucrători. De asemenea, prezentul regulament ar trebui să nu aducă atingere exercitării drepturilor fundamentale, astfel cum sunt recunoscute în statele membre și la nivelul Uniunii, inclusiv dreptului sau libertății de a intra în grevă sau de a întreprinde alte acțiuni care țin de sistemele specifice de relații de muncă din statele membre, precum și dreptului de a negocia, de a încheia și de a pune în aplicare contracte colective de muncă sau de a desfășura acțiuni colective în conformitate cu dreptul intern. Prezentul regulament ar trebui să nu aducă atingere dispozițiilor care vizează îmbunătățirea condițiilor de muncă în ceea ce privește munca prin intermediul platformelor, prevăzute într-o Directivă a Parlamentului European și a Consiliului privind îmbunătățirea condițiilor de muncă pentru lucrul prin intermediul platformelor. 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. De asemenea, 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 dreptul respectiv nu intră în domeniul de aplicare al prezentului regulament sau urmărește alte obiective legitime de interes public decât cele urmărite de prezentul regulament. De exemplu, dreptul intern al muncii și dreptul intern privind protecția minorilor, și anume a persoanelor cu vârsta sub 18 ani, ținând seama de Comentariul general nr. 25 (2021) la Convenția UNCRC cu privire la drepturile copiilor în legătură cu mediul digital, în măsura în care nu sunt specifice sistemelor de IA și urmăresc alte obiective legitime de interes public, ar trebui să nu fie afectate de prezentul regulament.

(10) Dreptul fundamental la protecția datelor cu caracter personal este protejat în special de Regulamentele (UE) 2016/679[11] și (UE) 2018/1725[12] ale Parlamentului European și ale Consiliului și de Directiva (UE) 2016/680 a Parlamentului European și a Consiliului[13]. Directiva 2002/58/CE a Parlamentului European și a Consiliului[14] protejează, în plus, viața privată și confidențialitatea comunicațiilor, inclusiv prin faptul că prevede condiții pentru stocarea și accesarea pe echipamente terminale a oricăror date cu și fără caracter personal. Respectivele acte legislative ale Uniunii asigură temeiul prelucrării durabile și responsabile a datelor, inclusiv atunci când seturile de date conțin un amestec de date cu caracter personal și date fără caracter personal. Prezentul regulament nu urmărește să aducă atingere aplicării dreptului în vigoare al Uniunii care reglementează prelucrarea datelor cu caracter personal, nici sarcinilor și competențelor autorităților de supraveghere independente care sunt competente să monitorizeze respectarea instrumentelor respective.

---

11 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).

12 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).

13 Directiva (UE) 2016/680 a Parlamentului European și a Consiliului din 27 aprilie 2016 privind protecția persoanelor fizice referitor la prelucrarea datelor cu caracter personal de către autoritățile competente în scopul prevenirii, depistării, investigării sau urmăririi penale a infracțiunilor sau al executării pedepselor și privind libera circulație a acestor date și de abrogare a Deciziei-cadru 2008/977/JAI a Consiliului (JO L 119, 4.5.2016, p. 89).

14 Directiva 2002/58/CE a Parlamentului European și a Consiliului din 12 iulie 2002 privind prelucrarea datelor personale și protejarea confidențialității în sectorul comunicațiilor publice (Directiva asupra confidențialității și comunicațiilor electronice) (JO L 201, 31.7.2002, p. 37).

Prezentul regulament nu aduce atingere nici obligațiilor furnizorilor și implementatorilor de sisteme de IA în rolul lor de operatori de date sau de persoane împuternicite de operatori, care decurg din dreptul Uniunii sau din dreptul național 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 că persoanele vizate continuă să beneficieze de toate drepturile și garanțiile care le sunt acordate de dreptul Uniunii, printre care se numără drepturile legate de procesul decizional individual complet automatizat, inclusiv 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 efectivă 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.

(11) Prezentul regulament ar trebui să nu aducă atingere dispozițiilor privind răspunderea furnizorilor de servicii intermediare prevăzute în Regulamentul (UE) 2022/2065 al Parlamentului European și al Consiliului[15].

[15] Regulamentul (UE) 2022/2065 al Parlamentului European și al Consiliului din 19 octombrie 2022 privind o piață unică pentru serviciile digitale și de modificare a Directivei 2000/31/CE (Regulamentul privind serviciile digitale) (JO L 277, 27.10.2022, p. 1).

(12) Noțiunea de „sistem de IA” din prezentul regulament ar trebui să fie definită în mod clar și ar trebui să fie aliniată îndeaproape la lucrările organizațiilor internaționale care își desfășoară activitatea în domeniul IA, pentru a asigura securitatea juridică și a facilita convergența internațională și acceptarea pe scară largă, oferind în același timp flexibilitatea necesară pentru a ține seama de evoluțiile tehnologice rapide din acest domeniu. În plus, definiția ar trebui să se bazeze pe caracteristicile esențiale ale sistemelor de IA, care le diferențiază de sistemele software sau abordările de programare tradiționale mai simple, și nu ar trebui să acopere sistemele care se bazează pe reguli definite exclusiv de persoane fizice pentru a executa în mod automat anumite operațiuni. O caracteristică esențială a sistemelor de IA este capabilitatea lor de a realiza deducții. Această capabilitate se referă la procesul de obținere a rezultatelor, cum ar fi previziuni, conținut, recomandări sau decizii, care pot influența mediile fizice și virtuale, precum și la capabilitatea sistemelor de IA de a deriva modele sau algoritmi, sau ambele, din date sau din datele de intrare. Printre tehnicile folosite în timpul conceperii unui sistem de IA care fac posibilă realizarea de deducții se numără abordările bazate pe învățarea automată, care presupun a învăța, pe baza datelor, cum pot fi atinse anumite obiective, și abordările bazate pe logică și pe cunoaștere, care presupun realizarea de deducții pornind de la cunoștințe codificate sau de la reprezentarea simbolică a sarcinii de rezolvat. Capacitatea unui sistem de IA de a realiza deducții depășește simpla prelucrare de date, făcând posibile învățarea, raționamentul sau modelarea. Termenul „bazat pe calculator” se referă la faptul că sistemele de IA rulează pe calculatoare.

Trimiterea la obiective explicite sau implicite subliniază faptul că sistemele de IA pot funcționa în conformitate cu obiective definite explicite sau cu obiective implicite. Obiectivele sistemului de IA pot fi diferite de scopul preconizat al sistemului de IA într-un context specific. În sensul prezentului regulament, mediile ar trebui să fie înțelese ca fiind contextele în care funcționează sistemele de IA, în timp ce rezultatele generate de sistemele de IA reflectă diferitele funcții îndeplinite de acestea și includ previziuni, conținut, recomandări sau decizii. Sistemele de IA sunt concepute pentru a funcționa cu diferite niveluri de autonomie, ceea ce înseamnă că au un anumit grad de independență a acțiunilor față de implicarea umană și anumite capabilități de a funcționa fără intervenție umană. Adaptabilitatea de care un sistem de IA ar putea da dovadă după implementare se referă la capabilitățile de autoînvățare, care permit sistemului să se modifice în timpul utilizării. Sistemele de IA 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).

(13) Noțiunea de „implementator” menționată în prezentul regulament ar trebui să fie interpretată ca făcând referire la orice persoană fizică sau juridică, inclusiv la o autoritate publică, o agenție sau un alt organism, care utilizează un sistem de IA aflat sub autoritatea sa, cu excepția cazului în care sistemul de IA este utilizat în cursul unei activități personale, fără caracter profesional. În funcție de tipul de sistem de IA, utilizarea sistemului poate afecta alte persoane decât implementatorul.

(14) Noțiunea de „date biometrice” utilizată în prezentul regulament ar trebui să fie interpretată în concordanță cu noțiunea de „date biometrice”, astfel cum este definită la articolul 4 punctul 14 din Regulamentul (UE) 2016/679, la articolul 3 punctul 18 din Regulamentul (UE) 2018/1725 și la articolul 3 punctul 13 din Directiva (UE) 2016/680. Datele biometrice pot permite autentificarea, identificarea sau clasificarea persoanelor fizice, precum și recunoașterea emoțiilor acestora.

(15) Noțiunea de „identificare biometrică” menționată în prezentul regulament ar trebui să fie definită drept recunoașterea automată a unor trăsături umane fizice, fiziologice și comportamentale, precum fața, mișcările ochilor, forma corpului, vocea, intonația, mersul, postura, frecvența cardiacă, tensiunea arterială, mirosul, particularitățile de tastare, în scopul de a stabili identitatea unei persoane comparând datele biometrice ale persoanei respective cu date biometrice ale unor persoane stocate într-o bază de date de referință, indiferent dacă persoana în cauză și-a dat sau nu consimțământul. Nu se încadrează aici sistemele de IA destinate a fi utilizate pentru verificarea biometrică, care include autentificarea, al căror unic scop este de a confirma că o anumită persoană fizică este persoana care susține că este și de a confirma identitatea unei persoane fizice cu unicul scop de a-i permite accesul la un serviciu, deblocarea unui dispozitiv sau accesul securizat într-o incintă.

(16) Noțiunea de „clasificare biometrică” menționată în prezentul regulament ar trebui să fie definită drept încadrarea persoanelor fizice în categorii specifice pe baza datelor lor biometrice. Astfel de categorii specifice se pot referi la aspecte precum sexul, vârsta, culoarea părului, culoarea ochilor, tatuajele, trăsăturile comportamentale sau de personalitate, limba, religia, apartenența la o minoritate națională, orientarea sexuală sau politică. Nu se încadrează aici sistemele de clasificare biometrică care constituie un element pur auxiliar legat intrinsec de un alt serviciu comercial, ceea ce înseamnă că, din motive tehnice obiective, elementul respectiv nu poate fi utilizat fără serviciul principal, iar integrarea acelui element sau a acelei funcționalități nu este un mijloc de a eluda aplicabilitatea normelor prezentului regulament. De exemplu, filtrele care clasifică caracteristicile faciale sau corporale utilizate pe piețele online ar putea constitui un astfel de element auxiliar, deoarece pot fi utilizate numai în legătură cu serviciul principal care constă în vânzarea unui produs, permițând consumatorului să vizualizeze cum ar arăta produsul pe el însuși și ajutându-l să ia o decizie de cumpărare. Filtrele utilizate în cadrul serviciilor de rețele de socializare care clasifică caracteristicile faciale sau corporale pentru a permite utilizatorilor să adauge sau să modifice fotografii sau materiale video ar putea, de asemenea, să fie considerate elemente auxiliare, deoarece un astfel de filtru nu poate fi utilizat fără serviciul principal de rețea de socializare care constă în partajarea de conținut online.

(17) Noțiunea de „sistem de identificare biometrică la distanță” menționată în prezentul regulament ar trebui să fie definită din punct de vedere funcțional ca fiind un sistem de IA destinat identificării persoanelor fizice fără implicarea activă a acestora, de regulă de la distanță, prin compararea datelor biometrice ale unei persoane cu datele biometrice conținute într-o bază de date de referință, indiferent de tehnologia specifică, procesele specifice sau tipurile specifice de date biometrice utilizate. Astfel de sisteme de identificare biometrică la distanță sunt utilizate, de regulă, pentru a percepe mai multe persoane sau comportamentul acestora simultan, cu scopul de a facilita în mod semnificativ identificarea persoanelor fizice fără implicarea lor activă. Nu se încadrează aici sistemele de IA destinate a fi utilizate pentru verificarea biometrică, care include autentificarea, al căror unic scop este de a confirma că o anumită persoană fizică este persoana care susține că este și de a confirma identitatea unei persoane fizice cu unicul scop de a-i permite accesul la un serviciu, deblocarea unui dispozitiv sau accesul securizat într-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 pot fi utilizate pentru prelucrarea datelor biometrice ale unui număr mare de persoane fără implicarea lor activă. 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. În acest caz sunt utilizate 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.

(18) Noțiunea de „sistem de recunoaștere a emoțiilor” menționată în prezentul regulament ar trebui să fie definită ca un sistem de IA destinat identificării sau deducerii emoțiilor sau intențiilor persoanelor fizice pe baza datelor lor biometrice. Noțiunea se referă la emoții sau intenții precum fericirea, tristețea, furia, surpriza, dezgustul, stânjeneala, entuziasmul, rușinea, disprețul, satisfacția și amuzamentul. Nu sunt incluse stări fizice, cum ar fi durerea sau oboseala, inclusiv, de exemplu, sistemele utilizate pentru detectarea stării de oboseală a piloților sau conducătorilor auto profesioniști în scopul prevenirii accidentelor. De asemenea, nu este inclusă simpla detectare a expresiilor, gesturilor sau mișcărilor evidente, decât dacă sunt utilizate pentru identificarea sau deducerea emoțiilor. Expresiile respective pot fi expresii faciale de bază, cum ar fi o încruntătură sau un zâmbet, ori gesturi, cum ar fi mișcarea mâinilor, a brațelor sau a capului, ori caracteristici ale vocii unei persoane, cum ar fi o voce ridicată sau vorbitul în șoaptă.

(19) În sensul prezentului regulament, noțiunea de „spațiu accesibil publicului” ar trebui să fie înțeleasă ca referindu-se la orice spațiu fizic accesibil unui număr nedeterminat de persoane fizice, indiferent dacă spațiul în cauză este proprietate privată sau publică și indiferent de activitatea pentru care poate fi utilizat spațiul, cum ar fi comerț, de exemplu, magazine, restaurante, cafenele; servicii, de exemplu, bănci, activități profesionale, structuri de primire turistică; sport, de exemplu, piscine, săli de sport, stadioane; transporturi, de exemplu, stații de autobuz și de metrou, gări, aeroporturi, mijloace de transport; divertisment, de exemplu, cinematografe, teatre, muzee, săli de concerte și de conferințe, agrement sau altele, de exemplu, drumuri și piețe publice, parcuri, păduri, terenuri de joacă. Totodată, un spațiu ar trebui să fie 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 condiția de a avea o anumită vârstă. În schimb, un spațiu 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 spațiului. Simpla posibilitate de acces (cum ar fi o ușă descuiată sau o poartă deschisă într-un gard) nu implică faptul că spațiul 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 spații care nu sunt accesibile publicului. Spațiile accesibile publicului nu ar trebui să includă închisorile sau punctele de control la frontieră. Alte spații pot cuprinde atât spații accesibile publicului, cât și spații care nu sunt 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 sunt nici ele vizate, 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.

(20) Pentru a obține beneficii cât mai mari de pe urma sistemelor de IA, protejând în același timp drepturile fundamentale, sănătatea și siguranța, și pentru a permite controlul democratic, alfabetizarea în domeniul IA ar trebui să le ofere furnizorilor, implementatorilor și persoanelor afectate noțiunile necesare pentru a lua decizii în cunoștință de cauză cu privire la sistemele de IA. Aceste noțiuni pot varia în funcție de contextul relevant și pot include înțelegerea aplicării corecte a elementelor tehnice în faza de dezvoltare a sistemului de IA, măsurile care trebuie aplicate în timpul utilizării sale, modalitățile adecvate de interpretare a rezultatelor sistemului de IA și, în cazul persoanelor afectate, cunoștințele necesare pentru a înțelege impactul pe care îl vor avea asupra lor deciziile luate cu ajutorul IA. În contextul aplicării prezentului regulament, alfabetizarea în domeniul IA ar trebui să ofere tuturor actorilor relevanți din lanțul valoric al IA informațiile necesare pentru a asigura conformitatea adecvată și aplicarea corectă a regulamentului. În plus, punerea în aplicare pe scară largă a măsurilor de alfabetizare în domeniul IA și introducerea unor acțiuni subsecvente adecvate ar putea contribui la îmbunătățirea condițiilor de muncă și, în cele din urmă, ar putea susține consolidarea unei IA de încredere și inovarea în acest domeniu în Uniune. Comitetul european pentru inteligența artificială (denumit în continuare „comitetul”) ar trebui să sprijine Comisia pentru a promova instrumente de alfabetizare în domeniul IA, sensibilizarea publicului și înțelegerea beneficiilor, a riscurilor, a garanțiilor, a drepturilor și a obligațiilor care decurg din utilizarea sistemelor de IA. În cooperare cu părțile interesate relevante, Comisia și statele membre ar trebui să faciliteze elaborarea unor coduri de conduită voluntare pentru a promova alfabetizarea în domeniul IA în rândul persoanelor care se ocupă de dezvoltarea, exploatarea și utilizarea IA.

(21) 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 implementatorilor de sisteme de IA stabiliți în Uniune.

(22) 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 într-o țară terță în legătură cu o activitate care urmează să fie desfășurată de un sistem de IA care s-ar califica drept prezentând un grad ridicat de risc. În aceste circumstanțe, sistemul de IA utilizat de operator într-o țară terță ar putea prelucra date colectate în Uniune și transferate din Uniune în mod legal și ar putea furniza operatorului contractant din Uniune rezultatele produse de sistemul de IA respectiv ca urmare a prelucrării respective, fără ca sistemul 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 implementatorilor de sisteme de IA care sunt stabiliți într-o țară terță, în măsura în care rezultatele produse de sistemele respective sunt destinate a fi utilizate 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 acestea acționează în cadrul acordurilor internaționale sau de cooperare încheiate la nivelul Uniunii sau la nivel național pentru cooperarea în materie de aplicare a legii și cooperarea judiciară cu Uniunea sau cu statele membre, cu condiția ca țara terță sau organizația internațională relevantă să ofere garanții adecvate în ceea ce privește protecția drepturilor și libertăților fundamentale ale persoanelor. După caz, acest lucru s-ar putea aplica activităților desfășurate de entitățile cărora țările terțe le-au încredințat îndeplinirea unor sarcini specifice în sprijinul unei astfel de cooperări judiciare și în materie de aplicare a legii. Cadrele de cooperare sau acordurile sus-menționate au fost încheiate bilateral între statele membre și țări terțe sau între Uniunea Europeană, Europol sau alte agenții ale Uniunii, pe de o parte, și țări terțe sau organizații internaționale, pe de altă parte. Autoritățile competente cu supravegherea autorităților de aplicare a legii și a autorităților judiciare în temeiul prezentului regulament ar trebui să evalueze dacă respectivele cadre de cooperare sau acorduri internaționale includ garanții adecvate în ceea ce privește protecția drepturilor și libertăților fundamentale ale persoanelor. Autoritățile naționale destinatare și instituțiile, organele, oficiile și agențiile Uniunii care utilizează astfel de rezultate în Uniune rămân responsabile pentru asigurarea faptului că utilizarea lor respectă dreptul Uniunii. La revizuirea acordurilor internaționale respective sau la încheierea unor acorduri noi în viitor, părțile contractante ar trebui să depună toate eforturile pentru a alinia acordurile respective la cerințele prezentului regulament.

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

(24) În cazul și în măsura în care sistemele de IA sunt introduse pe piață, puse în funcțiune sau utilizate cu sau fără modificarea lor în scopuri militare, de apărare sau de securitate națională, sistemele respective ar trebui să fie 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 a statelor membre și ale politicii de apărare comune a Uniunii, care intră sub incidența titlului V capitolul 2 din TUE; acestea fac obiectul dreptului internațional public, care este, prin urmare, cadrul juridic mai adecvat pentru reglementarea sistemelor de IA în contextul utilizării forței letale și a 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) din 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 acestui cadru în alte scopuri, de exemplu în scopuri civile sau umanitare, de aplicare a 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 de IA în alte scopuri decât cele militare, de apărare sau de securitate națională ar trebui să asigure conformitatea sistemului de IA 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 care face obiectul excluderii, și anume în scop militar, de apărare sau de securitate națională, și pentru unul sau mai multe scopuri care nu fac obiectul excluderii, de exemplu în scopuri civile sau de aplicare a legii, intră în domeniul de aplicare al prezentului regulament, iar furnizorii sistemelor respective 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, utilizare care este exclusă din domeniul de aplicare al prezentului regulament. Un sistem de IA introdus pe piață în scopuri civile sau de aplicare a 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.

(25) Prezentul regulament ar trebui să sprijine inovarea, ar trebui să respecte libertatea științei și nu ar trebui să submineze activitatea de cercetare și dezvoltare. Prin urmare, este necesar să se excludă din domeniul său de aplicare sistemele și modelele de IA dezvoltate și puse în funcțiune în mod specific în scopul unic al cercetării și dezvoltării științifice. În plus, este necesar să se asigure că prezentul regulament nu afectează într-un alt mod activitatea de cercetare și dezvoltare științifică privind sistemele sau modelele de IA înainte de a fi introduse pe piață sau puse în funcțiune. În ceea ce privește activitatea de cercetare, testare și dezvoltare orientată spre produse aferentă sistemelor sau modelelor de IA, dispozițiile prezentului regulament nu ar trebui, de asemenea, să se aplice înainte ca aceste sisteme și modele să fie puse în funcțiune sau introduse pe piață. Această excludere nu aduce atingere obligației de a respecta prezentul regulament în cazul în care 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 în domeniul IA și testarea în condiții reale. În plus, fără a aduce atingere excluderii sistemelor de IA dezvoltate și puse în funcțiune în mod specific 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 caz, toate activitățile de cercetare și dezvoltare ar trebui să se desfășoare în conformitate cu standardele etice și profesionale recunoscute pentru cercetarea științifică, precum și în conformitate cu dreptul aplicabil al Uniunii.

(26) Pentru a introduce un set proporțional și eficace de norme obligatorii pentru sistemele de IA, ar trebui să fie 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 IA care sunt inacceptabile, 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.

(27) Deși abordarea bazată pe riscuri reprezintă temelia pentru un set proporțional și eficace de norme obligatorii, este important să se reamintească Orientările în materie de etică pentru o IA fiabilă din 2019, elaborate de Grupul independent de experți la nivel înalt privind IA numit de Comisie. În orientările respective, grupul de experți a elaborat șapte principii etice fără caracter obligatoriu pentru IA, care sunt menite să contribuie la asigurarea faptului că IA este de încredere și că este solidă din punct de vedere etic. Cele șapte principii sunt: implicarea și supravegherea umană; robustețea tehnică și siguranța; respectarea vieții private și guvernanța datelor; transparența; diversitatea, nediscriminarea și echitatea; bunăstarea socială și de mediu și asumarea răspunderii. Fără a aduce atingere cerințelor obligatorii din punct de vedere juridic prevăzute în prezentul regulament și în orice alt act legislativ aplicabil al Uniunii, aceste orientări contribuie la conceperea unei IA coerente, de încredere și centrate pe factorul uman, în conformitate cu carta și cu valorile pe care se întemeiază Uniunea. Potrivit orientărilor Grupului de experți la nivel înalt privind IA, implicarea și supravegherea umană înseamnă că sistemele de IA sunt dezvoltate și utilizate ca un instrument ce servește oamenilor, respectă demnitatea umană și autonomia personală și funcționează într-un mod care poate fi controlat și supravegheat în mod corespunzător de către oameni.

Robustețea tehnică și siguranța înseamnă că sistemele de IA sunt dezvoltate și utilizate într-un mod care asigură robustețea în caz de probleme și reziliența la încercările de a modifica utilizarea sau performanța sistemului de IA în vederea permiterii utilizării ilegale de către terți și care reduce la minimum prejudiciile neintenționate. Respectarea vieții private și guvernanța datelor înseamnă că sistemele de IA sunt dezvoltate și utilizate în conformitate cu normele privind protecția vieții private și a datelor și că, în același timp, se prelucrează date care respectă standarde ridicate de calitate și de integritate. Transparența înseamnă că sistemele de IA sunt dezvoltate și utilizate într-un mod care permite trasabilitatea și explicabilitatea adecvate, aducând totodată la cunoștința oamenilor faptul că interacționează sau comunică cu un sistem de IA și informând în mod corespunzător implementatorii cu privire la capabilitățile și limitele respectivului sistem de IA și persoanele afectate cu privire la drepturile lor. Diversitatea, nediscriminarea și echitatea înseamnă că sistemele de IA sunt dezvoltate și utilizate într-un mod care presupune implicarea a diverși actori și promovează accesul egal, egalitatea de gen și diversitatea culturală, evitând totodată efectele discriminatorii și prejudecățile inechitabile interzise prin dreptul Uniunii sau dreptul intern. Bunăstarea socială și de mediu înseamnă că sistemele de IA sunt dezvoltate și utilizate într-un mod durabil, care respectă mediul și care aduce beneficii tuturor ființelor umane, monitorizându-se și evaluându-se totodată efectele pe termen lung asupra persoanelor, a societății și a democrației. Aplicarea acestor principii ar trebui să fie transpusă, atunci când este posibil, în conceperea și utilizarea modelelor de IA. În orice caz, aceste principii ar trebui să servească drept bază pentru elaborarea codurilor de conduită în temeiul prezentului regulament. Toate părțile interesate, inclusiv industria, mediul academic, societatea civilă și organizațiile de standardizare, sunt încurajate să ia în considerare, după caz, principiile etice pentru dezvoltarea de bune practici și standarde voluntare.

(28) Pe lângă numeroasele utilizări benefice ale IA, aceasta poate fi utilizată și 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 abuzive și ar trebui să fie 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 consacrate în cartă, inclusiv dreptul la nediscriminare, la protecția datelor și la viața privată și drepturile copilului.

(29) Tehnicile de manipulare bazate pe IA pot fi utilizate pentru a convinge anumite persoane să manifeste comportamente nedorite sau pentru a le înșela, împingându-le să ia decizii într-un mod care le subminează și le afectează autonomia, capacitatea decizională și libera alegere. Introducerea pe piață, punerea în funcțiune sau utilizarea anumitor sisteme de IA având drept obiectiv sau drept efect denaturarea semnificativă a comportamentului uman, caz în care este probabil să se producă prejudicii semnificative, mai ales cu efecte negative suficient de importante asupra sănătății fizice sau psihologice ori a intereselor financiare, sunt deosebit de periculoase și, prin urmare, ar trebui să fie interzise. Astfel de sisteme de IA implementează componente subliminale, cum ar fi stimuli audio, sub formă de imagini sau video, pe care persoanele nu le pot percepe întrucât stimulii respectivi depășesc percepția umană, sau alte tehnici manipulatoare sau înșelătoare care subminează sau afectează autonomia, capacitatea decizională sau libera alegere ale unei persoane în astfel de moduri încât oamenii nu sunt conștienți de astfel de tehnici sau, chiar dacă sunt conștienți de acestea, tot pot fi înșelați sau sunt incapabili să le controleze sau să li se opună. Acest lucru ar putea fi facilitat, de exemplu, de interfețele mașină-creier sau de realitatea virtuală, deoarece acestea permit un nivel mai ridicat de control asupra stimulilor prezentați persoanelor, în măsura în care acești stimuli pot denatura semnificativ comportamentul persoanelor într-un mod deosebit de dăunător. În plus, sistemele de IA pot exploata și în alte moduri vulnerabilitățile unei persoane sau ale unui anumit grup de persoane din cauza vârstei sau a dizabilității acestora în sensul Directivei (UE) 2019/882 a Parlamentului European și a Consiliului[16] 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 sau care aparțin minorităților etnice sau religioase.

---

16 Directiva (UE) 2019/882 a Parlamentului European și a Consiliului din 17 aprilie 2019 privind cerințele de accesibilitate aplicabile produselor și serviciilor (JO L 151, 7.6.2019, p. 70).

Astfel de sisteme de IA pot fi introduse pe piață, puse în funcțiune sau utilizate având drept obiectiv sau drept efect denaturarea semnificativă a comportamentului unei persoane, într-un mod care cauzează sau este susceptibil în mod rezonabil să cauzeze prejudicii semnificative persoanei respective sau grupului respectiv ori unei alte persoane sau altor grupuri de persoane, inclusiv prejudicii care se pot acumula în timp, și, prin urmare, ar trebui să fie interzise. Este posibil să nu se poată presupune că există intenția de a denatura comportamentul în cazul în care denaturarea rezultă din factori externi sistemului de IA asupra cărora furnizorul sau implementatorul nu deține controlul, și anume factori care ar putea să nu fie prevăzuți în mod rezonabil și, prin urmare, să nu poată fi atenuați de către furnizorul sau implementatorul sistemului de IA. În orice caz, nu este necesar ca furnizorul sau implementatorul să aibă intenția de a cauza un prejudiciu semnificativ, cu condiția ca un astfel de prejudiciu să rezulte din practicile de manipulare sau de exploatare bazate pe IA. Interdicțiile privind astfel de practici în domeniul IA sunt complementare dispozițiilor cuprinse în Directiva 2005/29/CE a Parlamentului European și a Consiliului[17], în special faptul că practicile comerciale neloiale care conduc la prejudicii economice sau financiare pentru consumatori sunt interzise în toate circumstanțele, indiferent dacă sunt puse în aplicare 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 dreptul și cu standardele medicale aplicabile, de exemplu în ceea ce privește consimțământul explicit al persoanelor în cauză sau al reprezentanților lor legali. În plus, practicile comerciale comune și legitime, de exemplu în domeniul publicității, care respectă dreptul aplicabil nu ar trebui să fie considerate, în sine, ca reprezentând practici dăunătoare de manipulare bazate pe IA.

---

[17] Directiva 2005/29/CE a Parlamentului European și a Consiliului din 11 mai 2005 privind practicile comerciale neloiale ale întreprinderilor de pe piața internă față de consumatori și de modificare a Directivei 84/450/CEE a Consiliului, a Directivelor 97/7/CE, 98/27/CE și 2002/65/CE ale Parlamentului European și ale Consiliului și a Regulamentului (CE) nr. 2006/2004 al Parlamentului European și al Consiliului („Directiva privind practicile comerciale neloiale”) (JO L 149, 11.6.2005, p. 22).

(30) Sistemele de clasificare biometrică care se bazează pe datele biometrice ale persoanelor fizice, cum ar fi fața sau amprentele digitale ale unei persoane, pentru a face presupuneri sau deducții cu privire la opiniile politice, apartenența la un sindicat, convingerile religioase sau filozofice, rasa, viața sexuală sau orientarea sexuală ale unei persoane ar trebui să fie interzise. Această interdicție nu ar trebui să se refere la etichetarea, filtrarea sau clasificarea legală, în funcție de datele biometrice, a seturilor de date biometrice obținute în conformitate cu dreptul Uniunii sau cu dreptul intern, cum ar fi sortarea imaginilor în funcție de culoarea părului sau de culoarea ochilor, care poate fi utilizată, de exemplu, în domeniul aplicării legii.

(31) Sistemele de IA care permit atribuirea unui punctaj social persoanelor fizice de către actori privați sau publici 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 sau grupurile de persoane pe baza mai multor puncte de date legate de comportamentul lor social în contexte multiple sau de caracteristici personale sau de personalitate cunoscute, deduse sau preconizate de-a lungul anumitor perioade de timp. Punctajul social obținut din astfel de sisteme de IA poate duce la un tratament prejudiciabil 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 prejudiciabil care este disproporționat sau nejustificat în raport cu gravitatea comportamentului lor social. Sistemele de IA care implică astfel de practici inacceptabile de atribuire a unui punctaj și care conduc la astfel de rezultate prejudiciabile sau nefavorabile ar trebui, prin urmare, să fie interzise. Această interdicție nu ar trebui să afecteze practicile legale de evaluare a persoanelor fizice care sunt realizate într-un scop specific în conformitate cu dreptul Uniunii și cu dreptul național.

(32) Utilizarea sistemelor de IA pentru identificarea biometrică la distanță „în timp real” a persoanelor fizice în spațiile accesibile publicului în scopul aplicării legii este deosebit de intruzivă pentru drepturile și libertățile persoanelor în cauză, în măsura în care poate afecta viața privată a unei părți mari a populației, poate inspira un sentiment de supraveghere constantă și poate descuraja indirect exercitarea libertății de întrunire și a altor drepturi fundamentale. Inexactitățile tehnice ale sistemelor de IA destinate identificării biometrice la distanță a persoanelor fizice pot conduce la rezultate distorsionate de prejudecăți și pot avea efecte discriminatorii. Astfel de rezultate distorsionate și efecte discriminatorii posibile sunt deosebit de relevante în ceea ce privește vârsta, etnia, rasa, sexul sau dizabilitatea. 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 în contextul activităților de aplicare a legii sau impactate de acestea.

(33) Prin urmare, utilizarea sistemelor respective în scopul aplicării legii ar trebui să fie interzisă, cu excepția situațiilor enumerate în mod exhaustiv și definite în mod precis în care utilizarea este strict necesară pentru un interes public substanțial, a cărui importanță este superioară riscurilor. Situațiile respective implică căutarea anumitor victime ale unor infracțiuni, inclusiv persoane dispărute, anumite amenințări la adresa vieții sau a siguranței fizice a persoanelor fizice sau privind un atac terorist și localizarea sau identificarea autorilor infracțiunilor enumerate într-o anexă la prezentul regulament sau a persoanelor suspectate de acestea, 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 patru ani și astfel cum sunt definite în dreptul intern al 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, lista infracțiunilor prevăzută în anexa la prezentul regulament se bazează pe cele 32 de infracțiuni enumerate în Decizia-cadru 2002/584/JAI a Consiliului[18], ținând seama de faptul că unele infracțiuni sunt, în practică, susceptibile să fie mai relevante decât altele, în sensul că recurgerea la identificarea biometrică la distanță „în timp real” ar putea, în mod previzibil, fi necesară și proporțională în grade foarte diferite pentru urmărirea practică a localizării sau a identificării unui autor al diferitelor infracțiuni enumerate sau a unei persoane suspectate de acestea, și având în vedere diferențele probabile în ceea ce privește gravitatea, probabilitatea și amploarea prejudiciului sau posibilele consecințe negative.

[18] 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).

O amenințare iminentă la adresa vieții sau a siguranței fizice a unor persoane fizice ar putea rezulta și dintr-o perturbare gravă a infrastructurii critice, astfel cum este definită la articolul 2 punctul 4 din Directiva (UE) 2022/2557 a Parlamentului European și a Consiliului[19], în cazul în care perturbarea sau distrugerea unei astfel de infrastructuri critice ar genera o amenințare iminentă la adresa vieții sau a siguranței fizice a unei persoane, inclusiv prin afectarea gravă a aprovizionării cu produse de bază a populației sau a exercitării funcțiilor de bază ale statului. În plus, prezentul regulament ar trebui să mențină capacitatea autorităților 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 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 persoane care, în cursul unui control de identitate, fie refuză să fie identificate, fie sunt incapabile să își declare sau să își dovedească identitatea, fără ca autoritățile în cauză să fie obligate prin prezentul regulament să obțină o autorizație prealabilă. Ar putea fi vorba, de exemplu, de o persoană implicată într-o infracțiune care fie nu dorește, fie, din cauza unui accident sau a unei afecțiuni medicale, nu poate să își divulge identitatea autorităților de aplicare a legii.

[19] Directiva (UE) 2022/2557 a Parlamentului European și a Consiliului din 14 decembrie 2022 privind reziliența entităților critice și de abrogare a Directivei 2008/114/CE a Consiliului (JO L 333, 27.12.2022, p. 164).

(34) Pentru a se asigura că sistemele respective 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 precis definite, ar trebui să fie 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, ar trebui să se recurgă la utilizarea sistemelor de identificare biometrică la distanță „în timp real” în spațiile accesibile publicului în scopul aplicării legii numai pentru a confirma identitatea persoanei vizate în mod specific și această utilizare ar trebui să se limiteze la ceea ce este strict necesar din punct de vedere al perioadei de timp, precum și al sferei de aplicare geografică și personală, având în vedere în special dovezile sau indicațiile privind amenințările, victimele sau autorul infracțiunii. Utilizarea sistemului de identificare biometrică la distanță în timp real în spațiile accesibile publicului ar trebui să fie autorizată numai dacă autoritatea relevantă de aplicare a legii a finalizat o evaluare a impactului asupra drepturilor fundamentale și, cu excepția cazului în care se prevede altfel în prezentul regulament, a înregistrat sistemul în baza de date prevăzută în prezentul regulament. Baza de date de referință a persoanelor ar trebui să fie adecvată pentru fiecare caz de utilizare în fiecare dintre situațiile menționate mai sus.

(35) Fiecare utilizare a unui sistem de identificare biometrică la distanță „în timp real” în spațiile accesibile publicului în scopul aplicării 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 a cărei decizie este obligatorie. O astfel de autorizație ar trebui, în principiu, să fie obținută înainte de utilizarea sistemului de IA în vederea identificării uneia sau mai multor persoane. Ar trebui să fie permise excepții de la această regulă în situații justificate în mod corespunzător din motive de urgență, și anume în situațiile în care necesitatea de a utiliza sistemele în cauză este de natură să facă imposibilă în mod efectiv și obiectiv obținerea unei autorizații înainte de începerea utilizării sistemului de IA. În astfel de situații de urgență, utilizarea sistemului de IA ar trebui să fie limitată la ceea ce este minim și absolut necesar și ar trebui să facă obiectul unor garanții și condiții adecvate, astfel cum sunt stabilite în dreptul intern și specificate de către însăși autoritatea de aplicare a legii în contextul fiecărui caz individual de utilizare urgentă. În plus, în astfel de situații, autoritatea de aplicare a legii ar trebui să solicite o astfel de autorizație și să furnizeze în același timp motivele pentru care nu a fost în măsură să o solicite mai devreme, fără întârzieri nejustificate și cel târziu în termen de 24 de ore. În cazul în care solicitarea unei astfel de autorizații este respinsă, utilizarea sistemelor de identificare biometrică în timp real legate de autorizația respectivă ar trebui să înceteze cu efect imediat și toate datele legate de utilizarea respectivă ar trebui să fie înlăturate și șterse. Aceste date includ datele de intrare dobândite direct de un sistem de IA în cursul utilizării unui astfel de sistem, precum și rezultatele și produsele obținute în cadrul utilizării legate de autorizația respectivă, dar nu ar trebui să includă datele de intrare dobândite în mod legal în conformitate cu un alt act legislativ al Uniunii sau național. În orice caz, nicio decizie care produce un efect juridic negativ asupra unei persoane nu ar trebui să fie luată exclusiv pe baza unui produs al sistemului de identificare biometrică la distanță.

(36) Pentru a-și îndeplini sarcinile în conformitate cu cerințele prevăzute în prezentul regulament, precum și în normele naționale, autoritatea relevantă de supraveghere a pieței și autoritatea națională pentru protecția datelor ar trebui să fie notificate cu privire la fiecare utilizare a sistemului de identificare biometrică în timp real. Autoritățile de supraveghere a pieței și autoritățile naționale pentru protecția datelor care au fost notificate ar trebui să prezinte Comisiei un raport anual privind utilizarea sistemelor de identificare biometrică în timp real.

(37) 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 respectiv 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. Astfel de norme naționale ar trebui să fie notificate Comisiei în termen de 30 de zile de la adoptare.

(38) Utilizarea sistemelor de IA pentru identificarea biometrică la distanță în timp real a persoanelor fizice în spațiile accesibile publicului în scopul aplicării legii implică în mod necesar prelucrarea de date biometrice. Normele din prezentul regulament care interzic, sub rezerva anumitor excepții, o astfel de utilizare, care se întemeiază 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 posibile numai în măsura în care sunt compatibile cu cadrul stabilit de prezentul regulament, fără a exista, în afara cadrului respectiv, posibilitatea ca autoritățile competente, atunci când acționează în scopul aplicării legii, să utilizeze astfel de sisteme și să prelucreze astfel de date în legătură cu utilizarea respectivă 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 (UE) 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 aplicare a legii, inclusiv de către autoritățile competente, nu ar trebui să facă obiectul cadrului specific privind o astfel de utilizare în scopul aplicării legii stabilit de prezentul regulament. Prin urmare, o astfel de utilizare în alte scopuri decât aplicarea legii nu ar trebui să facă obiectul solicitării unei autorizații în temeiul prezentului regulament și al normelor de drept intern detaliate aplicabile prin care autorizația respectivă poate produce efecte.

(39) Orice prelucrare de date biometrice și alte 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 aplicării 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 ceea ce privește alte scopuri decât aplicarea legii, articolul 9 alineatul (1) din Regulamentul (UE) 2016/679 și articolul 10 alineatul (1) din Regulamentul (UE) 2018/1725 interzic prelucrarea de date biometrice, sub rezerva unor excepții limitate prevăzute la articolele respective. În vederea aplicării articolului 9 alineatul (1) din Regulamentul (UE) 2016/679, utilizarea identificării biometrice la distanță în alte scopuri decât aplicarea legii a făcut deja obiectul unor decizii de interzicere luate de autoritățile naționale pentru protecția datelor.

(40) 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) primul paragraf litera (g) în măsura în care se aplică utilizării sistemelor de clasificare biometrică pentru activități în domeniul cooperării polițienești și al cooperării judiciare în materie penală, la articolul 5 alineatul (1) primul paragraf litera (d) în măsura în care se aplică utilizării sistemelor de IA care intră sub incidența dispoziției respective, la articolul 5 alineatul (1) primul paragraf litera (h) și alineatele (2)-(6) și la articolul 26 alineatul (10) din prezentul regulament adoptate în temeiul articolului 16 din TFUE, referitoare la prelucrarea datelor cu caracter personal de către statele membre atunci când exercită activități care intră în domeniul de aplicare al părții a treia titlul V capitolul 4 sau 5 din TFUE, în cazurile în care 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.

(41) 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) primul paragraf litera (g) în măsura în care se aplică utilizării sistemelor de clasificare biometrică pentru activități în domeniul cooperării polițienești și al cooperării judiciare în materie penală, la articolul 5 alineatul (1) primul paragraf litera (d) în măsura în care se aplică utilizării sistemelor de IA care intră sub incidența dispoziției respective, la articolul 5 alineatul (1) primul paragraf litera (h) și alineatele (2)-(6) și la articolul 26 alineatul (10) din prezentul regulament adoptate în temeiul articolului 16 din TFUE, referitoare la prelucrarea datelor cu caracter personal de către statele membre atunci când exercită activități care intră în domeniul de aplicare al părții a treia titlul V capitolul 4 sau 5 din TFUE și Danemarca nu face obiectul aplicării normelor respective.

(42) În conformitate cu prezumția de nevinovăție, persoanele fizice din Uniune ar trebui să fie întotdeauna judecate în funcție de comportamentul lor real. Persoanele fizice nu ar trebui să fie niciodată judecate în funcție de comportamentul preconizat de IA exclusiv pe baza creării profilurilor lor, a trăsăturilor lor de personalitate sau a unor caracteristici precum cetățenia, locul nașterii, locul de reședință, numărul de copii, nivelul datoriilor sau tipul de autoturism, dacă nu există o suspiciune rezonabilă, bazată pe fapte obiective verificabile, că persoana respectivă este implicată într-o activitate infracțională și dacă nu se face o evaluare în acest sens de către un om. Prin urmare, ar trebui să fie interzise evaluările riscurilor efectuate în legătură cu persoane fizice pentru a evalua probabilitatea ca acestea să comită infracțiuni sau pentru a anticipa producerea unei infracțiuni reale sau potențiale exclusiv pe baza creării profilurilor acestor persoane sau a evaluării trăsăturilor lor de personalitate și a caracteristicilor lor. În orice caz, această interdicție nu privește și nici nu afectează analiza de risc care nu se bazează pe crearea de profiluri ale persoanelor sau pe trăsăturile de personalitate și caracteristicile persoanelor, cum ar fi sistemele de IA care utilizează analiza de risc pentru a evalua probabilitatea de fraudă financiară din partea întreprinderilor pe baza unor tranzacții suspecte sau instrumentele analitice de risc utilizate pentru a prevedea probabilitatea localizării de către autoritățile vamale a stupefiantelor sau a mărfurilor ilicite, de exemplu pe baza rutelor de trafic cunoscute.

(43) Introducerea pe piață, punerea în funcțiune în scopul specific respectiv și utilizarea sistemelor de IA care creează sau extind baze de date de recunoaștere facială prin extragerea fără scop precis de imagini faciale de pe internet sau din înregistrări TVCI ar trebui să fie interzise, deoarece această practică amplifică sentimentul de supraveghere în masă și poate duce la încălcări grave ale drepturilor fundamentale, inclusiv ale dreptului la viață privată.

(44) Există preocupări serioase cu privire la baza științifică a sistemelor de IA care vizează identificarea sau deducerea emoțiilor, în special deoarece exprimarea emoțiilor variază considerabil de la o cultură la alta și de la o situație la alta și chiar la nivelul unei singure persoane. Printre principalele deficiențe ale unor astfel de sisteme se numără fiabilitatea limitată, lipsa specificității și posibilitățile limitate de generalizare. Prin urmare, sistemele de IA care identifică sau deduc emoțiile sau intențiile persoanelor fizice pe baza datelor lor biometrice pot genera rezultate discriminatorii și pot fi intruzive pentru drepturile și libertățile persoanelor în cauză. Având în vedere dezechilibrul de putere în contextul muncii sau al educației, combinat cu caracterul intruziv al acestor sisteme, ele ar putea conduce la un tratament prejudiciabil sau nefavorabil al anumitor persoane fizice sau al unor grupuri întregi de astfel de persoane. Prin urmare, ar trebui să fie interzise introducerea pe piață, punerea în funcțiune și utilizarea sistemelor de IA destinate a fi utilizate pentru a detecta starea emoțională a persoanelor în situații legate de locul de muncă și de educație. Această interdicție nu ar trebui să se aplice sistemelor de IA introduse pe piață strict din motive medicale sau de siguranță, cum ar fi sistemele destinate utilizării în scop terapeutic.

(45) Practicile interzise de dreptul Uniunii, inclusiv dreptul privind protecția datelor, dreptul privind nediscriminarea, dreptul privind protecția consumatorilor și dreptul concurenței, nu ar trebui să fie afectate de prezentul regulament.

(46) Sistemele de IA cu grad ridicat de risc ar trebui să fie introduse pe piața Uniunii, puse în funcțiune sau utilizate numai dacă respectă anumite cerințe obligatorii. Cerințele respective 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. Pe baza noului cadru legislativ, astfel cum s-a clarificat în Comunicarea Comisiei intitulată „«Ghidul albastru» din 2022 referitor la punerea în aplicare a normelor UE privind produsele”[20], regula generală este că cel puțin un act juridic din legislația de armonizare a Uniunii, cum ar fi Regulamentele (UE) 2017/745[21] și (UE) 2017/746[22] ale Parlamentului European și ale Consiliului sau Directiva 2006/42/CE a Parlamentului European și a Consiliului[23], poate fi aplicabil unui singur produs, deoarece punerea la dispoziție sau punerea în funcțiune poate avea loc numai atunci când produsul respectă întreaga legislație de armonizare a Uniunii aplicabilă. Pentru a se asigura coerența și a se evita sarcinile administrative sau costurile inutile, furnizorii unui produs care conține unul sau mai multe sisteme de IA cu grad ridicat de risc, cărora li se aplică cerințele prezentului regulament și ale legislației de armonizare a Uniunii astfel cum este conținută într-o anexă la prezentul regulament, ar trebui să fie flexibili în ceea ce privește deciziile operaționale cu privire la modul optim de asigurare a conformității unui produs care conține unul sau mai multe sisteme de IA cu toate cerințele aplicabile din respectiva legislație de armonizare a 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 ar trebui să reducă la minimum orice eventuală restricționare a comerțului internațional.

---

20 JO C 247, 29.6.2022, p. 1.

21 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).

22 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).

23 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).

(47) Sistemele de IA ar putea avea un impact negativ asupra sănătății și siguranței persoanelor, în special atunci când funcționează drept componente de siguranță 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 ajung 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 și să își îndeplinească funcțiile în condiții de siguranță 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.

(48) 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 grad ridicat de risc. 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, dreptul la nediscriminarea, dreptul la educație, protecția consumatorilor, drepturile lucrătorilor, drepturile persoanelor cu dizabilități, egalitatea de gen, drepturile de proprietate intelectuală, dreptul la o cale de atac eficientă și la un proces echitabil, dreptul la apărare și prezumția de nevinovăție și dreptul la o bună administrare. Pe lângă aceste drepturi, este important să se sublinieze faptul că copiii au drepturi specifice, astfel cum sunt consacrate la articolul 24 din cartă și în Convenția Organizației Națiunilor Unite cu privire la drepturile copilului, detaliată în Comentariul general nr. 25 la aceasta privind mediul digital, ambele impunând 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, să fie luat în considerare atunci când se evaluează gravitatea prejudiciului pe care îl poate cauza un sistem de IA, inclusiv în ceea ce privește sănătatea și siguranța persoanelor.

(49) 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[24], al Regulamentului (UE) nr. 167/2013 al Parlamentului European și al Consiliului[25], al Regulamentului (UE) nr. 168/2013 al Parlamentului European și al Consiliului[26], al Directivei 2014/90/UE a Parlamentului European și a Consiliului[27], al Directivei (UE) 2016/797 a Parlamentului European și a Consiliului[28], al Regulamentului (UE) 2018/858 al Parlamentului European și al Consiliului[29],

---

[24] 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).

[25] 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).

[26] 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).

[27] 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).

[28] 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).

[29] 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).

al Regulamentului (UE) 2018/1139 al Parlamentului European și al Consiliului[30] și al Regulamentului (UE) 2019/2144 al Parlamentului European și al Consiliului[31], este oportun să se modifice respectivele acte legislative pentru a se asigura luarea în considerare de către Comisie, pe baza specificităților tehnice și de reglementare ale fiecărui sector și fără a afecta mecanismele și autoritățile existente de guvernanță, de evaluare a conformității și de aplicare a legislației instituite în acestea, a cerințelor obligatorii pentru sistemele de IA cu grad ridicat de risc prevăzute în prezentul regulament atunci când adoptă orice act delegat sau de punere în aplicare relevant pe baza respectivelor acte legislative.

---

[30] 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).

[31] 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 Comisiei (JO L 325, 16.12.2019, p. 1).

(50) În ceea ce privește sistemele de IA care sunt componente de siguranță ale produselor sau care sunt ele însele produse care intră în domeniul de aplicare al anumitor acte legislative de armonizare ale Uniunii enumerate într-o anexă la prezentul regulament, este oportun să fie clasificate ca prezentând un grad ridicat de risc în temeiul prezentului regulament în cazul în care produsul respectiv este supus procedurii de evaluare a conformității efectuate de un organism terț de evaluare a conformității în temeiul respectivelor acte legislative de armonizare relevante ale 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, dispozitivele medicale pentru diagnostic in vitro, cele din industria auto și aeronautică.

(51) Clasificarea unui sistem de IA ca prezentând un grad ridicat de risc 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 ca prezentând un grad ridicat de risc în conformitate cu criteriile stabilite în actele legislative de armonizare relevante ale Uniunii care se aplică produsului. Acesta este, în special, cazul Regulamentelor (UE) 2017/745 și (UE) 2017/746, care prevăd o evaluare a conformității de către un terț pentru produsele cu grad mediu de risc și cu grad ridicat de risc.

(52) În ceea ce privește sistemele de IA autonome, și anume alte sisteme de IA cu grad ridicat de risc decât cele care sunt componente de siguranță ale unor produse sau care sunt ele însele produse, este oportun să fie clasificate ca prezentând un grad ridicat de risc dacă, având în vedere scopul lor preconizat, prezintă un risc ridicat de a aduce prejudicii sănătății și siguranței sau drepturilor fundamentale ale persoanelor, ținându-se 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 precizate în prezentul regulament. Identificarea sistemelor respective se bazează pe aceeași metodologie și pe aceleași criterii avute în vedere pentru eventuale modificări viitoare ale listei de sisteme de IA cu grad ridicat de risc, modificări pe care Comisia ar trebui să fie împuternicită să le adopte, prin intermediul unor acte delegate, pentru a ține seama de ritmul rapid al dezvoltării tehnologice și de eventualele modificări în utilizarea sistemelor de IA.

(53) De asemenea, este important să se clarifice faptul că pot exista cazuri specifice în care sistemele de IA menționate în domenii predefinite specificate în prezentul regulament nu conduc la un risc semnificativ de a aduce prejudicii intereselor juridice protejate în cadrul domeniilor respective, deoarece nu influențează în mod semnificativ procesul decizional sau nu aduc prejudicii substanțiale intereselor respective. În sensul prezentului regulament, un sistem de IA care nu influențează în mod semnificativ rezultatul procesului decizional ar trebui să fie înțeles ca fiind un sistem de IA care nu are un impact asupra substanței și, prin urmare, nici asupra rezultatului procesului decizional, indiferent dacă este uman sau automatizat. Un sistem de IA care nu influențează în mod semnificativ rezultatul procesului decizional ar putea include situații în care sunt îndeplinite una sau mai multe dintre condițiile prezentate în continuare. Prima condiție ar trebui să fie aceea ca sistemul de IA să fie destinat să îndeplinească o sarcină procedurală restrânsă, de exemplu un sistem de IA care transformă date nestructurate în date structurate, un sistem de IA care clasifică pe categorii documentele primite sau un sistem de IA care este utilizat pentru a detecta duplicatele dintr-un număr mare de candidaturi. Aceste sarcini au un caracter atât de restrâns și de limitat încât prezintă doar riscuri reduse, riscuri care nu cresc prin utilizarea unui sistem de IA într-un context enumerat ca utilizare cu grad ridicat de risc într-o anexă la prezentul regulament. A doua condiție ar trebui să fie ca sarcina îndeplinită de sistemul de IA să fie menită să îmbunătățească rezultatul unei activități umane finalizate anterior care poate fi relevantă în sensul utilizărilor cu grad ridicat de risc enumerate într-o anexă la prezentul regulament. Având în vedere aceste caracteristici, sistemul de IA adaugă doar un nivel suplimentar unei activități umane, prezentând în consecință un risc redus. Această condiție s-ar aplica, de exemplu, sistemelor de IA care sunt menite să îmbunătățească limbajul utilizat în documente redactate anterior, de exemplu în ceea ce privește tonul profesional, stilul academic de limbaj sau alinierea textului la mesajele specifice unei anumite mărci. A treia condiție ar trebui să fie aceea ca sistemul de IA să fie destinat să detecteze modelele decizionale sau devierile de la modele decizionale anterioare.

Riscul ar fi redus deoarece utilizarea sistemului de IA este ulterioară unei evaluări finalizate anterior de către un om, pe care nu este destinată să o înlocuiască sau să o influențeze fără o revizuire adecvată de către un om. Printre aceste sisteme de IA se numără, de exemplu, cele care, având în vedere un anumit model de notare folosit de un cadru didactic, pot fi utilizate pentru a verifica *ex post* dacă respectivul cadru didactic s-a abătut de la modelul de notare în cauză și pentru a semnala astfel eventuale inconsecvențe sau anomalii. A patra condiție ar trebui să fie aceea ca sistemul de IA să fie destinat să îndeplinească o sarcină care este doar pregătitoare pentru o evaluare relevantă pentru scopurile sistemelor de IA enumerate într-o anexă la prezentul regulament, făcând astfel ca posibilul impact al rezultatelor sistemului să prezinte un risc foarte scăzut pentru evaluarea ulterioară bazată pe ele. Această condiție se referă, printre altele, la soluțiile inteligente de gestionare a fișierelor, care includ diverse funcții, cum ar fi indexarea, căutarea, prelucrarea textelor și a vorbirii sau corelarea datelor cu alte surse de date, ori la sistemele de IA utilizate pentru traducerea documentelor inițiale. În orice caz, ar trebui să se considere că sistemele de IA utilizate în situații cu grad ridicat de risc enumerate într-o anexă la prezentul regulament prezintă riscuri semnificative de prejudicii la adresa sănătății, siguranței sau drepturilor fundamentale dacă implică crearea de profiluri în sensul articolului 4 punctul 4 din Regulamentul (UE) 2016/679 sau al articolului 3 punctul 4 din Directiva (UE) 2016/680 sau al articolului 3 punctul 5 din Regulamentul (UE) 2018/1725. Pentru a asigura trasabilitatea și transparența, un furnizor care consideră pe baza condițiilor menționate mai sus că un sistem de IA nu prezintă un grad ridicat de risc ar trebui să întocmească documentația pentru evaluare înainte ca sistemul respectiv să fie introdus pe piață sau pus în funcțiune și ar trebui să furnizeze respectiva documentație autorităților naționale competente, la cerere. Furnizorul ar trebui să fie obligat să înregistreze sistemul de IA în baza de date a UE instituită în temeiul prezentului regulament. Pentru a oferi îndrumare suplimentară în vederea punerii în practică a condițiilor în care sistemele de IA enumerate într-o anexă la prezentul regulament nu prezintă, în mod excepțional, un grad ridicat de risc, Comisia ar trebui, după consultarea comitetului, să furnizeze orientări care să detalieze respectiva punere în practică, completate de o listă cuprinzătoare de exemple practice de cazuri de utilizare a sistemelor de IA cu grad ridicat de risc și cazuri de utilizare fără grad ridicat de risc.

(54) Întrucât datele biometrice constituie o categorie specială de date cu caracter personal, este oportun ca mai multe cazuri de utilizare critică a sistemelor biometrice să fie clasificate ca prezentând un grad ridicat de risc, în măsura în care utilizarea acestora este permisă în temeiul dreptului Uniunii și al dreptului intern relevant. Inexactitățile tehnice ale sistemelor de IA destinate identificării biometrice la distanță a persoanelor fizice pot conduce la rezultate distorsionate de prejudecăți și pot avea efecte discriminatorii. Riscul unor astfel de rezultate distorsionate de prejudecăți și efecte discriminatorii este deosebit de relevant în ceea ce privește vârsta, etnia, rasa, sexul sau dizabilitățile. Prin urmare, sistemele de identificare biometrică la distanță ar trebui să fie clasificate ca prezentând un grad ridicat de risc, având în vedere riscurile pe care le implică. Nu se încadrează în această clasificare sistemele de IA destinate a fi utilizate pentru verificarea biometrică, inclusiv pentru autentificare, al cărei unic scop este de a confirma că o anumită persoană fizică este cine susține că este și de a confirma identitatea unei persoane fizice cu unicul scop de a-i permite accesul la un serviciu, deblocarea unui dispozitiv sau accesul securizat într-o incintă. În plus, ar trebui să fie clasificate ca prezentând un grad ridicat de risc sistemele de IA destinate a fi utilizate pentru clasificarea biometrică în funcție de atribute sau caracteristici sensibile protejate în temeiul articolului 9 alineatul (1) din Regulamentul (UE) 2016/679 pe baza datelor biometrice, în măsura în care nu sunt interzise în temeiul prezentului regulament, și sistemele de recunoaștere a emoțiilor care nu sunt interzise în temeiul prezentului regulament. Sistemele biometrice destinate a fi utilizate exclusiv în scopul aplicării măsurilor de securitate cibernetică și de protecție a datelor cu caracter personal nu ar trebui să fie considerate sisteme de IA cu grad ridicat de risc.

(55) În ceea ce privește gestionarea și exploatarea infrastructurii critice, este oportun să se clasifice ca prezentând un grad ridicat de risc sistemele de IA destinate utilizării drept componente de siguranță în cadrul gestionării și exploatării infrastructurilor digitale critice enumerate la punctul 8 din anexa la Directiva (UE) 2022/2557, a traficului rutier și a aprovizionării cu apă, gaz, încălzire și energie electrică, deoarece defectarea lor sau funcționarea lor defectuoasă 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 ale infrastructurii digitale critice, 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 sistemele de monitorizare a presiunii apei sau sistemele de control al alarmei de incendiu în centrele de cloud computing.

(56) Implementarea sistemelor de IA în educație este importantă pentru a promova educația și formarea digitală de înaltă calitate și pentru a permite tuturor cursanților și cadrelor didactice să dobândească și să partajeze aptitudinile și competențele digitale necesare, inclusiv educația în domeniul mass-mediei și gândirea critică, pentru a participa activ la economie, în societate și la procesele democratice. Cu toate acestea, sistemele de IA utilizate în educație sau în formarea profesională, în special pentru stabilirea accesului sau a admiterii, pentru repartizarea persoanelor în instituții sau programe educaționale și de formare profesională la toate nivelurile, pentru evaluarea rezultatelor învățării unei persoane, pentru evaluarea nivelului adecvat de instruire al unei persoane, pentru influențarea semnificativă a nivelului de educație și formare pe care îl vor primi sau îl vor putea accesa persoanele sau pentru monitorizarea și detectarea comportamentului interzis al elevilor și studenților în timpul testelor, ar trebui să fie clasificate drept sisteme de IA cu grad ridicat de risc, deoarece pot determina parcursul educațional și profesional din viața unei persoane și, prin urmare, pot afecta capacitatea acesteia de a-și asigura mijloace de subzistență. Atunci când sunt concepute și utilizate în mod necorespunzător, astfel de sisteme pot fi deosebit de intruzive și pot încălca dreptul la educație și formare, precum și dreptul de a nu fi discriminat și pot perpetua tipare istorice de discriminare, de exemplu împotriva femeilor, a anumitor grupe de vârstă, a persoanelor cu dizabilități sau a persoanelor de anumite origini rasiale ori etnice sau cu o anumită orientare sexuală.

(57) De asemenea, 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 care afectează condițiile relației legate de muncă, pentru promovarea și încetarea relațiilor contractuale legate de muncă, pentru alocarea sarcinilor pe baza comportamentului individual sau a trăsăturilor sau caracteristicilor personale, precum și pentru monitorizarea sau evaluarea persoanelor aflate în relații contractuale legate de muncă, ar trebui să fie clasificate ca prezentând un grad ridicat de risc, deoarece aceste sisteme pot avea un impact semnificativ asupra viitoarelor perspective de carieră, asupra mijloacelor de subzistență ale acestor persoane și asupra drepturilor lucrătorilor. Relațiile contractuale relevante legate de muncă ar trebui să implice într-un mod semnificativ angajații și persoanele care prestează servicii prin intermediul platformelor, astfel cum se menționează în Programul de lucru al Comisiei pentru 2021. 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 tipare istorice de discriminare, de exemplu împotriva femeilor, a anumitor grupe de vârstă, a persoanelor cu dizabilități sau a persoanelor de anumite origini rasiale ori etnice sau cu o anumită orientare sexuală. Sistemele de IA utilizate pentru a monitoriza performanța și comportamentul acestor persoane pot, de asemenea, să le submineze drepturile fundamentale la protecția datelor și la viața privată.

(58) Un alt domeniu în care utilizarea sistemelor de IA merită o atenție deosebită este accesul și posibilitatea de a beneficia de anumite prestații și servicii publice și private esențiale, necesare pentru ca oamenii să participe pe deplin în societate sau să își îmbunătățească nivelul de trai. În special, persoanele fizice care solicită sau primesc prestații și servicii esențiale de asistență publică din partea autorităților publice, și anume servicii de îngrijiri de sănătate, prestații de asigurări sociale, servicii sociale care oferă protecție în cazuri precum maternitatea, boala, accidentele de muncă, dependența, bătrânețea, pierderea locului de muncă, precum și asistență socială și legată de locuințe, sunt de regulă dependente 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 să fie acordate, refuzate, reduse, revocate sau recuperate de autorități, inclusiv dacă beneficiarii au dreptul legitim la astfel de prestații 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 efectivă și, prin urmare, ar trebui să fie 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 plus, sistemele de IA utilizate pentru a evalua punctajul de credit sau bonitatea persoanelor fizice ar trebui să fie 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 telecomunicații. Sistemele de IA utilizate în aceste scopuri pot duce la discriminare între persoane sau între grupuri și pot perpetua tipare istorice de discriminare, de exemplu pe criterii de origine rasială sau etnică, sex, dizabilitate, vârstă sau orientare sexuală, sau pot crea noi forme de impact discriminatoriu. Cu toate acestea, sistemele de IA prevăzute de dreptul Uniunii în scopul detectării fraudelor în furnizarea de servicii financiare și în scopuri prudențiale pentru a calcula cerințele de capital ale instituțiilor de credit și ale întreprinderilor de asigurări nu ar trebui să fie considerate ca prezentând un grad ridicat de risc în temeiul prezentului regulament. În plus, sistemele de IA destinate a fi utilizate pentru evaluarea riscurilor și stabilirea prețurilor pentru asigurarea de sănătate și de viață în cazul persoanelor fizice pot avea, de asemenea, un impact semnificativ asupra mijloacelor de subzistență ale persoanelor și, dacă nu sunt concepute, dezvoltate și utilizate în mod corespunzător, pot încălca drepturile lor fundamentale și pot avea consecințe grave pentru viața și sănătatea oamenilor, cum ar fi excluziunea financiară și discriminarea. În cele din urmă, sistemele de IA utilizate pentru evaluarea și clasificarea apelurilor de urgență ale persoanelor fizice sau pentru distribuirea sau stabilirea priorităților în distribuirea serviciilor de primă intervenție de urgență, inclusiv de către poliție, pompieri și asistența medicală, precum și în cadrul sistemelor de triaj medical de urgență al pacienților, ar trebui de asemenea să fie clasificate ca prezentând un grad ridicat de risc, deoarece iau decizii în situații foarte critice pentru viața și sănătatea persoanelor și pentru bunurile acestora.

(59) Având în vedere rolul și responsabilitatea lor, 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 nu este alimentat cu date de înaltă calitate, nu îndeplinește cerințe adecvate de performanță, acuratețe sau robustețe sau nu este proiectat și testat în mod corespunzător înainte de a fi introdus pe piață sau pus în funcțiune în alt mod, sistemul de IA poate selecta persoanele într-un mod discriminatoriu sau, la un nivel mai general, în mod incorect ori injust. În plus, exercitarea unor drepturi procedurale fundamentale importante, cum ar fi dreptul la o cale de atac efectivă 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 fie clasificate ca prezentând un grad ridicat de risc, în măsura în care utilizarea lor este permisă în temeiul dreptului Uniunii și al dreptului intern relevant, o serie de sisteme de IA destinate a fi utilizate în contextul aplicării 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 reparații efective.

Având în vedere natura activităților 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 sau în numele acestora sau de instituțiile, organele, oficiile sau agențiile Uniunii în sprijinul autorităților de aplicare a legii pentru a evalua riscul ca o persoană fizică să devină victimă a infracțiunilor, ca poligrafe și instrumente similare pentru evaluarea fiabilității probelor în cursul investigării sau urmăririi penale a infracțiunilor și, în măsura în care nu se interzice în temeiul prezentului regulament, pentru a evalua riscul ca o persoană fizică să comită o infracțiune sau o recidivă, nu numai pe baza creării de profiluri ale persoanelor fizice, a evaluării trăsăturilor de personalitate și a caracteristicilor lor sau a comportamentului infracțional anterior al persoanelor fizice sau al grupurilor, precum și pentru a crea profiluri în cursul depistării, investigării sau urmăririi penale a infracțiunilor. Sistemele de IA destinate în mod specific 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 dreptului Uniunii privind combaterea spălării banilor, nu ar trebui să fie clasificate ca 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. Utilizarea instrumentelor de IA de către autoritățile de aplicare a legii și de alte autorități relevante nu ar trebui să devină un factor de inegalitate sau de excluziune. Impactul utilizării instrumentelor de IA asupra drepturilor la apărare ale suspecților nu ar trebui să fie ignorat, în special dificultatea de a obține informații semnificative cu privire la funcționarea acestor sisteme și, în consecință, dificultatea de a contesta rezultatele acestora în instanță, în special de către persoanele fizice care fac obiectul investigării.

(60) Sistemele de IA utilizate în domeniile migrației, azilului și gestionării controlului la frontiere 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, protecție internațională și bună administrare. Prin urmare, este oportun să fie clasificate ca prezentând un grad ridicat de risc, în măsura în care utilizarea lor este permisă în temeiul dreptului Uniunii și al dreptului intern relevant, sistemele de IA destinate a fi utilizate de către autoritățile publice competente ori în numele acestora sau de către instituțiile, organele, oficiile sau agențiile Uniunii care au atribuții în domeniile migrației, azilului și gestionării controlului la frontiere ca poligrafe și instrumente similare, pentru a evalua anumite riscuri prezentate de persoanele fizice care intră pe teritoriul unui stat membru sau care solicită viză sau azil, pentru a acorda asistență autorităților publice competente în ceea ce privește examinarea, inclusiv evaluarea conexă a fiabilității probelor, a 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, în scopul detectării, al recunoașterii sau al identificării persoanelor fizice în contextul migrației, al azilului și al gestionării controlului la frontiere, cu excepția verificării documentelor de călătorie.

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 Regulamentul (CE) nr. 810/2009 al Parlamentului European și al Consiliului[32], de Directiva 2013/32/UE a Parlamentului European și a Consiliului[33] și de alte dispoziții relevante din dreptul Uniunii. Statele membre sau instituțiile, organele, oficiile și agențiile Uniunii nu ar trebui în niciun caz să utilizeze sistemele de IA în domeniul migrației, azilului și gestionării controlului la frontiere ca mijloc de eludare a obligațiilor lor internaționale în temeiul Convenției ONU privind statutul refugiaților întocmită la Geneva la 28 iulie 1951, astfel cum a fost modificată prin Protocolul din 31 ianuarie 1967. De asemenea, respectivele sisteme de IA nu ar trebui să fie utilizate pentru a încălca în vreun fel principiul nereturnării sau pentru a refuza căi legale sigure și eficace de intrare pe teritoriul Uniunii, inclusiv dreptul la protecție internațională.

---

32 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).

33 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).

(61) Anumite sisteme de IA destinate administrării justiției și proceselor democratice ar trebui să fie clasificate ca prezentând 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 efectivă și la un proces echitabil. În special, pentru a aborda potențialele riscuri de prejudecăți, erori și opacitate, este oportun să fie calificate drept sisteme cu grad ridicat de risc sistemele de IA destinate să fie utilizate de o autoritate judiciară sau în numele acesteia pentru a ajuta autoritățile judiciare să cerceteze și să interpreteze faptele și legea și să aplice legea unui set concret de fapte. Sistemele de IA destinate a fi utilizate de organismele de soluționare alternativă a litigiilor în aceste scopuri ar trebui, de asemenea, să fie considerate ca având un grad ridicat de risc atunci când rezultatele procedurilor de soluționare alternativă a litigiilor produc efecte juridice pentru părți. Utilizarea instrumentelor de IA poate sprijini puterea de decizie a judecătorilor sau independența sistemului judiciar, dar nu ar trebui să le înlocuiască: procesul decizional final trebuie să rămână o activitate umană. Clasificarea sistemelor de IA ca prezentând un grad ridicat de risc nu ar trebui, totuși, să se extindă la sistemele de IA destinate unor activități administrative pur auxiliare care nu afectează administrarea efectivă a justiției în cazuri individuale, cum ar fi anonimizarea sau pseudonimizarea hotărârilor judecătorești, a documentelor sau a datelor, comunicarea între membrii personalului, sarcinile administrative.

(62) Fără a aduce atingere normelor prevăzute în Regulamentul (UE) 2024/... al Parlamentului European și al Consiliului[34+] și pentru a aborda riscurile de ingerințe externe nejustificate în dreptul de vot consacrat la articolul 39 din cartă și de efecte adverse asupra democrației și a statului de drept, sistemele de IA destinate a fi utilizate pentru a influența rezultatul unor alegeri sau al unui referendum sau comportamentul de vot al persoanelor fizice în exercitarea votului lor în cadrul alegerilor sau al referendumurilor ar trebui să fie clasificate drept sisteme de IA cu grad ridicat de risc, cu excepția sistemelor de IA la ale căror rezultate persoanele fizice nu sunt expuse în mod direct, cum ar fi instrumentele utilizate pentru organizarea, optimizarea și structurarea campaniilor politice din punct de vedere administrativ și logistic.

(63) Faptul că un sistem de IA este clasificat ca sistem de IA cu grad ridicat de risc în temeiul prezentului regulament nu ar trebui să fie interpretat ca indicând 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 detectarea stării emoționale 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 aplicabilă a Uniunii și din dreptul intern aplicabil. Prezentul regulament nu ar trebui să fie 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.

---

[34] Regulamentul (UE) nr. 2024/… al Parlamentului European și al Consiliului din … privind transparența și vizarea unui public-țintă în publicitatea politică (JO L, …, ELI: …).

[+] JO: a se introduce în text numărul regulamentului din PE-CONS 90/23 [2021/0381 (COD)] și a se completa nota de subsol corespunzătoare.

(64) Pentru atenuarea riscurilor generate de sistemele de IA cu grad ridicat de risc introduse pe piață sau puse în funcțiune și pentru a asigura un nivel înalt de credibilitate, ar trebui să se aplice anumite cerințe obligatorii în cazul sistemelor de IA cu grad ridicat de risc, ținând seama de scopul preconizat și de contextul utilizării sistemului de IA și în conformitate cu sistemul de gestionare a riscurilor care urmează să fie instituit de furnizor. Măsurile adoptate de furnizori pentru a se conforma cerințelor obligatorii din prezentul regulament ar trebui să țină seama de stadiul general recunoscut al tehnologiei în materie de IA, să fie proporționale și eficace pentru a îndeplini obiectivele prezentului regulament. Pe baza noului cadru legislativ, astfel cum s-a clarificat în Comunicarea Comisiei intitulată „«Ghidul albastru» din 2022 referitor la punerea în aplicare a normelor UE privind produsele", regula generală este că cel puțin un act juridic din legislația de armonizare a Uniunii poate fi aplicabil unui singur produs, deoarece punerea la dispoziție sau punerea în funcțiune poate avea loc numai atunci când produsul respectă întreaga legislație de armonizare a Uniunii aplicabilă. Pericolele sistemelor de IA care fac obiectul cerințelor prezentului regulament se referă la aspecte diferite față de legislația existentă de armonizare a Uniunii și, prin urmare, cerințele prezentului regulament ar completa corpul existent al legislației de armonizare a Uniunii. De exemplu, mașinile sau dispozitivele medicale care încorporează un sistem de IA ar putea prezenta riscuri care nu sunt abordate de cerințele esențiale de sănătate și siguranță prevăzute în legislația armonizată relevantă a Uniunii, deoarece legislația sectorială respectivă nu abordează riscurile specifice sistemelor de IA.

Acest lucru necesită o aplicare simultană și complementară a diferitelor acte legislative. Pentru a se asigura coerența și a se evita sarcinile administrative și costurile inutile, furnizorii unui produs care conține unul sau mai multe sisteme de IA cu grad ridicat de risc, cărora li se aplică cerințele prezentului regulament și ale legislației de armonizare a Uniunii bazate pe noul cadru legislativ și care figurează într-o anexă la prezentul regulament, ar trebui să fie flexibili în ceea ce privește deciziile operaționale cu privire la modul optim de asigurare a conformității unui produs care conține unul sau mai multe sisteme de IA cu toate cerințele aplicabile din respectiva legislație armonizată a Uniunii. Această flexibilitate ar putea însemna, de exemplu, o decizie a furnizorului de a integra o parte a proceselor de testare și raportare necesare, informațiile și documentația impuse în temeiul prezentului regulament în documentația și în procedurile deja existente impuse în temeiul legislației de armonizare existente a Uniunii bazate pe noul cadru legislativ și care figurează într-o anexă la prezentul regulament. Acest lucru nu ar trebui să submineze în niciun fel obligația furnizorului de a respecta toate cerințele aplicabile.

(65) Sistemul de gestionare a riscurilor ar trebui să constea într-un proces iterativ continuu care este preconizat și derulat pe parcursul întregului ciclu de viață al unui sistem de IA cu grad ridicat de risc. Respectivul proces ar trebui să aibă drept scop identificarea și atenuarea riscurilor relevante reprezentate de sistemele de IA pentru sănătate, siguranță și drepturile fundamentale. Sistemul de gestionare a riscurilor ar trebui să fie evaluat și actualizat periodic pentru a se asigura eficacitatea sa continuă, precum și justificarea și documentarea oricăror decizii și acțiuni semnificative luate în temeiul prezentului regulament. Acest proces ar trebui să garanteze faptul că furnizorul identifică riscurile sau efectele negative și pune în aplicare măsuri de atenuare pentru riscurile cunoscute și previzibile în mod rezonabil reprezentate de sistemele de IA pentru sănătate, siguranță și drepturile fundamentale, având în vedere scopul preconizat al acestora și utilizarea necorespunzătoare previzibilă în mod rezonabil ale acestor sisteme, inclusiv posibilele riscuri care decurg din interacțiunea dintre sistemele de IA și mediul în care funcționează. Sistemul de gestionare a riscurilor ar trebui să adopte cele mai adecvate măsuri de gestionare a riscurilor, având în vedere stadiul cel mai avansat al tehnologiei în domeniul IA. Atunci când identifică cele mai adecvate măsuri de gestionare a riscurilor, furnizorul ar trebui să documenteze și să explice alegerile făcute și, după caz, să implice experți și părți interesate externe. Atunci când identifică utilizarea necorespunzătoare previzibilă în mod rezonabil a sistemelor de IA cu grad ridicat de risc, furnizorul ar trebui să acopere utilizările sistemelor de IA în legătură cu care se poate aștepta în mod rezonabil, să rezulte dintr-un comportament uman ușor previzibil în contextul caracteristicilor specifice și al utilizării unui anumit sistem de IA, deși utilizările respective nu sunt acoperite în mod direct de scopul preconizat și nu sunt prevăzute în instrucțiunile de utilizare. Orice circumstanțe cunoscute sau previzibile legate de utilizarea sistemului de IA cu grad ridicat de risc în conformitate cu scopul său preconizat sau în condiții de utilizare necorespunzătoare previzibilă în mod rezonabil, care pot conduce la riscuri pentru sănătate și siguranță sau pentru drepturile fundamentale, ar trebui să fie incluse în instrucțiunile de utilizare care sunt furnizate de furnizor. Scopul este de a se asigura că implementatorul le cunoaște și le ia în considerare atunci când utilizează sistemul de IA cu grad ridicat de risc. Identificarea și punerea în aplicare a măsurilor de atenuare a riscurilor în caz de utilizare necorespunzătoare previzibilă în temeiul prezentului regulament nu ar trebui să necesite din partea furnizorului antrenare suplimentară specifică pentru sistemul de IA cu grad ridicat de risc pentru a aborda utilizarea necorespunzătoare previzibilă. Cu toate acestea, furnizorii sunt încurajați să ia în considerare astfel de măsuri suplimentare de antrenare pentru a atenua utilizările necorespunzătoare previzibile în mod rezonabil, după cum este necesar și adecvat.

(66) Cerințele ar trebui să se aplice sistemelor de IA cu grad ridicat de risc în ceea ce privește gestionarea riscurilor, calitatea și relevanța seturilor de date utilizate, documentația tehnică și păstrarea evidențelor, transparența și furnizarea de informații către implementatori, supravegherea umană, robustețea, acuratețea și securitatea cibernetică. Aceste cerințe sunt necesare pentru a atenua în mod eficace riscurile pentru sănătate, siguranță și drepturile fundamentale. Nefiind disponibile în mod rezonabil alte măsuri mai puțin restrictive privind comerțul, respectivele restricții în calea comerțului nu sunt astfel nejustificate.

(67) Datele de înaltă calitate și accesul la date de înaltă calitate joacă un rol vital în ceea ce privește furnizarea structurii și asigurarea performanței multor sisteme de IA, în special atunci când se utilizează tehnici care implică antrenarea modelelor, 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 o sursă de discriminare, interzisă de dreptul Uniunii. Seturile de date de înaltă calitate de antrenare, de validare și de testare necesită punerea în aplicare a unor practici adecvate de guvernanță și gestionare a datelor. Seturile de date de antrenare, de validare și de testare, inclusiv etichetele, ar trebui să fie relevante, suficient de reprezentative și, pe cât posibil, fără erori și complete, având în vedere scopul preconizat al sistemului. Pentru a facilita respectarea dreptului Uniunii în materie de protecție a datelor, cum ar fi Regulamentul (UE) 2016/679, practicile de guvernanță și gestionare a datelor ar trebui să includă, în cazul datelor cu caracter personal, transparența cu privire la scopul inițial al colectării datelor. Seturile de date ar trebui să aibă, de asemenea, proprietățile statistice adecvate, inclusiv în ceea ce privește persoanele sau grupurile de persoane în legătură cu care se intenționează să fie utilizat sistemul de IA cu grad ridicat de risc, acordând o atenție deosebită atenuării posibilelor prejudecăți din seturile de date, care ar putea afecta sănătatea și siguranța persoanelor, ar putea avea un impact negativ asupra drepturilor fundamentale sau ar putea conduce la discriminare interzisă în temeiul dreptului Uniunii, în special în cazul în care datele de ieșire influențează datele de intrare pentru operațiunile viitoare („bucle de feedback”). Prejudecățile pot fi, de exemplu, inerente seturilor de date subiacente, mai ales când sunt utilizate date istorice, sau pot fi generate în timpul implementării în condiții reale a sistemelor.

Rezultatele produse de sistemele de IA ar putea fi influențate de aceste prejudecăți inerente care tind să crească treptat și astfel să perpetueze și să amplifice discriminarea existentă, în special pentru persoanele care aparțin anumitor grupuri vulnerabile, inclusiv grupuri rasiale sau etnice. Cerința ca seturile de date să fie, pe cât posibil, complete și fără erori nu ar trebui să afecteze utilizarea tehnicilor de protejare a vieții private în contextul dezvoltării și testării sistemelor de IA. În special, seturile de date 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 geografic, contextual, comportamental sau funcțional în care este destinat să fie utilizat sistemul de IA. Cerințele legate de guvernanța datelor pot fi respectate prin recurgerea la părți terțe care oferă servicii de conformitate certificate, inclusiv verificarea guvernanței datelor, a integrității seturilor de date și a practicilor de antrenare, validare și testare a datelor, în măsura în care este asigurată respectarea cerințelor în materie de date din prezentul regulament.

(68) Pentru dezvoltarea și evaluarea sistemelor de IA cu grad ridicat de risc, anumiți actori, cum ar fi furnizorii, organismele notificate și alte entități relevante, cum ar fi centrele europene de inovare digitală, unitățile de testare și experimentare și cercetătorii, ar trebui să poată accesa și utiliza seturi de date de înaltă calitate în domeniile de activitate ale actorilor respectivi 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 privind sănătatea va facilita accesul nediscriminatoriu la datele privind sănătatea și antrenarea algoritmilor IA cu 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.

(69) Dreptul la viața privată și la protecția datelor cu caracter personal trebuie să fie garantat pe parcursul întregului ciclu de viață al sistemului de IA. În acest sens, principiile reducerii la minimum a datelor și protecției datelor începând cu momentul conceperii și în mod implicit, astfel cum sunt prevăzute în dreptul Uniunii privind protecția datelor, sunt aplicabile atunci când sunt prelucrate date cu caracter personal. Măsurile luate de furnizori pentru a asigura respectarea principiilor respective pot include nu numai anonimizarea și criptarea, ci și folosirea unei tehnologii care permite să se aplice algoritmi datelor și antrenarea sistemelor de IA, fără ca aceste date să fie transmise între părți și fără ca înseși datele primare sau datele structurate să fie copiate, fără a aduce atingere cerințelor privind guvernanța datelor prevăzute în prezentul regulament.

(70) Pentru a proteja dreptul altora împotriva discriminării care ar putea rezulta din prejudecățile inerente sistemelor de IA, furnizorii ar trebui să poată să prelucreze și categorii speciale de date cu caracter personal, ca o chestiune de interes public major în înțelesul articolului 9 alineatul (2) litera (g) din Regulamentul (UE) 2016/679 și al articolului 10 alineatul (2) litera (g) din Regulamentul (UE) 2018/1725, în mod excepțional, în măsura în care este strict necesar în scopul asigurării detectării și corectării prejudecăților în legătură cu sistemele de IA cu grad ridicat de risc, sub rezerva unor garanții adecvate pentru drepturile și libertățile fundamentale ale persoanelor fizice și în urma aplicării tuturor condițiilor prevăzute în temeiul prezentului regulament în plus față de condițiile prevăzute în Regulamentele (UE) 2016/679 și (UE) 2018/1725 și în Directiva (UE) 2016/680.

(71) Deținerea de informații ușor de înțeles 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 toată durata lor de viață este esențială pentru a permite trasabilitatea sistemelor respective, pentru a verifica conformitatea cu cerințele prevăzute în prezentul regulament, precum și pentru monitorizarea funcționării lor și pentru monitorizarea ulterioară introducerii pe piață. 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 și a facilita monitorizarea ulterioară introducerii pe piață. Aceste informații ar trebui să includă caracteristicile generale, capabilitățile și limitările sistemului, algoritmii, datele, procesele de antrenare, testare și validare utilizate, precum și documentația privind sistemul relevant de gestionare a riscurilor și ar trebui să fie redactate într-o formă clară și cuprinzătoare. Documentația tehnică ar trebui să fie actualizată permanent și în mod adecvat pe toată durata de viață a sistemului de IA. În plus, sistemele de IA cu grad ridicat de risc ar trebui să permită din punct de vedere tehnic înregistrarea automată a evenimentelor, prin intermediul unor fișiere de jurnalizare, de-a lungul duratei de viață a sistemului.

(72) Pentru a răspunde preocupărilor legate de opacitatea și complexitatea anumitor sisteme de IA și pentru a-i ajuta pe implementatori să își îndeplinească obligațiile care le revin în temeiul prezentului regulament, ar trebui să fie impusă transparența pentru sistemele de IA cu grad ridicat de risc înainte ca acestea să fie introduse pe piață sau puse în funcțiune. Sistemele de IA cu grad ridicat de risc ar trebui să fie proiectate astfel încât să le permită implementatorilor să înțeleagă modul în care funcționează sistemul de IA, să îi evalueze funcționalitatea și să îi înțeleagă punctele forte și limitările. Sistemele de IA cu grad ridicat de risc ar trebui să fie însoțite de informații adecvate sub formă de instrucțiuni de utilizare. Astfel de informații ar trebui să includă caracteristicile, capabilitățile și limitările performanței sistemului de IA. Acestea ar acoperi informații privind posibile circumstanțe cunoscute și previzibile legate de utilizarea sistemului de IA cu grad ridicat de risc, inclusiv acțiuni ale implementatorului care pot influența comportamentul și performanța sistemului, din cauza cărora sistemul de IA poate genera riscuri pentru sănătate, siguranță și drepturile fundamentale, privind modificările care au fost prestabilite și evaluate din punctul de vedere al conformității de către furnizor și privind măsurile relevante de supraveghere umană, inclusiv măsurile de facilitare a interpretării rezultatelor sistemului de IA de către implementatori. Transparența, inclusiv instrucțiunile de utilizare însoțitoare, ar trebui să ajute implementatorii să utilizeze sistemul și să îi sprijine să ia decizii în cunoștință de cauză. Printre altele, implementatorii ar trebui să fie mai în măsură să aleagă corect sistemul pe care intenționează să îl utilizeze, având în vedere obligațiile care le sunt aplicabile, să fie informați despre utilizările preconizate și interzise și să utilizeze sistemul de IA în mod corect și adecvat. Pentru a spori lizibilitatea și accesibilitatea informațiilor incluse în instrucțiunile de utilizare, ar trebui să fie incluse, după caz, exemple ilustrative, de exemplu privind limitările și utilizările preconizate și interzise ale sistemului de IA. Furnizorii ar trebui să se asigure că toată documentația, inclusiv instrucțiunile de utilizare, conține informații semnificative, cuprinzătoare, accesibile și ușor de înțeles, ținând seama de nevoile și cunoștințele previzibile ale implementatorilor vizați. Instrucțiunile de utilizare ar trebui să fie puse la dispoziție într-o limbă ușor de înțeles de către implementatorii vizați, astfel cum se stabilește de statul membru în cauză.

(73) Sistemele de IA cu grad ridicat de risc ar trebui să fie concepute și dezvoltate astfel încât persoanele fizice să poată supraveghea funcționarea lor și să se poată asigura că ele sunt utilizate conform destinației lor și că impactul lor este abordat pe parcursul întregului ciclu de viață al sistemului. 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. De asemenea, este esențial, după caz, să se asigure faptul că sistemele de IA cu grad ridicat de risc includ mecanisme de ghidare și informare a unei persoane fizice căreia i-a fost încredințată supravegherea umană pentru a lua decizii în cunoștință de cauză pentru a stabili dacă, când și cum să intervină pentru a evita consecințele negative sau riscurile sau pentru a opri sistemul dacă nu funcționează astfel cum s-a prevăzut. Având în vedere consecințele semnificative pentru persoane în cazul unei concordanțe incorecte generate de anumite sisteme de identificare biometrică, este oportun să se prevadă o cerință de supraveghere umană mai strictă pentru sistemele respective, astfel încât implementatorul 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 fișierele de jurnalizare generate de sistem. Având în vedere particularitățile din domeniile aplicării legii, migrației, controlului la frontiere și azilului, această cerință nu ar trebui să se aplice în cazul în care dreptul Uniunii sau dreptul intern consideră că aplicarea cerinței respective este disproporționată.

(74) 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, având în vedere scopul lor preconizat și în conformitate cu stadiul de avansare al tehnologiei general recunoscut. Comisia și organizațiile și părțile interesate relevante sunt încurajate să țină seama în mod corespunzător de atenuarea riscurilor și a impacturilor negative ale sistemului de IA. Nivelul preconizat al indicatorilor de performanță ar trebui să fie declarat în instrucțiunile de utilizare însoțitoare. Furnizorii sunt îndemnați să comunice aceste informații implementatorilor într-un mod clar și ușor de înțeles, fără induceri în eroare sau declarații înșelătoare. Dreptul Uniunii privind metrologia legală, inclusiv Directivele 2014/31/UE[35] și 2014/32/UE[36] ale Parlamentului European și ale Consiliului, urmărește să asigure acuratețea măsurătorilor și să contribuie la transparența și echitatea tranzacțiilor comerciale. În acest context, în cooperare cu părțile interesate și organizațiile relevante, cum ar fi autoritățile din domeniul metrologiei și al etalonării, Comisia ar trebui să încurajeze, după caz, elaborarea unor valori de referință și a unor metodologii de măsurare pentru sistemele de IA. În acest sens, Comisia ar trebui să țină seama de partenerii internaționali care lucrează în domeniul metrologiei și al indicatorilor de măsurare relevanți referitori la IA și să colaboreze cu partenerii respectivi.

---

35 Directiva 2014/31/UE a Parlamentului European și a Consiliului din 26 februarie 2014 privind armonizarea legislației statelor membre referitoare la punerea la dispoziție pe piață a aparatelor de cântărit cu funcționare neautomată (JO L 96, 29.3.2014, p. 107).

36 Directiva 2014/32/UE a Parlamentului European și a Consiliului din 26 februarie 2014 privind armonizarea legislației statelor membre referitoare la punerea la dispoziție pe piață a mijloacelor de măsurare (JO L 096, 29.3.2014, p. 149).

(75) 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 prejudiciabil sau altfel indezirabil, care poate rezulta din limitările din cadrul sistemelor sau al mediului în care funcționează sistemele (de exemplu, erori, defecțiuni, inconsecvențe, situații neprevăzute). Prin urmare, ar trebui să fie luate măsuri tehnice și organizatorice pentru a asigura robustețea sistemelor de IA cu grad ridicat de risc, de exemplu prin proiectarea și dezvoltarea de soluții tehnice adecvate pentru a preveni sau a reduce la minimum comportamentul prejudiciabil sau altfel indezirabil în alt mod. Soluțiile tehnice respective pot include, de exemplu, mecanisme 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 distorsionate de prejudecăți generate de sistemul de IA.

(76) 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 se pot folosi de active specifice de IA, cum ar fi seturi de date de antrenament (de exemplu, otrăvirea datelor) sau modele antrenate (de exemplu, atacuri contradictorii sau inferențe din datele membrilor – *membership inference*), 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, cum ar fi controalele de securitate, ținând seama, după caz, și de infrastructura TIC subiacentă.

(77) Fără a aduce atingere cerințelor legate de robustețe și acuratețe prevăzute în prezentul regulament, sistemele de IA cu grad ridicat de risc care intră în domeniul de aplicare al Regulamentului Parlamentului European și al Consiliului privind cerințele orizontale în materie de securitate cibernetică pentru produsele cu elemente digitale, în conformitate cu regulamentul respectiv, pot demonstra conformitatea cu cerințele de securitate cibernetică prevăzute în prezentul regulament prin îndeplinirea cerințelor esențiale de securitate cibernetică prevăzute în regulamentul respectiv. Atunci când îndeplinesc cerințele esențiale ale Regulamentului Parlamentului European și al Consiliului privind cerințele orizontale în materie de securitate cibernetică pentru produsele cu elemente digitale, sistemele de IA cu grad ridicat de risc ar trebui să fie considerate conforme cu cerințele de securitate cibernetică prevăzute în prezentul regulament, în măsura în care îndeplinirea cerințelor respective este demonstrată în declarația de conformitate UE sau în părți ale acesteia emise în temeiul regulamentului respectiv. În acest scop, evaluarea riscurilor în materie de securitate cibernetică asociate unui produs cu elemente digitale clasificat drept sistem de IA cu grad ridicat de risc în conformitate cu prezentul regulament, efectuată în temeiul Regulamentului Parlamentului European și al Consiliului privind cerințele orizontale în materie de securitate cibernetică pentru produsele cu elemente digitale, ar trebui să ia în considerare riscurile la adresa rezilienței cibernetice a unui sistem de IA în ceea ce privește încercările unor părți terțe neautorizate de a-i modifica utilizarea, comportamentul sau performanța, inclusiv vulnerabilitățile specifice IA, cum ar fi otrăvirea datelor sau atacurile contradictorii, precum și, după caz, riscurile la adresa drepturilor fundamentale, astfel cum se prevede în prezentul regulament.

(78) Procedura de evaluare a conformității prevăzută de prezentul regulament ar trebui să se aplice în ceea ce privește cerințele esențiale în materie de securitate cibernetică ale unui produs cu elemente digitale care intră sub incidența Regulamentului Parlamentului European și al Consiliului privind cerințele orizontale în materie de securitate cibernetică pentru produsele cu elemente digitale și clasificat drept sistem de IA cu grad ridicat de risc în temeiul prezentului regulament. Totuși, această regulă nu ar trebui să conducă la reducerea nivelului necesar de asigurare pentru produsele critice cu elemente digitale care intră sub incidența Regulamentului Parlamentului European și al Consiliului privind cerințele orizontale în materie de securitate cibernetică pentru produsele cu elemente digitale. Prin urmare, prin derogare de la această regulă, sistemele de IA cu grad ridicat de risc care intră în domeniul de aplicare al prezentului regulament și care sunt calificate, de asemenea, drept produse importante și critice cu elemente digitale în temeiul Regulamentului Parlamentului European și al Consiliului privind cerințele orizontale în materie de securitate cibernetică pentru produsele cu elemente digitale și cărora li se aplică procedura de evaluare a conformității bazată pe control intern prevăzută într-o anexă la prezentul regulament fac obiectul dispozițiilor privind evaluarea conformității din Regulamentul Parlamentului European și al Consiliului privind cerințele orizontale în materie de securitate cibernetică pentru produsele cu elemente digitale în ceea ce privește cerințele esențiale în materie de securitate cibernetică din regulamentul respectiv. În acest caz, pentru toate celelalte aspecte reglementate de prezentul regulament ar trebui să se aplice dispozițiile respective privind evaluarea conformității bazate pe control intern prevăzute într-o anexă la prezentul regulament. Valorificând cunoașterea și cunoștințele de specialitate din ENISA în ceea ce privește politica în materie de securitate cibernetică și sarcinile atribuite ENISA în temeiul Regulamentului (UE) 2019/881 al Parlamentului European și al Consiliului[37], Comisia ar trebui să coopereze cu ENISA în ceea ce privește aspectele legate de securitatea cibernetică a sistemelor de IA.

---

[37] 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. 15).

(79) 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.

(80) În calitate de semnatare ale Convenției Națiunilor Unite privind drepturile persoanelor cu dizabilități, Uniunea și statele membre sunt obligate din punct de vedere juridic să protejeze persoanele cu dizabilități împotriva discriminării și să promoveze egalitatea acestora, să se asigure că persoanele cu dizabilități au acces, în condiții de egalitate cu ceilalți, la tehnologiile și sistemele informației și comunicațiilor și să garanteze respectarea vieții private a persoanelor cu dizabilități. Având în vedere importanța și utilizarea în creștere a sistemelor de IA, aplicarea principiilor proiectării universale la toate noile tehnologii și servicii ar trebui să asigure accesul deplin și egal al tuturor persoanelor potențial afectate de tehnologiile IA sau care utilizează aceste tehnologii, inclusiv al persoanelor cu dizabilități, într-un mod care să țină seama pe deplin de demnitatea și diversitatea lor inerentă. Prin urmare, este esențial ca furnizorii să asigure conformitatea deplină cu cerințele de accesibilitate, inclusiv cu Directiva (UE) 2016/2102 a Parlamentului European și a Consiliului[38] și cu Directiva (UE) 2019/882. Furnizorii ar trebui să asigure conformitatea cu aceste cerințe din faza de proiectare. Prin urmare, măsurile necesare ar trebui să fie integrate cât mai mult posibil în proiectarea sistemului de IA cu grad ridicat de risc.

---

38 Directiva (UE) 2016/2102 a Parlamentului European și a Consiliului din 26 octombrie 2016 privind accesibilitatea site-urilor web și a aplicațiilor mobile ale organismelor din sectorul public (JO L 327, 2.12.2016, p. 1).

(81) Furnizorul ar trebui să instituie un sistem bine pus la punct 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. Furnizorii de sisteme de IA cu grad ridicat de risc care fac obiectul unor obligații privind sistemele de management al calității în temeiul dreptului sectorial relevant al Uniunii ar trebui să aibă posibilitatea de a include elementele sistemului de management al calității prevăzut în prezentul regulament ca parte a sistemului existent de management al calității prevăzut în respectivul drept sectorial al Uniunii. Complementaritatea dintre prezentul regulament și dreptul sectorial existent al Uniunii ar trebui, de asemenea, să fie luată în considerare în viitoarele activități de standardizare sau orientări adoptate de Comisie. 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.

(82) Pentru a permite aplicarea prezentului regulament și pentru 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, furnizorii stabiliți în țări terțe ar trebui să desemneze, prin mandat scris, un reprezentant autorizat stabilit în Uniune. Respectivul reprezentant 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 furnizorii respectivi care nu sunt stabiliți în Uniune și în îndeplinirea rolului de persoană de contact a acestora stabilită în Uniune.

(83) Având în vedere natura și complexitatea lanțului valoric pentru sistemele de IA și în conformitate cu noul cadru legislativ, este esențial să se asigure securitatea juridică și să se faciliteze respectarea prezentului regulament. Prin urmare, este necesar să se clarifice rolul și obligațiile specifice ale operatorilor relevanți de-a lungul lanțului valoric respectiv, cum ar fi importatorii și distribuitorii care pot contribui la dezvoltarea sistemelor de IA. 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 ca importator.

(84) Pentru a se asigura securitatea juridică, este necesar să se clarifice că, în anumite condiții specifice, orice distribuitor, importator, implementator sau altă parte terță ar trebui să fie considerat drept furnizor al unui sistem de IA cu grad ridicat de risc și, prin urmare, să își asume toate obligațiile relevante. Acest lucru ar fi valabil dacă partea 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, fără a aduce atingere dispozițiilor contractuale care prevăd că obligațiile sunt alocate în alt mod. Acest lucru ar fi valabil și dacă partea respectivă aduce o modificare substanțială unui sistem de IA cu grad ridicat de risc care a fost deja introdus pe piață sau a fost deja pus în funcțiune și într-un mod în care acesta rămâne un sistem de IA cu grad ridicat de risc în conformitate cu prezentul regulament sau dacă modifică scopul preconizat al unui sistem de IA, inclusiv al unui sistem de IA de uz general, care nu a fost clasificat ca prezentând un grad ridicat de risc și care a fost deja introdus pe piață sau pus în funcțiune, într-un mod în care sistemul de IA devine un sistem de IA cu grad ridicat de risc în conformitate cu prezentul regulament. Aceste dispoziții ar trebui să se aplice fără a aduce atingere dispozițiilor mai specifice stabilite în anumite acte legislative de armonizare ale Uniunii întemeiate pe noul cadru legislativ, împreună cu care ar trebui să se aplice prezentul regulament. De exemplu, articolul 16 alineatul (2) din Regulamentul (UE) 2017/745, 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.

(85) Sistemele de IA de uz general pot fi utilizate în sine ca sisteme de IA cu grad ridicat de risc sau pot fi componente ale altor sisteme de IA cu grad ridicat de risc. Prin urmare, având în vedere natura lor specifică și pentru a asigura o partajare echitabilă a responsabilităților de-a lungul lanțului valoric al IA, furnizorii de astfel de sisteme ar trebui, indiferent dacă pot fi utilizate ca sisteme de IA cu grad ridicat de risc ca atare de alți furnizori sau drept componente ale unor sisteme de IA cu grad ridicat de risc și cu excepția cazului în care se prevede altfel în prezentul regulament, să coopereze îndeaproape cu furnizorii sistemelor de IA cu grad ridicat de risc relevante pentru a permite respectarea de către acestea a obligațiilor relevante în temeiul prezentului regulament și cu autoritățile competente instituite în temeiul prezentului regulament.

(86) În cazul în care, în condițiile prevăzute în prezentul regulament, furnizorul care a introdus inițial sistemul de IA pe piață sau l-a pus în funcțiune nu ar mai trebui să fie considerat furnizor în sensul prezentului regulament și în cazul în care furnizorul respectiv nu a exclus în mod expres schimbarea sistemului de IA într-un sistem de IA cu grad ridicat de risc, primul furnizor ar trebui totuși să coopereze îndeaproape, să pună la dispoziție informațiile necesare și să furnizeze accesul tehnic și alte tipuri de asistență preconizate în mod rezonabil care sunt necesare pentru îndeplinirea obligațiilor prevăzute în prezentul regulament, în special în ceea ce privește respectarea cerințelor privind evaluarea conformității sistemelor de IA cu grad ridicat de risc.

(87) În plus, în cazul în care un sistem de IA cu grad ridicat de risc care este o componentă de siguranță a unui produs care intră în domeniul de aplicare al legislației de armonizare a Uniunii întemeiate pe noul cadru legislativ nu este introdus pe piață sau pus în funcțiune independent de produs, fabricantul produsului definit în legislația respectivă ar trebui să respecte obligațiile furnizorului stabilite în prezentul regulament și ar trebui, în special, să se asigure că sistemul de IA încorporat în produsul final respectă cerințele prezentului regulament.

(88) De-a lungul lanțului valoric al IA, numeroase părți furnizează adesea sisteme, instrumente și servicii de IA, dar și componente sau procese care sunt încorporate de furnizor în sistemul de IA, cu diferite obiective, inclusiv antrenarea modelelor, reconversia modelelor, testarea și evaluarea modelelor, integrarea în software sau alte aspecte ale dezvoltării de modele. Respectivele părți au un rol important în lanțul valoric față de furnizorul sistemului de IA cu grad ridicat de risc în care sunt integrate sistemele, instrumentele, serviciile, componentele sau procesele lor de IA și ar trebui să îi ofere acestui furnizor, printr-un acord scris, informațiile, capabilitățile, accesul tehnic și alte tipuri de asistență necesare bazate pe stadiul de avansare al tehnologiei general recunoscut, pentru a permite furnizorului să respecte pe deplin obligațiile prevăzute în prezentul regulament, fără a-și compromite propriile drepturi de proprietate intelectuală sau secrete comerciale.

(89) Părțile terțe care pun la dispoziția publicului instrumente, servicii, procese sau componente de IA, altele decât modelele de IA de uz general, ar trebui să nu fie obligate să respecte cerințe care vizează responsabilitățile de-a lungul lanțului valoric al IA, în special față de furnizorul care le-a utilizat sau le-a integrat, atunci când aceste instrumente, servicii, procese sau componente de IA sunt puse la dispoziție sub licență liberă și deschisă. Dezvoltatorii de instrumente, servicii, procese sau componente de IA libere și cu sursă deschisă, altele decât modelele de IA de uz general, ar trebui să fie încurajați să pună în aplicare practici de documentare adoptate pe scară largă, cum ar fi carduri însoțitoare ale modelelor și fișe de date, ca modalitate de a accelera schimbul de informații de-a lungul lanțului valoric al IA, permițând promovarea unor sisteme de IA fiabile în Uniune.

(90) Comisia ar putea elabora și recomanda un model voluntar de clauze contractuale între furnizorii de sisteme de IA cu grad ridicat de risc și părțile terțe care furnizează instrumente, servicii, componente sau procese care sunt utilizate sau integrate în sistemele de IA cu grad ridicat de risc, pentru a facilita cooperarea de-a lungul lanțului valoric. Atunci când elaborează modelul voluntar de clauze contractuale, Comisia ar trebui să ia în considerare și eventualele cerințe contractuale aplicabile în anumite sectoare sau situații economice.

(91) 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 implementatori. Implementatorii ar trebui, în special, să ia măsurile tehnice și organizatorice adecvate pentru a se asigura că utilizează sisteme de IA cu grad ridicat de risc în conformitate cu instrucțiunile de utilizare și ar trebui să fie prevăzute și alte obligații în ceea ce privește monitorizarea funcționării sistemelor de IA și păstrarea evidențelor, după caz. În plus, implementatorii ar trebui să se asigure că persoanele desemnate să pună în aplicare instrucțiunile de utilizare și supravegherea umană, astfel cum sunt prevăzute în prezentul regulament, au competența necesară, în special un nivel adecvat de alfabetizare, formare și autoritate în domeniul IA pentru a îndeplini în mod corespunzător sarcinile respective. Respectivele obligații nu ar trebui să aducă atingere altor obligații ale implementatorilor în ceea ce privește sistemele de IA cu grad ridicat de risc în temeiul dreptului Uniunii sau al dreptului intern.

(92) Prezentul regulament nu aduce atingere obligațiilor angajatorilor de a informa sau de a informa și consulta lucrătorii sau reprezentanții acestora în temeiul dreptului și al practicilor Uniunii sau naționale, inclusiv al Directivei 2002/14/CE a Parlamentului European și a Consiliului[39], cu privire la deciziile de punere în funcțiune sau de utilizare a sistemelor de IA. Este în continuare necesar să se asigure informarea lucrătorilor și a reprezentanților acestora cu privire la implementarea planificată a sistemelor de IA cu grad ridicat de risc la locul de muncă în cazul în care nu sunt îndeplinite condițiile pentru respectivele obligații de informare sau de informare și consultare prevăzute în alte instrumente juridice. În plus, un astfel de drept la informare este auxiliar și necesar în raport cu obiectivul de protecție a drepturilor fundamentale care stă la baza prezentului regulament. Prin urmare, prezentul regulament ar trebui să prevadă o cerință de informare în acest sens, fără a afecta drepturile existente ale lucrătorilor.

[39] Directiva 2002/14/CE a Parlamentului European și a Consiliului din 11 martie 2002 de stabilire a unui cadru general de informare și consultare a lucrătorilor din Comunitatea Europeană (JO L 80, 23.3.2002, p. 29).

(93) Deși riscurile legate de sistemele de IA pot rezulta din modul în care sunt proiectate sistemele respective, pot decurge riscuri și din modul în care aceste sisteme de IA sunt utilizate. Prin urmare, implementatorii sistemelor de IA cu grad ridicat de risc joacă un rol esențial în garantarea faptului că drepturile fundamentale sunt protejate, completând obligațiile furnizorului la dezvoltarea sistemului de IA. Implementatorii sunt cei mai în măsură să înțeleagă modul în care sistemul de IA cu grad ridicat de risc va fi utilizat concret și, prin urmare, pot identifica potențialele riscuri semnificative care nu au fost prevăzute în faza de dezvoltare, datorită cunoașterii mai exacte a contextului de utilizare, a persoanelor sau a grupurilor de persoane care ar putea fi afectate, inclusiv a grupurilor vulnerabile. Implementatorii de sisteme de IA cu grad ridicat de risc enumerate într-o anexă la prezentul regulament joacă, de asemenea, un rol esențial în informarea persoanelor fizice și ar trebui, atunci când iau decizii sau contribuie la luarea deciziilor referitoare la persoane fizice, după caz, să informeze persoanele fizice că fac obiectul utilizării sistemului de IA cu grad ridicat de risc. Aceste informații ar trebui să includă scopul urmărit și tipul de decizii luate. Implementatorul ar trebui, de asemenea, să informeze persoanele fizice cu privire la dreptul lor la o explicație furnizată în temeiul prezentului regulament. În ceea ce privește sistemele de IA cu grad ridicat de risc utilizate în scopul aplicării legii, această obligație ar trebui să fie pusă în aplicare în conformitate cu articolul 13 din Directiva (UE) 2016/680.

(94) Orice prelucrare a datelor biometrice implicate în utilizarea sistemelor de IA pentru identificarea biometrică în scopul aplicării legii trebuie să respecte articolul 10 din Directiva (UE) 2016/680, care permite o astfel de prelucrare numai atunci când este strict necesară, sub rezerva unor garanții adecvate pentru drepturile și libertățile persoanei vizate, și atunci când este autorizată de dreptul Uniunii sau de dreptul intern. O astfel de utilizare, atunci când este autorizată, trebuie, de asemenea, să respecte principiile prevăzute la articolul 4 alineatul (1) din Directiva (UE) 2016/680, inclusiv legalitatea, echitatea și transparența, limitarea scopului, exactitatea și limitarea stocării.

(95) Fără a aduce atingere dreptului aplicabil al Uniunii, în special Regulamentului (UE) 2016/679 și Directivei (UE) 2016/680, având în vedere caracterul intruziv al sistemelor de identificare biometrică la distanță ulterioară, utilizarea sistemelor de identificare biometrică la distanță ulterioară ar trebui să facă obiectul unor garanții. Sistemele de identificare biometrică la distanță ulterioară ar trebui să fie utilizate întotdeauna într-un mod proporțional, legitim și strict necesar și, prin urmare, adaptat, în ceea ce privește persoanele care urmează să fie identificate, localizarea, acoperirea temporală și pe baza unui set de date închis de înregistrări video obținute în mod legal. În orice caz, sistemele de identificare biometrică la distanță ulterioară nu ar trebui să fie utilizate în cadrul aplicării legii pentru a conduce la o supraveghere arbitrară. Condițiile pentru identificarea biometrică la distanță ulterioară nu ar trebui, în niciun caz, să ofere o bază pentru a eluda condițiile interdicției și excepțiile stricte pentru identificarea biometrică la distanță în timp real.

(96) Pentru a se asigura în mod eficient că drepturile fundamentale sunt protejate, implementatorii de sisteme de IA cu grad ridicat de risc care sunt organisme de drept public sau entitățile private care furnizează servicii publice și implementatorii care implementează anumite sisteme de IA cu grad ridicat de risc enumerate într-o anexă la prezentul regulament, cum ar fi entitățile bancare sau de asigurări, ar trebui să efectueze o evaluare a impactului asupra drepturilor fundamentale înainte de a pune aceste sisteme în funcțiune. Serviciile importante pentru persoanele fizice care sunt de natură publică pot fi furnizate și de entități private. Entitățile private care furnizează astfel de servicii publice sunt legați de sarcini de interes public, cum ar fi în domeniul educației, al îngrijirilor de sănătate, al serviciilor sociale, al locuințelor, al administrării justiției. Scopul evaluării impactului asupra drepturilor fundamentale este ca implementatorul să identifice riscurile specifice pentru drepturile persoanelor sau ale grupurilor de persoane care ar putea fi afectate și să identifice măsurile care trebuie luate în cazul materializării riscurilor respective. Evaluarea impactului ar trebui să fie efectuată înainte de implementarea sistemului de IA cu grad ridicat de risc și ar trebui să fie actualizată atunci când implementatorul consideră că oricare dintre factorii relevanți s-au schimbat. Evaluarea impactului ar trebui să identifice procesele relevante ale implementatorului în care sistemul de IA cu grad ridicat de risc va fi utilizat în conformitate cu scopul său preconizat și ar trebui să includă o descriere a perioadei de timp și a frecvenței în care se intenționează utilizarea sistemului, precum și a categoriilor specifice de persoane fizice și grupuri care sunt susceptibile de a fi afectate în contextul specific de utilizare.

Evaluarea ar trebui să includă, de asemenea, identificarea riscurilor specifice de prejudiciu care ar putea avea un impact asupra drepturilor fundamentale ale persoanelor sau grupurilor respective. Atunci când efectuează această evaluare, implementatorul ar trebui să țină seama de informațiile relevante pentru o evaluare adecvată a impactului, inclusiv de informațiile furnizate de furnizorul sistemului de IA cu grad ridicat de risc în instrucțiunile de utilizare, dar fără a se limita la aceste informații. Având în vedere riscurile identificate, implementatorii ar trebui să stabilească măsurile care trebuie luate în cazul materializării acestor riscuri, inclusiv, de exemplu, mecanisme de guvernanță în acest context specific de utilizare, cum ar fi mecanisme de supraveghere umană în conformitate cu instrucțiunile de utilizare sau proceduri de tratare a plângerilor și proceduri aferente măsurilor reparatorii, deoarece acestea ar putea fi esențiale pentru atenuarea riscurilor la adresa drepturilor fundamentale în cazuri concrete de utilizare. După efectuarea respectivei evaluări a impactului, implementatorul ar trebui să îi notifice acest lucru autorității relevante de supraveghere a pieței. După caz, pentru a colecta informațiile relevante necesare pentru efectuarea evaluării impactului, implementatorii de sisteme de IA cu grad ridicat de risc, în special atunci când sistemele de IA sunt utilizate în sectorul public, ar putea implica părțile interesate relevante, inclusiv reprezentanții grupurilor de persoane susceptibile de a fi afectate de sistemul de IA, experții independenți și organizațiile societății civile în efectuarea unor astfel de evaluări ale impactului și în conceperea măsurilor care trebuie luate în cazul materializării riscurilor. Oficiul european pentru inteligența artificială (Oficiul pentru IA) ar trebui să elaboreze un model de chestionar pentru a facilita conformitatea și a reduce sarcina administrativă pentru implementatori.

(97) Noțiunea de modele de IA de uz general ar trebui să fie definită în mod clar și separată de noțiunea de sisteme de IA pentru a asigura securitatea juridică. Definiția ar trebui să se bazeze pe caracteristicile funcționale esențiale ale unui model de IA de uz general, în special pe generalitate și pe capabilitatea de a îndeplini în mod competent o gamă largă de sarcini distincte. Aceste modele sunt, de regulă, antrenate pe volume mari de date, prin diverse metode, cum ar fi învățarea autosupravegheată, nesupravegheată sau prin întărire. Modelele de IA de uz general pot fi introduse pe piață în diferite moduri, inclusiv prin biblioteci, interfețe de programare a aplicațiilor (API), sub formă de descărcare directă sau sub formă de copie fizică. Aceste modele pot fi modificate suplimentar sau calibrate și astfel transformate în modele noi. Deși modelele de IA sunt componente esențiale ale sistemelor de IA, ele nu constituie sisteme de IA în sine. Modelele de IA necesită adăugarea de componente suplimentare, cum ar fi, de exemplu, o interfață cu utilizatorul, pentru a deveni sisteme de IA. Modelele de IA sunt, de regulă, integrate în sistemele de IA și fac parte din acestea. Prezentul regulament prevede norme specifice pentru modelele de IA de uz general și pentru modelele de IA de uz general care prezintă riscuri sistemice, norme care ar trebui să se aplice și atunci când aceste modele sunt integrate sau fac parte dintr-un sistem de IA. Ar trebui să se înțeleagă că obligațiile furnizorilor de modele de IA de uz general ar trebui să se aplice odată ce modelele de IA de uz general sunt introduse pe piață.

Atunci când furnizorul unui model de IA de uz general integrează un model propriu în propriul sistem de IA care este pus la dispoziție pe piață sau pus în funcțiune, modelul respectiv ar trebui să fie considerat ca fiind introdus pe piață și, prin urmare, obligațiile prevăzute în prezentul regulament pentru modele ar trebui să se aplice în continuare în plus față de cele pentru sistemele de IA. Obligațiile stabilite pentru modele nu ar trebui în niciun caz să se aplice atunci când un model propriu este utilizat pentru procese pur interne care nu sunt esențiale pentru furnizarea unui produs sau a unui serviciu către terți, iar drepturile persoanelor fizice nu sunt afectate. Având în vedere potențialele lor efecte negative semnificative, modelele de IA de uz general cu risc sistemic ar trebui să facă întotdeauna obiectul obligațiilor relevante în temeiul prezentului regulament. Definiția nu ar trebui să acopere modelele de IA utilizate înainte de introducerea lor pe piață în scopul unic al activităților de cercetare, dezvoltare și creare de prototipuri. Acest lucru nu aduce atingere obligației de a se conforma prezentului regulament atunci când, în urma unor astfel de activități, se introduce pe piață un model.

(98) În timp ce generalitatea unui model ar putea fi determinată, printre altele, și de o serie de parametri, ar trebui să se considere că modelele cu cel puțin un miliard de parametri și antrenate cu un volum mare de date utilizând autosupravegherea la scară largă prezintă o generalitate semnificativă și îndeplinesc în mod competent o gamă largă de sarcini distincte.

(99) Modelele de IA generative de mari dimensiuni sunt un exemplu tipic de model de IA de uz general, având în vedere că permit generarea flexibilă de conținut, cum ar fi sub formă de text, audio, imagini sau video, care pot răspunde cu ușurință unei game largi de sarcini distincte.

(100) Atunci când un model de IA de uz general este integrat într-un sistem de IA sau face parte dintr-un astfel de sistem, acest sistem ar trebui să fie considerat a fi un sistem de IA de uz general atunci când, în urma acestei integrări, acest sistem are capabilitatea de a servi unei varietăți de scopuri. Un sistem de IA de uz general poate fi utilizat direct sau poate fi integrat în alte sisteme de IA.

(101) Furnizorii de modele de IA de uz general au un rol și o responsabilitate deosebite de-a lungul lanțului valoric al IA, deoarece modelele pe care le furnizează pot constitui baza pentru o serie de sisteme din aval, adesea furnizate de furnizori din aval care au nevoie de o bună înțelegere a modelelor și a capabilităților acestora, atât pentru a permite integrarea unor astfel de modele în produsele lor, cât și pentru a-și îndeplini obligațiile care le revin în temeiul prezentului regulament sau al altor regulamente. Prin urmare, ar trebui să fie stabilite măsuri proporționale de transparență, inclusiv întocmirea și ținerea la zi a documentației, precum și furnizarea de informații privind modelul de IA de uz general pentru utilizarea sa de către furnizorii din aval. Documentația tehnică ar trebui să fie pregătită și ținută la zi de către furnizorul modelului de IA de uz general în scopul de a o pune, la cerere, la dispoziția Oficiului pentru IA și a autorităților naționale competente. Setul minim de elemente care trebuie incluse în această documentație ar trebui să fie stabilit în anexele specifice la prezentul regulament. Comisia ar trebui să fie împuternicită să modifice anexele respective prin intermediul unor acte delegate în funcție de evoluțiile tehnologice.

(102) Software-ul și datele, inclusiv modelele, lansate sub licență liberă și cu sursă deschisă care le permite să fie partajate în mod deschis și pe care utilizatorii le pot accesa, utiliza, modifica și redistribui liber sau versiuni modificate ale acestora, pot contribui la cercetare și inovare pe piață și pot oferi oportunități semnificative de creștere pentru economia Uniunii. Ar trebui să se considere că modelele de IA de uz general lansate sub licențe libere și cu sursă deschisă asigură niveluri ridicate de transparență și deschidere dacă parametrii lor, inclusiv ponderile, informațiile privind arhitectura modelului și informațiile privind utilizarea modelului, sunt puși la dispoziția publicului. Licența ar trebui să fie considerată ca fiind liberă și cu sursă deschisă și atunci când le permite utilizatorilor să ruleze, să copieze, să distribuie, să studieze, să modifice și să îmbunătățească software-ul și datele, inclusiv modelele, cu condiția ca furnizorul inițial al modelului să fie menționat și ca termenii de distribuție identici sau comparabili să fie respectați.

(103) Componentele de IA libere și cu sursă deschisă acoperă software-ul și datele, inclusiv modelele și modelele, instrumentele, serviciile sau procesele de IA de uz general ale unui sistem de IA. Componentele de IA libere și cu sursă deschisă pot fi furnizate prin diferite canale, inclusiv prin dezvoltarea lor în depozite deschise. În sensul prezentului regulament, componentele de IA care sunt furnizate contra unui preț sau monetizate în alt mod, inclusiv prin furnizarea de sprijin tehnic sau de alte servicii, inclusiv prin intermediul unei platforme software, legate de componenta de IA, sau utilizarea datelor cu caracter personal din alte motive decât în scopul exclusiv de îmbunătățire a securității, a compatibilității sau a interoperabilității software-ului, cu excepția tranzacțiilor dintre microîntreprinderi, nu ar trebui să beneficieze de excepțiile prevăzute pentru componentele de IA libere și cu sursă deschisă. Punerea la dispoziție a componentelor de IA prin intermediul depozitelor deschise nu ar trebui, în sine, să constituie o monetizare.

(104) Furnizorii de modele de IA de uz general care sunt lansate sub licență liberă și cu sursă deschisă și ai căror parametri, inclusiv ponderile, informațiile privind arhitectura modelului și informațiile privind utilizarea modelului, sunt puși la dispoziția publicului ar trebui să facă obiectul unor excepții în ceea ce privește cerințele legate de transparență impuse modelelor de IA de uz general, cu excepția cazului în care se poate considera că prezintă un risc sistemic, caz în care circumstanța că modelul este transparent și însoțit de o licență cu sursă deschisă nu ar trebui să fie considerată un motiv suficient pentru a exclude respectarea obligațiilor prevăzute în prezentul regulament. În orice caz, având în vedere că lansarea modelelor de IA de uz general sub licență liberă și cu sursă deschisă nu dezvăluie neapărat informații substanțiale cu privire la setul de date utilizat pentru antrenarea sau calibrarea modelului și la modul în care a fost astfel asigurată conformitatea cu dreptul privind drepturile de autor, excepția prevăzută pentru modelele de IA de uz general de la respectarea cerințelor legate de transparență nu ar trebui să se refere la obligația de a prezenta un rezumat cu privire la conținutul utilizat pentru antrenarea modelelor și la obligația de a institui o politică de respectare a dreptului Uniunii privind drepturile de autor, în special pentru a identifica și a respecta rezervarea drepturilor în temeiul articolului 4 alineatul (3) din Directiva (UE) 2019/790 a Parlamentului European și a Consiliului[40].

[40] Directiva (UE) 2019/790 a Parlamentului European și a Consiliului din 17 aprilie 2019 privind dreptul de autor și drepturile conexe pe piața unică digitală și de modificare a Directivelor 96/9/CE și 2001/29/CE (JO L 130, 17.5.2019, p. 92).

(105) Modelele de IA de uz general, în special modelele de IA generative de mari dimensiuni, capabile să genereze text, imagini și alte conținuturi, prezintă oportunități unice de inovare, dar și provocări pentru artiști, autori și alți creatori și pentru modul în care conținutul lor creativ este creat, distribuit, utilizat și consumat. Dezvoltarea și antrenarea unor astfel de modele necesită acces la volume mari de text, imagini, materiale video și alte date. Tehnicile de extragere a textului și a datelor pot fi utilizate pe scară largă în acest context pentru obținerea și analizarea unui astfel de conținut, care poate fi protejat prin drepturi de autor și drepturi conexe. Orice utilizare a unui conținut protejat prin drepturi de autor necesită autorizare din partea titularului de drepturi în cauză, cu excepția cazului în care se aplică excepții și limitări relevante ale drepturilor de autor. Directiva (UE) 2019/790 a introdus excepții și limitări care permit reproduceri și extrageri ale operelor sau ale altor obiecte protejate, în scopul extragerii de text și de date, în anumite condiții. În temeiul acestor norme, titularii de drepturi pot alege să își rezerve drepturile asupra operelor lor sau asupra altor obiecte protejate ale lor pentru a preveni extragerea de text și de date, cu excepția cazului în care acest lucru se face în scopul cercetării științifice. În cazul în care drepturile de neparticipare au fost rezervate în mod expres într-un mod adecvat, furnizorii de modele de IA de uz general trebuie să obțină o autorizație din partea titularilor de drepturi dacă doresc să efectueze extragere de text și de date din astfel de opere.

(106) Furnizorii care introduc modele de IA de uz general pe piața Uniunii ar trebui să asigure respectarea obligațiilor relevante prevăzute în prezentul regulament. În acest scop, furnizorii de modele de IA de uz general ar trebui să instituie o politică de respectare a dreptului Uniunii privind drepturile de autor și drepturile conexe, în special pentru a identifica și a respecta rezervarea drepturilor exprimată de titularii de drepturi în temeiul articolului 4 alineatul (3) din Directiva (UE) 2019/790. Orice furnizor care introduce un model de IA de uz general pe piața Uniunii ar trebui să respecte această obligație, indiferent de jurisdicția în care au loc actele relevante pentru drepturile de autor care stau la baza antrenării respectivelor modele de IA de uz general. Acest lucru este necesar pentru a asigura condiții de concurență echitabile între furnizorii de modele de IA de uz general, în care niciun furnizor nu ar trebui să poată obține un avantaj competitiv pe piața Uniunii prin aplicarea unor standarde privind drepturile de autor mai scăzute decât cele prevăzute în Uniune.

(107) Pentru a spori transparența datelor utilizate în preantrenarea și antrenarea modelelor de IA de uz general, inclusiv a textului și a datelor protejate de dreptul privind drepturile de autor, este adecvat ca furnizorii de astfel de modele să elaboreze și să pună la dispoziția publicului un rezumat suficient de detaliat al conținutului utilizat pentru antrenarea modelului de IA de uz general. Ținând seama în mod corespunzător de necesitatea de a proteja secretele comerciale și informațiile comerciale confidențiale, acest rezumat ar trebui să aibă un domeniu de aplicare în general cuprinzător, în loc să fie detaliat din punct de vedere tehnic, pentru a facilita părților cu interese legitime, inclusiv titularilor de drepturi de autor, să își exercite drepturile și să asigure respectarea drepturilor lor în temeiul dreptului Uniunii, de exemplu prin enumerarea principalelor colecții sau seturi de date folosite la antrenarea modelului, cum ar fi bazele de date sau arhivele de date de mari dimensiuni, private sau publice, și prin furnizarea unei explicații narative cu privire la alte surse de date utilizate. Este oportun ca Oficiul pentru IA să furnizeze un model pentru rezumat, care ar trebui să fie simplu, eficace și să permită furnizorului să furnizeze rezumatul solicitat sub formă narativă.

(108) În ceea ce privește obligațiile impuse furnizorilor de modele de IA de uz general de a institui o politică de respectare a dreptul Uniunii privind drepturile de autor și de a pune la dispoziția publicului un rezumat al conținutului utilizat pentru antrenare, Oficiul pentru IA ar trebui să monitorizeze dacă furnizorul și-a îndeplinit obligațiile respective fără a verifica sau a efectua o evaluare operă cu operă a datelor de antrenament în ceea ce privește respectarea drepturilor de autor. Prezentul regulament nu aduce atingere aplicării normelor în materie de drepturi de autor prevăzute în dreptul Uniunii.

(109) Respectarea obligațiilor aplicabile furnizorilor de modele de IA de uz general ar trebui să fie corespunzătoare și proporțională cu tipul de furnizor de model, excluzând necesitatea respectării pentru persoanele care dezvoltă sau utilizează modele în alte scopuri decât cele profesionale sau de cercetare științifică, care ar trebui totuși să fie încurajate să respecte în mod voluntar aceste cerințe. Fără a aduce atingere dreptului Uniunii privind drepturile de autor, respectarea obligațiilor respective ar trebui să țină seama în mod corespunzător de dimensiunea furnizorului și să permită modalități simplificate de asigurare a respectării cerințelor pentru IMM-uri, inclusiv pentru întreprinderile nou-înființate, care nu ar trebui să reprezinte un cost excesiv și să descurajeze utilizarea unor astfel de modele. În cazul unei modificări sau calibrări a unui model, obligațiile furnizorilor de modele de IA de uz general ar trebui să se limiteze la modificarea sau calibrarea respectivă, de exemplu prin completarea documentației tehnice deja existente cu informații privind modificările, inclusiv noi surse de date de antrenament, ca mijloc de respectare a obligațiilor privind lanțul valoric prevăzute în prezentul regulament.

(110) Modelele de IA de uz general ar putea prezenta riscuri sistemice care includ, printre altele, orice efecte negative reale sau previzibile în mod rezonabil în legătură cu accidente majore, perturbări ale sectoarelor critice și consecințe grave pentru sănătatea și siguranța publică, orice efecte negative reale sau previzibile în mod rezonabil asupra proceselor democratice, asupra securității publice și economice, diseminarea de conținut ilegal, fals sau discriminatoriu. Riscurile sistemice ar trebui să fie înțelese ca crescând odată cu capabilitățile modelului și cu amploarea modelului, pot apărea de-a lungul întregului ciclu de viață al modelului și sunt influențate de condițiile de utilizare necorespunzătoare, de fiabilitatea modelului, de echitatea modelului și de securitatea modelului, de nivelul de autonomie a modelului, de accesul său la instrumente, de modalitățile noi sau combinate, de strategiile de lansare și distribuție, de potențialul de eliminare a mecanismelor de protecție și de alți factori. În special, abordările internaționale au identificat până în prezent necesitatea de a acorda atenție riscurilor generate de potențialele utilizări necorespunzătoare intenționate sau de problemele neintenționate de control legate de alinierea la intenția umană; riscurilor chimice, biologice, radiologice și nucleare, cum ar fi modalitățile de reducere a barierelor la intrare, inclusiv pentru dezvoltarea, proiectarea, achiziționarea sau utilizarea de arme; capabilităților cibernetice ofensive, cum ar fi modalitățile care permit descoperirea, exploatarea sau utilizarea operațională a vulnerabilităților; efectelor interacțiunii și ale utilizării instrumentelor, inclusiv, de exemplu, capacitatea de a controla sistemele fizice și de a interfera cu infrastructura critică; riscurilor legate de posibilitatea ca modelele să facă copii după ele însele sau să se „autoreproducă” ori să antreneze alte modele; modurilor în care modelele pot da naștere unor prejudecăți dăunătoare și discriminării cu riscuri pentru indivizi, comunități sau societăți; facilitării dezinformării sau prejudicierii vieții private cu amenințări la adresa valorilor democratice și a drepturilor omului; riscului ca un anumit eveniment să conducă la o reacție în lanț cu efecte negative considerabile care ar putea afecta până la un întreg oraș, o întreagă activitate de domeniu sau o întreagă comunitate.

(111) Este oportun să se stabilească o metodologie pentru clasificarea modelelor de IA de uz general ca modele de IA de uz general cu riscuri sistemice. Întrucât riscurile sistemice rezultă din capabilități deosebit de ridicate, ar trebui să se considere că un model de IA de uz general prezintă riscuri sistemice dacă are capabilități cu impact ridicat, evaluate pe baza unor instrumente și metodologii tehnice adecvate sau dacă are un impact semnificativ asupra pieței interne din cauza amplorii sale. Capabilități cu impact ridicat în modelele de IA de uz general înseamnă capabilități care corespund capabilităților înregistrate în cele mai avansate modele de IA de uz general sau depășesc capabilitățile respective. Întreaga gamă de capabilități ale unui model ar putea fi mai bine înțeleasă după introducerea sa pe piață sau atunci când implementatorii interacționează cu modelul. În conformitate cu stadiul actual al tehnologiei la momentul intrării în vigoare a prezentului regulament, volumul cumulat de calcul utilizat pentru antrenarea modelului de IA de uz general măsurat în operații în virgulă mobilă este una dintre aproximările relevante pentru capabilitățile modelului. Volumul cumulat de calcul utilizat pentru antrenare include calculul utilizat pentru toate activitățile și metodele menite să consolideze capabilitățile modelului înainte de implementare, cum ar fi preantrenarea, generarea de date sintetice și calibrarea. Prin urmare, ar trebui să fie stabilit un prag inițial de operații în virgulă mobilă, care, dacă este atins de un model de IA de uz general, conduce la prezumția că modelul este un model de IA de uz general cu riscuri sistemice. Acest prag ar trebui să fie ajustat în timp pentru a reflecta schimbările tehnologice și industriale, cum ar fi îmbunătățirile algoritmice sau eficiența hardware sporită, și ar trebui să fie completat cu valori de referință și indicatori pentru capabilitatea modelului.

În acest scop, Oficiul pentru IA ar trebui să colaboreze cu comunitatea științifică, cu industria, cu societatea civilă și cu alți experți. Pragurile, precum și instrumentele și valorile de referință pentru evaluarea capabilităților cu impact ridicat ar trebui să fie indicatori puternici ai generalității, ai capabilităților modelului și ai riscului sistemic asociat modelelor de IA de uz general și ar putea lua în considerare modul în care modelul va fi introdus pe piață sau numărul de utilizatori pe care îi poate afecta. Pentru a completa acest sistem, Comisia ar trebui să aibă posibilitatea de a lua decizii individuale de desemnare a unui model de IA de uz general ca model de IA de uz general cu risc sistemic dacă se constată că un astfel de model are capabilități sau un impact echivalent cu cele acoperite de pragul stabilit. Decizia respectivă ar trebui luată pe baza unei evaluări globale a criteriilor pentru desemnarea unui model de IA de uz general cu risc sistemic prevăzute într-o anexă la prezentul regulament, cum ar fi calitatea sau dimensiunea setului de date de antrenament, numărul de utilizatori comerciali și finali, modalitățile referitoare la datele de intrare și de ieșire ale modelului, nivelul său de autonomie și de scalabilitate sau instrumentele la care are acces. La cererea motivată a unui furnizor al cărui model a fost desemnat drept model de IA de uz general cu risc sistemic, Comisia ar trebui să țină seama de cerere și poate decide să reevalueze dacă modelul de IA de uz general poate fi considerat în continuare ca prezentând riscuri sistemice.

(112) De asemenea, este necesar să se clarifice o procedură pentru clasificarea unui model de IA de uz general cu riscuri sistemice. Un model de IA de uz general care respectă pragul aplicabil pentru capabilitățile cu impact ridicat ar trebui să fie prezumat ca fiind un model de IA de uz general cu risc sistemic. Furnizorul ar trebui să notifice Oficiul pentru IA în termen de cel mult două săptămâni de la îndeplinirea cerințelor sau de la data la care devine cunoscut faptul că un model de IA de uz general va îndeplini cerințele care conduc la prezumția respectivă. Acest lucru este deosebit de relevant în legătură cu pragul de operații în virgulă mobilă, deoarece antrenarea modelelor de IA de uz general necesită o planificare considerabilă, care include alocarea în avans a resurselor de calcul și, prin urmare, furnizorii de modele de IA de uz general sunt în măsură să știe dacă modelul lor ar atinge pragul înainte de finalizarea antrenării. În contextul notificării respective, furnizorul ar trebui să poată demonstra că, având în vedere caracteristicile sale specifice, un model de IA de uz general nu prezintă, în mod excepțional, riscuri sistemice și că, prin urmare, nu ar trebui să fie clasificat drept model de IA de uz general cu riscuri sistemice. Aceste informații sunt valoroase deoarece Oficiul pentru IA poate să anticipeze introducerea pe piață a modelelor de IA de uz general cu riscuri sistemice, iar furnizorii pot începe să colaboreze cu Oficiul pentru IA din timp. Aceste informații sunt deosebit de importante în ceea ce privește modelele de IA de uz general care sunt planificate să fie lansate ca sursă deschisă, având în vedere că, după lansarea modelului cu sursă deschisă, măsurile necesare pentru a asigura respectarea obligațiilor prevăzute în prezentul regulament pot fi mai dificil de pus în aplicare.

(113) În cazul în care Comisia constată că un model de IA de uz general îndeplinește cerințele de clasificare ca model de IA de uz general cu risc sistemic, lucru care anterior fie nu fusese cunoscut, fie nu fusese notificat Comisiei de furnizorul relevant, Comisia ar trebui să fie împuternicită să îl desemneze ca atare. Un sistem de alerte calificate ar trebui să asigure faptul că Oficiul pentru IA este informat de către grupul științific cu privire la modele de IA de uz general care ar putea fi clasificate drept modele de IA de uz general cu risc sistemic, pe lângă activitățile de monitorizare ale Oficiului pentru IA.

(114) Furnizorii de modele de IA de uz general care prezintă riscuri sistemice ar trebui să facă obiectul, pe lângă obligațiile prevăzute pentru furnizorii de modele de IA de uz general, unor obligații menite să identifice și să atenueze riscurile respective și să asigure un nivel adecvat de protecție în materie de securitate cibernetică, indiferent dacă este furnizat ca model de sine stătător sau încorporat într-un sistem sau într-un produs de IA. Pentru a atinge obiectivele respective, prezentul regulament ar trebui să impună furnizorilor să efectueze evaluările necesare ale modelelor, în special înainte de prima lor introducere pe piață, inclusiv efectuarea și documentarea testării contradictorii a modelelor, inclusiv, după caz, prin testări interne sau externe independente. În plus, furnizorii de modele de IA de uz general cu riscuri sistemice ar trebui să evalueze și să atenueze în permanență riscurile sistemice, inclusiv, de exemplu, prin instituirea unor politici de gestionare a riscurilor, cum ar fi procesele de asigurare a răspunderii și de guvernanță, prin punerea în aplicare a monitorizării ulterioare introducerii pe piață, prin luarea de măsuri adecvate de-a lungul întregului ciclu de viață al modelului și prin cooperarea cu actorii relevanți de-a lungul lanțului valoric al IA.

(115) Furnizorii de modele de IA de uz general cu riscuri sistemice ar trebui să evalueze și să atenueze posibilele riscuri sistemice. Dacă, în pofida eforturilor de identificare și prevenire a riscurilor legate de un model de IA de uz general care poate prezenta riscuri sistemice, dezvoltarea sau utilizarea modelului cauzează un incident grav, furnizorul modelului de IA de uz general ar trebui să urmărească fără întârzieri nejustificate incidentul și să raporteze Comisiei și autorităților naționale competente orice informații relevante și posibile măsuri corective. În plus, furnizorii ar trebui să asigure un nivel adecvat de protecție în materie de securitate cibernetică pentru model și infrastructura fizică a acestuia, dacă este cazul, de-a lungul întregului ciclu de viață al modelului. Protecția în materie de securitate cibernetică legată de riscurile sistemice asociate utilizării răuvoitoare sau atacurilor ar trebui să ia în considerare în mod corespunzător scurgerile accidentale de modele, lansările neautorizate, eludarea măsurilor de siguranță și apărarea împotriva atacurilor cibernetice, a accesului neautorizat sau a furtului de modele. Această protecție ar putea fi facilitată prin securizarea ponderilor modelelor, a algoritmilor, a serverelor și a seturilor de date, de exemplu prin măsuri de securitate operațională pentru securitatea informațiilor, politici specifice în materie de securitate cibernetică, soluții tehnice și consacrate adecvate și controale ale accesului cibernetic și fizic, adecvate circumstanțelor relevante și riscurilor implicate.

(116) Oficiul pentru IA ar trebui să încurajeze și să faciliteze elaborarea, revizuirea și adaptarea unor coduri de bune practici, ținând seama de abordările internaționale. Toți furnizorii de modele de IA de uz general ar putea fi invitați să participe. Pentru a se asigura că codurile de bune practici reflectă stadiul actual al tehnologiei și țin seama în mod corespunzător de un set divers de perspective, Oficiul pentru IA ar trebui să colaboreze cu autoritățile naționale competente relevante și ar putea, după caz, să se consulte cu organizațiile societății civile și cu alte părți interesate și experți relevanți, inclusiv cu grupul științific, pentru elaborarea unor astfel de coduri. Codurile de bune practici ar trebui să se refere la obligațiile furnizorilor de modele de IA de uz general și de modele de IA de uz general care prezintă riscuri sistemice. În plus, în ceea ce privește riscurile sistemice, codurile de bune practici ar trebui să contribuie la stabilirea unei taxonomii a tipurilor și naturii riscurilor sistemice la nivelul Uniunii, inclusiv a surselor acestora. Codurile de bune practici ar trebui să se axeze, de asemenea, pe măsuri specifice de evaluare și de atenuare a riscurilor.

(117) Codurile de bune practici ar trebui să reprezinte un instrument central pentru respectarea corespunzătoare a obligațiilor prevăzute în prezentul regulament pentru furnizorii de modele de IA de uz general. Furnizorii ar trebui să se poată baza pe coduri de bune practici pentru a demonstra respectarea obligațiilor. Prin intermediul unor acte de punere în aplicare, Comisia poate decide să aprobe un cod de bune practici și să îi acorde o valabilitate generală în Uniune sau, alternativ, să prevadă norme comune pentru punerea în aplicare a obligațiilor relevante, în cazul în care, până la momentul în care prezentul regulament devine aplicabil, un cod de bune practici nu poate fi finalizat sau nu este considerat adecvat de către Oficiul pentru IA. Odată ce un standard armonizat este publicat și evaluat ca fiind adecvat pentru a acoperi obligațiile relevante de către Oficiul pentru IA, furnizorii ar trebui să beneficieze de prezumția de conformitate în cazul în care respectă un standard european armonizat. În plus, furnizorii de modele de IA de uz general ar trebui să poată demonstra conformitatea utilizând mijloace alternative adecvate, dacă nu sunt disponibile coduri de bune practici sau standarde armonizate sau dacă aleg să nu se bazeze pe acestea.

(118) Prezentul regulament reglementează sistemele de IA și modelele de IA prin impunerea anumitor cerințe și obligații pentru actorii relevanți de pe piață care le introduc pe piață, le pun în funcțiune sau le utilizează în Uniune, completând astfel obligațiile pentru furnizorii de servicii intermediare care încorporează astfel de sisteme sau modele în serviciile lor reglementate de Regulamentul (UE) 2022/2065. În măsura în care astfel de sisteme sau modele sunt încorporate în platforme online foarte mari sau în motoare de căutare online foarte mari desemnate, acestea fac obiectul cadrului de gestionare a riscurilor prevăzut în Regulamentul (UE) 2022/2065. În consecință, ar trebui să se presupună că obligațiile corespunzătoare din prezentul regulament sunt îndeplinite, cu excepția cazului în care apar riscuri sistemice semnificative care nu intră sub incidența Regulamentului (UE) 2022/2065 și sunt identificate în astfel de modele. În acest cadru, furnizorii de platforme online foarte mari și de motoare de căutare online foarte mari sunt obligați să evalueze potențialele riscuri sistemice care decurg din proiectarea, funcționarea și utilizarea serviciilor lor, inclusiv modul în care proiectarea sistemelor algoritmice utilizate în cadrul serviciului poate contribui la astfel de riscuri, precum și riscurile sistemice care decurg din potențialele utilizări necorespunzătoare. Acești furnizori sunt, de asemenea, obligați să ia măsuri adecvate de atenuare, cu respectarea drepturilor fundamentale.

(119) Având în vedere ritmul rapid al inovării și al evoluției tehnologice a serviciilor digitale care intră în domeniul de aplicare al diferitelor instrumente din dreptul Uniunii, în special având în vedere utilizarea și percepția destinatarilor lor, sistemele de IA care fac obiectul prezentului regulament pot fi furnizate ca servicii intermediare sau ca părți ale acestora în sensul Regulamentului (UE) 2022/2065, care ar trebui să fie interpretat într-un mod neutru din punct de vedere tehnologic. De exemplu, sistemele de IA pot fi utilizate pentru a furniza motoare de căutare online, în special în măsura în care un sistem de IA, cum ar fi un chatbot online, efectuează căutări, în principiu, pe toate site-urile web, apoi încorporează rezultatele în cunoștințele sale existente și utilizează cunoștințele actualizate pentru a genera un singur rezultat care combină diferite surse de informații.

(120) În plus, obligațiile impuse prin prezentul regulament furnizorilor și implementatorilor anumitor sisteme de IA pentru a permite detectarea și divulgarea faptului că rezultatele sistemelor respective sunt generate sau manipulate artificial sunt deosebit de relevante pentru a facilita punerea în aplicare efectivă a Regulamentului (UE) 2022/2065. Acest lucru este valabil în special în ceea ce privește obligațiile furnizorilor de platforme online foarte mari sau de motoare de căutare online foarte mari de a identifica și a atenua riscurile sistemice care pot apărea în urma diseminării conținutului care a fost generat sau manipulat artificial, în special riscul privind efectele negative reale sau previzibile asupra proceselor democratice, asupra discursului civic și asupra proceselor electorale, inclusiv prin dezinformare.

(121) 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, pentru a promova inovarea, precum și competitivitatea și creșterea pe piața unică. Conformitatea cu standardele armonizate, astfel cum sunt definite la articolul 2 punctul 1 litera (c) din Regulamentul (UE) nr. 1025/2012 al Parlamentului European și al Consiliului[41], care ar trebui, în mod normal, să reflecte stadiul actual al tehnologiei, ar trebui să fie un mijloc prin care furnizorii să demonstreze conformitatea cu cerințele prezentului regulament. Prin urmare, ar trebui să fie încurajată o reprezentare echilibrată a intereselor, care să implice toate părțile interesate relevante în elaborarea standardelor, în special IMM-urile, organizațiile consumatorilor și părțile interesate din domeniul mediului și din domeniul social, în conformitate cu articolele 5 și 6 din Regulamentul (UE) nr. 1025/2012. Pentru a facilita conformitatea, solicitările de standardizare ar trebui să fie emise de Comisie fără întârzieri nejustificate. Atunci când elaborează solicitarea de standardizare, Comisia ar trebui să consulte forumul consultativ și comitetul pentru a colecta cunoștințele de specialitate relevante. 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 și după consultarea forumului consultativ, specificații comune pentru anumite cerințe în temeiul prezentului regulament.

---

[41] 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).

Specificația comună ar trebui să constituie o soluție excepțională de rezervă, pentru a facilita obligația furnizorului de a respecta cerințele prezentului regulament, atunci când solicitarea de standardizare nu a fost acceptată de niciuna dintre organizațiile de standardizare europene sau când standardele armonizate relevante abordează insuficient preocupările în materie de drepturi fundamentale ori când standardele armonizate nu corespund solicitării sau atunci când există întârzieri în adoptarea unui standard armonizat adecvat. În cazul în care o astfel de întârziere în adoptarea unui standard armonizat se datorează complexității tehnice a standardului respectiv, acest lucru ar trebui să fie luat în considerare de Comisie înainte de a avea în vedere stabilirea unor specificații comune. Atunci când elaborează specificații comune, Comisia este încurajată să coopereze cu partenerii internaționali și cu organismele de standardizare internaționale.

(122) Este oportun ca, fără a aduce atingere utilizării standardelor armonizate și a specificațiilor comune, să se prezume că furnizorii unui sistem de IA cu grad ridicat de risc care a fost antrenat și testat pe baza unor date care reflectă cadrul geografic, comportamental, contextual sau funcțional specific în care se intenționează utilizarea sistemului de IA respectă măsura relevantă prevăzută în temeiul cerinței privind guvernanța datelor stabilită în prezentul regulament. Fără a aduce atingere cerințelor legate de robustețe și acuratețe prevăzute în prezentul regulament, în conformitate cu articolul 54 alineatul (3) din Regulamentul (UE) 2019/881, ar trebui să se prezume că 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, iar referințele aferente au fost publicate în *Jurnalul Oficial al Uniunii Europene*, respectă cerința de securitate cibernetică menționată în prezentul regulament, în măsura în care certificatul de securitate cibernetică sau declarația de conformitate sau părți ale acestora acoperă cerința de securitate cibernetică din prezentul regulament. Acest lucru nu aduce atingere caracterului voluntar al respectivului sistem de securitate cibernetică.

(123) 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.

(124) Este oportun ca, pentru a reduce la minimum sarcina impusă 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 bazate pe noul cadru legislativ, conformitatea acestor sisteme de IA cu cerințele prezentului regulament să fie evaluată ca parte a evaluării conformității prevăzute deja în legislația respectivă. Aplicabilitatea cerințelor prezentului regulament nu ar trebui, prin urmare, să afecteze logica specifică, metodologia sau structura generală a evaluării conformității în temeiul legislației de armonizare relevante a Uniunii.

(125) Având în vedere complexitatea sistemelor de IA cu grad ridicat de risc și riscurile asociate acestora, este important să se dezvolte o procedură adecvată de evaluare a conformității pentru sistemele de IA cu grad ridicat de risc care implică organisme notificate, așa-numita evaluare a conformității de către terți. Cu toate acestea, având în vedere experiența actuală 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 biometrie.

(126) În vederea efectuării de evaluări ale conformității de către terți atunci când este necesar, autoritățile naționale competente ar trebui să comunice lista organismelor notificate în temeiul prezentului regulament, cu condiția ca acestea să îndeplinească un set de cerințe, în special în ceea ce privește independența, competența, absența conflictelor de interese și cerințele minime de securitate cibernetică. Lista acestor organisme notificate ar trebui să fie 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 anexa I la Decizia nr. 768/2008/CE.

(127) În conformitate cu angajamentele asumate de Uniune în temeiul Acordului Organizației Mondiale a Comerțului privind barierele tehnice în calea comerțului, este adecvat să se faciliteze recunoașterea reciprocă a rezultatelor evaluării conformității obținute de organismele competente de evaluare a conformității, indiferent de teritoriul pe care sunt stabilite acestea, cu condiția ca respectivele organisme de evaluare a conformității instituite în temeiul dreptului unei țări terțe să îndeplinească cerințele aplicabile ale prezentului regulament, iar Uniunea să fi încheiat un acord în acest sens. În acest context, Comisia ar trebui să analizeze în mod activ posibile instrumente internaționale adecvate acestui scop și, în special, să urmărească încheierea de acorduri de recunoaștere reciprocă cu țări terțe.

(128) 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 a fi 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.

(129) 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. Pentru sistemele de IA cu grad ridicat de risc încorporate într-un produs ar trebui să fie aplicat un marcaj CE fizic care poate fi completat de un marcaj CE digital. Pentru sistemele de IA cu grad ridicat de risc furnizate exclusiv digital, ar trebui să fie utilizat un marcaj CE digital. Statele membre ar trebui să nu genereze obstacole nejustificate în calea introducerii pe piață sau a punerii în funcțiune a sistemelor de IA cu grad ridicat de risc care sunt conforme cu cerințele prevăzute în prezentul regulament și care poartă marcajul CE.

(130) În anumite condiții, disponibilitatea rapidă a tehnologiilor inovatoare poate fi esențială pentru sănătatea și siguranța persoanelor, pentru protecția mediului și combaterea schimbărilor climatice 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, de protecție a mediului și de protecție a activelor industriale și de infrastructură esențiale, autoritățile de supraveghere a pieței să poată autoriza introducerea pe piață sau punerea în funcțiune a unor sisteme de IA care nu au fost supuse unei evaluări a conformității. În situații justificate în mod corespunzător, astfel cum se prevede în prezentul regulament, 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 autorizarea autorității de supraveghere a pieței, cu condiția ca o astfel de autorizare să fie solicitată în timpul utilizării sau după utilizare, fără întârzieri nejustificate.

(131) Pentru a facilita activitatea Comisiei și a statelor membre în domeniul IA, 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 actelor legislative de armonizare relevante existente ale Uniunii, precum și furnizorii care consideră că un sistem de IA care figurează între situațiile cu grad ridicat de risc dintr-o anexă la prezentul regulament nu este, pe baza unei derogări, un sistem de IA cu grad ridicat de risc, ar trebui să aibă obligația de a se înregistra, precum și de a înregistra informații despre propriul sistem de IA într-o bază de date a UE, care urmează să fie creată și gestionată de Comisie. Înainte de a utiliza un sistem de IA care figurează între situațiile cu grad ridicat de risc dintr-o anexă la prezentul regulament, implementatorii sistemelor de IA cu grad ridicat de risc care sunt autorități, agenții sau organisme publice ar trebui să se înregistreze în baza de date respectivă și să selecteze sistemul pe care intenționează să îl utilizeze.

Ceilalți implementatori ar trebui să aibă dreptul de a face acest lucru în mod voluntar. Această secțiune a bazei de date a UE ar trebui să fie accesibilă publicului, în mod gratuit, informațiile ar trebui să fie ușor de parcurs, ușor de înțeles și prelucrabile automat. Baza de date a UE ar trebui, de asemenea, să fie ușor de utilizat, de exemplu prin furnizarea de funcționalități de căutare, inclusiv prin intermediul cuvintelor-cheie, care să permită publicului larg să găsească informațiile relevante care trebuie să fie transmise la înregistrarea sistemelor de IA cu grad ridicat de risc și cu privire la cazul de utilizare a sistemelor de IA cu grad ridicat de risc, prevăzute într-o anexă la prezentul regulament, cărora le corespund sistemele de IA cu grad ridicat de risc. Orice modificare substanțială a sistemelor de IA cu grad ridicat de risc ar trebui să se înregistreze, de asemenea, în baza de date a UE. Pentru sistemele de IA cu grad ridicat de risc din domeniul aplicării legii, al migrației, al azilului și al gestionării controlului la frontiere, obligațiile de înregistrare ar trebui să fie îndeplinite în cadrul unei secțiuni securizate, care nu este accesibilă publicului, a bazei de date a UE. Accesul la secțiunea securizată care nu este accesibilă publicului ar trebui să fie strict limitat la Comisie, precum și la autoritățile de supraveghere a pieței în ceea ce privește secțiunea lor națională din baza de date respectivă. Sistemele de IA cu grad ridicat de risc din domeniul infrastructurii critice ar trebui să fie înregistrate exclusiv la nivel național. Comisia ar trebui să fie operatorul bazei de date a UE, în conformitate cu Regulamentul (UE) 2018/1725. Pentru a asigura funcționalitatea deplină a bazei de date a UE, atunci când aceasta este implementată, procedura de stabilire a bazei de date ar trebui să includă dezvoltarea de specificații funcționale de către Comisie și un raport de audit independent. Comisia ar trebui să țină seama de riscurile în materie de securitate cibernetică atunci când își îndeplinește sarcinile de operator de date în baza de date a UE. Pentru a maximiza disponibilitatea și utilizarea bazei de date a UE de către public, baza de date a UE, inclusiv informațiile puse la dispoziție prin intermediul acesteia, ar trebui să îndeplinească cerințele prevăzute în Directiva (UE) 2019/882.

(132) 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 grad ridicat de risc 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 și sub rezerva unor excepții specifice pentru a ține seama de nevoia specială de a aplica legea. 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 rezonabil de bine informată, de atentă și de avizată, ținând seama de circumstanțele și contextul de utilizare. La punerea în aplicare a obligației respective, caracteristicile persoanelor fizice care aparțin grupurilor vulnerabile din motive de vârstă sau dizabilitate ar trebui să fie luate în considerare în măsura în care sistemul de IA este destinat să interacționeze și cu aceste grupuri. În plus, persoanele fizice ar trebui să fie informate atunci când sunt expuse la sisteme de IA care, prin prelucrarea datelor lor biometrice, 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. Astfel de informații și notificări ar trebui să fie furnizate în formate accesibile pentru persoanele cu dizabilități.

(133) O varietate de sisteme de IA poate genera cantități mari de conținut sintetic, pe care oamenii ajung să îl distingă din ce în ce mai greu de conținutul autentic, generat de om. Disponibilitatea pe scară largă și capabilitățile din ce în ce mai mari ale acestor sisteme au un impact semnificativ asupra integrității ecosistemului informațional și a încrederii în acesta, generând noi riscuri de dezinformare și manipulare la scară largă, de fraudă, de uzurpare a identității și de inducere în eroare a consumatorilor. Având în vedere impactul respectiv, ritmul tehnologic rapid și necesitatea unor noi metode și tehnici de urmărire a originii informațiilor, este oportun să se solicite furnizorilor acestor sisteme să încorporeze soluții tehnice care să permită marcarea într-un format prelucrabil automat și detectarea faptului că rezultatul a fost generat sau manipulat de un sistem de IA, și nu de un om. Aceste tehnici și metode ar trebui să fie suficient de fiabile, interoperabile, eficace și robuste, în măsura în care acest lucru este fezabil din punct de vedere tehnic, ținând seama de tehnicile disponibile sau de o combinație de astfel de tehnici, cum ar fi filigrane, identificări prin intermediul metadatelor, metode criptografice pentru a dovedi proveniența și autenticitatea conținutului, metode de înregistrare, amprente digitale sau alte tehnici, după caz. Atunci când pun în aplicare această obligație, furnizorii ar trebui, de asemenea, să țină seama de particularitățile și limitările diferitelor tipuri de conținut și de evoluțiile tehnologice și ale pieței relevante în domeniu, astfel cum se reflectă în stadiul de avansare general recunoscut al tehnologiei. Astfel de tehnici și metode pot fi puse în aplicare la nivelul sistemului de IA sau la nivelul modelului de IA, inclusiv al modelelor de IA de uz general care generează conținut, facilitând astfel îndeplinirea acestei obligații de către furnizorul din aval al sistemului de IA. Este oportun să se aibă în vedere că, pentru a rămâne proporțională, această obligație de marcare nu ar trebui să vizeze sistemele de IA care îndeplinesc în principal o funcție de asistare pentru editarea standard sau sistemele de IA care nu modifică în mod substanțial datele de intrare furnizate de implementator sau semantica acestora.

(134) Pe lângă soluțiile tehnice utilizate de furnizorii sistemului de IA, implementatorii 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, obiecte, locuri, entități sau evenimente existente și care ar crea unei persoane impresia falsă că sunt autentice sau adevărate (deepfake-uri), ar trebui, de asemenea, să dezvăluie în mod clar și distinct faptul că respectivul conținut a fost creat sau manipulat în mod artificial prin etichetarea în consecință a rezultatului generat de IA și divulgarea originii sale artificiale. Respectarea acestei obligații de transparență nu ar trebui să fie interpretată în sensul de a indica că utilizarea sistemului de IA sau a rezultatelor sale împiedică dreptul la libertatea de exprimare și dreptul la libertatea artelor și științelor garantate de cartă, în special atunci când conținutul face parte dintr-o lucrare sau dintr-un program în mod evident creativ, satiric, artistic, fictiv sau analog, sub rezerva unor garanții adecvate pentru drepturile și libertățile terților. În cazurile respective, obligația de transparență pentru deepfake-uri prevăzută în prezentul regulament se limitează la divulgarea existenței unui astfel de conținut generat sau manipulat într-un mod adecvat, care să nu împiedice expunerea lucrării sau posibilitatea de a beneficia de aceasta, inclusiv exploatarea și utilizarea normală a acesteia, menținând în același timp utilitatea și calitatea lucrării. În plus, este, de asemenea, oportun să se aibă în vedere o obligație similară de divulgare în ceea ce privește textul generat sau manipulat de IA, în măsura în care acesta este publicat cu scopul de a informa publicul cu privire la chestiuni de interes public, cu excepția cazului în care conținutul generat de IA a fost supus unui proces de verificare editorială sau revizuire umană și responsabilitatea editorială pentru publicarea conținutului este deținută de o persoană fizică sau juridică.

(135) Fără a aduce atingere caracterului obligatoriu și aplicabilității depline a obligațiilor privind transparența, Comisia poate, de asemenea, să încurajeze și să faciliteze elaborarea de coduri de bune practici la nivelul Uniunii cu scopul de a facilita punerea în aplicare efectivă a obligațiilor privind detectarea și etichetarea conținutului generat sau manipulat artificial, inclusiv de a sprijini modalitățile practice pentru a oferi accesul, după caz, la mecanisme de detectare și pentru a facilita cooperarea cu alți actori de-a lungul lanțului valoric, pentru a disemina conținutul sau a verifica autenticitatea și proveniența acestuia, astfel încât publicul să poată distinge efectiv conținutul generat de IA.

(136) Obligațiile impuse prin prezentul regulament furnizorilor și implementatorilor anumitor sisteme de IA pentru a permite detectarea și divulgarea faptului că rezultatele sistemelor respective sunt generate sau manipulate artificial sunt deosebit de relevante pentru a facilita punerea în aplicare efectivă a Regulamentului (UE) 2022/2065. Acest lucru este valabil în special în ceea ce privește obligațiile furnizorilor de platforme online foarte mari sau de motoare de căutare online foarte mari de a identifica și a atenua riscurile sistemice care pot apărea în urma diseminării conținutului care a fost generat sau manipulat artificial, în special riscul privind efectele negative reale sau previzibile asupra proceselor democratice, asupra discursului civic și asupra proceselor electorale, inclusiv prin dezinformare. Cerința de etichetare a conținutului generat de sistemele de IA în temeiul prezentului regulament nu aduce atingere obligației prevăzute la articolul 16 alineatul (6) din Regulamentul (UE) 2022/2065 pentru furnizorii de servicii de găzduire de a prelucra notificările privind conținutul ilegal primite în temeiul articolului 16 alineatul (1) din regulamentul respectiv și nu ar trebui să influențeze evaluarea și decizia privind ilegalitatea conținutului specific. Evaluarea respectivă ar trebui să fie efectuată exclusiv în raport cu normele care reglementează legalitatea conținutului.

(137) Respectarea obligațiilor privind transparența pentru sistemele de IA vizate de prezentul regulament nu ar trebui să fie interpretată ca indicând faptul că utilizarea sistemului de IA sau a rezultatelor sale este legală în temeiul prezentului regulament sau al altor dispoziții din dreptul Uniunii și al statelor membre și nu ar trebui să aducă atingere altor obligații de transparență pentru implementatorii sistemelor de IA prevăzute în dreptul Uniunii sau în cel intern.

(138) IA este o familie de tehnologii care se dezvoltă rapid și care necesită supraveghere reglementară și un spațiu sigur și controlat 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 care promovează inovarea, adaptat exigențelor viitorului și rezistent la inovări disruptive, statele membre ar trebui să se asigure că autoritățile lor naționale competente instituie cel puțin un spațiu de testare la nivel național în materie de reglementare în domeniul IA pentru a facilita dezvoltarea și testarea sistemelor de IA inovatoare aflate sub supraveghere reglementară strictă înainte ca aceste sisteme să fie introduse pe piață sau puse în funcțiune în alt mod. Statele membre ar putea, de asemenea, să îndeplinească această obligație prin participarea la spațiile de testare în materie de reglementare deja existente sau prin instituirea unui spațiu de testare în comun cu una sau mai multe autorități competente ale statelor membre, în măsura în care această participare asigură un nivel echivalent de acoperire națională pentru statele membre participante. Spațiile de testare în materie de reglementare în domeniul IA ar putea fi instituite în formă fizică, digitală sau hibridă și pot găzdui atât produse fizice, cât și produse digitale. Autoritățile de instituire ar trebui, de asemenea, să se asigure că spațiile de testare în materie de reglementare în domeniul IA dispun de resursele adecvate pentru funcționarea lor, inclusiv de resurse financiare și umane.

(139) Obiectivele spațiilor de testare în materie de reglementare în domeniul IA ar trebui să fie promovarea inovării în domeniul IA prin instituirea unui mediu de experimentare și testare controlat în faza de dezvoltare și în faza anterioară introducerii pe piață, cu scopul de a asigura conformitatea sistemelor de IA inovatoare cu prezentul regulament și cu alte dispoziții relevante din dreptul Uniunii și dreptul intern. În plus, spațiile de testare în materie de reglementare în domeniul IA ar trebui să urmărească sporirea securității juridice pentru inovatori și supravegherea și înțelegerea de către autoritățile competente a oportunităților, a riscurilor emergente și a impactului utilizării IA, facilitarea învățării în materie de reglementare pentru autorități și întreprinderi, inclusiv în vederea viitoarelor adaptări ale cadrului juridic, sprijinirea cooperării și a schimbului de bune practici cu autoritățile implicate în spațiul de testare în materie de reglementare în domeniul IA, precum și accelerarea accesului la piețe, inclusiv prin eliminarea barierelor din calea IMM-urilor, inclusiv a întreprinderilor nou-înființate. Spațiile de testare în materie de reglementare în domeniul IA ar trebui să fie disponibile pe scară largă în întreaga Uniune și ar trebui să se acorde o atenție deosebită accesibilității acestora pentru IMM-uri, inclusiv pentru întreprinderile nou-înființate. Participarea la spațiul de testare în materie de reglementare în domeniul IA ar trebui să se concentreze pe aspecte care fac ca furnizorii și potențialii furnizori să se confrunte cu o lipsă de securitate juridică atunci când încearcă să inoveze, să experimenteze cu IA în Uniune și să contribuie la învățarea bazată pe dovezi în materie de reglementare. Supravegherea sistemelor de IA în spațiul de testare în materie de reglementare în domeniul IA ar trebui, prin urmare, să vizeze dezvoltarea, antrenarea, testarea și validarea acestora înainte ca sistemele să fie introduse pe piață sau puse în funcțiune, precum și noțiunea de modificare substanțială care ar putea necesita o nouă procedură de evaluare a conformității și ocurența unei astfel de modificări. Orice riscuri semnificative identificate în cursul dezvoltării și testării unor astfel de sisteme de IA ar trebui să conducă la o atenuare adecvată și, în cazul în care atenuarea nu este posibilă, la suspendarea procesului de dezvoltare și testare.

După caz, autoritățile naționale competente care instituie spații de testare în materie de reglementare în domeniul 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 de IA, cum ar fi organizațiile de standardizare naționale sau europene, organismele notificate, unitățile de testare și experimentare, laboratoarele de cercetare și experimentare, centrele europene de inovare digitală 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 în domeniul IA și un cadru de cooperare între autoritățile relevante implicate în supravegherea spațiilor de testare. Spațiile de testare în materie de reglementare în domeniul IA instituite în temeiul prezentului regulament nu ar trebui să aducă atingere altor dispoziții de drept care permit instituirea altor spații de testare cu scopul de a asigura conformitatea cu alte dispoziții de drept 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 în domeniul IA, testarea în condiții reale poate fi, de asemenea, efectuată și supravegheată în cadrul spațiului de testare în materie de reglementare în domeniul IA.

(140) Prezentul regulament ar trebui să ofere furnizorilor și potențialilor furnizori din cadrul spațiului de testare în materie de reglementare în domeniul IA temeiul juridic pentru utilizarea datelor cu caracter personal colectate în alte scopuri pentru a dezvolta anumite sisteme de IA de interes public în cadrul spațiului de testare în materie de reglementare în domeniul IA numai în condiții specificate, 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, 6 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 drepturi ale persoanelor vizate în temeiul Regulamentelor (UE) 2016/679 și (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. Furnizorii și potențialii furnizori din cadrul spațiului de testare în materie de reglementare în domeniul IA ar trebui să asigure garanții adecvate și să coopereze cu autoritățile competente, inclusiv urmând orientările acestora și acționând cu promptitudine și cu bună-credință, în ceea ce privește atenuarea în mod adecvat a oricăror riscuri semnificative identificate la adresa siguranței, sănătății și a drepturilor fundamentale care ar putea apărea în timpul dezvoltării, testării și experimentării în spațiul de testare respectiv.

(141) Pentru a accelera procesul de dezvoltare și introducere pe piață a sistemelor de IA cu grad ridicat de risc enumerate într-o anexă la prezentul regulament, 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 în domeniul IA. Cu toate acestea, în astfel de cazuri, ținând seama de posibilele consecințe ale unor astfel de teste asupra persoanelor fizice, ar trebui să se garanteze faptul că prezentul regulament 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 cazurilor legate de aplicarea legii dacă 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 dreptului relevant privind protecția datelor și nu îi aduce atingere acestuia.

De asemenea, este important să se reducă la minimum riscurile și să se permită supravegherea de către autoritățile competente și, prin urmare, să se impună potențialilor furnizori să facă demersurile necesare pentru prezentarea unui plan de testare în condiții reale autorității competente de supraveghere a pieței, să se înregistreze testările în secțiuni specifice din baza de date a UE, sub rezerva unor excepții limitate, să se instituie limite privind perioada pentru care se poate efectua testarea și să se impună garanții suplimentare pentru persoanele care aparțin anumitor grupuri vulnerabile, precum și un acord scris care să definească rolurile și responsabilitățile potențialilor furnizori și implementatori și supravegherea eficace de către personalul competent implicat în testarea în condiții reale. În plus, este oportun să se prevadă garanții suplimentare pentru a se asigura că previziunile, recomandările sau deciziile sistemului de IA pot fi efectiv inversate și ignorate și că datele cu caracter personal sunt protejate și sunt șterse atunci când subiecții își retrag consimțământul de a participa la testare, fără a aduce atingere drepturilor lor în calitate de persoane vizate în temeiul dreptului Uniunii privind protecția datelor. În ceea ce privește transferul de date, este, de asemenea, oportun să se prevadă că datele colectate și prelucrate în scopul testării în condiții reale ar trebui să fie transferate către țări terțe numai cu condiția punerii în aplicare a unor garanții adecvate și aplicabile în temeiul dreptului Uniunii, în special în conformitate cu bazele pentru transferul de date cu caracter personal în temeiul dreptului Uniunii privind protecția datelor, în timp ce pentru datele fără caracter personal sunt instituite garanții adecvate în conformitate cu dreptul Uniunii, cum ar fi Regulamentele (UE) 2022/868[42] și (UE) 2023/2854[43] ale Parlamentului European și ale Consiliului.

---

[42] Regulamentul (UE) 2022/868 al Parlamentului European și al Consiliului din 30 mai 2022 privind guvernanța datelor la nivel european și de modificare a Regulamentului (UE) 2018/1724 (Regulamentul privind guvernanța datelor) (JO L 152, 3.6.2022, p. 1).

[43] Regulamentul (UE) 2023/2854 al Parlamentului European și al Consiliului din 13 decembrie 2023 privind norme armonizate pentru un acces echitabil la date și o utilizare corectă a acestora și de modificare a Regulamentului (UE) 2017/2394 și a Directivei (UE) 2020/1828 (Regulamentul privind datele) (JO L, 2023/2854, 22.12.2023, ELI: http://data.europa.eu/eli/reg/2023/2854/oj).

(142) Pentru a se asigura că IA conduce la rezultate benefice din punct de vedere social și ecologic, statele membre sunt încurajate să sprijine și să promoveze cercetarea și dezvoltarea de soluții de IA în sprijinul rezultatelor benefice din punct de vedere social și ecologic, cum ar fi soluțiile bazate pe IA pentru a spori accesibilitatea pentru persoanele cu dizabilități, pentru a combate inegalitățile socioeconomice sau pentru a îndeplini obiectivele de mediu, alocând resurse suficiente, inclusiv finanțare publică și din partea Uniunii, și, după caz și cu condiția îndeplinirii criteriilor de eligibilitate și de selecție, luând în considerare în special proiectele care urmăresc astfel de obiective. Aceste proiecte ar trebui să se bazeze pe principiul cooperării interdisciplinare dintre dezvoltatorii de IA, experții în materie de inegalitate și nediscriminare, accesibilitate, drepturile consumatorilor, de mediu și digitale, precum și cadrele universitare.

(143) Pentru a promova și proteja inovarea, este important să fie luate în considerare în mod deosebit interesele IMM-urilor, inclusiv ale întreprinderilor nou-înființate care sunt furnizori și implementatori de sisteme de IA. În acest scop, statele membre ar trebui să elaboreze inițiative care să vizeze operatorii respectivi, inclusiv în ceea ce privește sensibilizarea și comunicarea informațiilor. Statele membre ar trebui să ofere IMM-urilor, inclusiv întreprinderilor nou-înființate, care au un sediu social sau o sucursală în Uniune, acces prioritar la spațiile de testare în materie de reglementare în domeniul IA, cu condiția ca acestea să îndeplinească condițiile de eligibilitate și criteriile de selecție și fără a împiedica alți furnizori și potențiali furnizori să acceseze spațiile de testare, cu condiția să fie îndeplinite aceleași condiții și criterii. Statele membre ar trebui să utilizeze canalele existente și, după caz, să stabilească noi canale specifice de comunicare cu IMM-urile, inclusiv întreprinderile nou-înființate, implementatorii și alți inovatori și, după caz, cu autoritățile publice locale, pentru a sprijini IMM-urile pe tot parcursul dezvoltării lor, oferind orientări și răspunzând la întrebări cu privire la punerea în aplicare a prezentului regulament. După caz, aceste canale ar trebui să colaboreze pentru a crea sinergii și pentru a asigura omogenitatea orientărilor pe care le furnizează IMM-urilor, inclusiv întreprinderilor nou-înființate, și implementatorilor. În plus, statele membre ar trebui să faciliteze participarea IMM-urilor și a altor părți interesate relevante la procesele de elaborare a standardelor. De asemenea, ar trebui să fie luate în considerare interesele și nevoile specifice ale furnizorilor care sunt IMM-uri, inclusiv întreprinderi nou-înființate, atunci când organismele notificate stabilesc taxe de evaluare a conformității. Comisia ar trebui să evalueze periodic costurile de certificare și de conformitate suportate de IMM-uri, inclusiv de întreprinderile nou-înființate, prin consultări transparente și ar trebui să colaboreze cu statele membre pentru a reduce aceste costuri.

De exemplu, 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 relevantă din partea furnizorilor și pentru comunicarea cu operatorii este o limbă înțeleasă pe larg de un număr cât mai mare de implementatori transfrontalieri. Pentru a răspunde nevoilor specifice ale IMM-urilor, inclusiv ale întreprinderilor nou-înființate, Comisia ar trebui să furnizeze modele standardizate pentru domeniile vizate de prezentul regulament, la solicitarea comitetului. În plus, Comisia ar trebui să completeze eforturile statelor membre prin furnizarea unei platforme unice de informare cu informații ușor de utilizat în ceea ce privește prezentul regulament destinate tuturor furnizorilor și implementatorilor, prin organizarea unor campanii de comunicare adecvate pentru sensibilizarea cu privire la obligațiile care decurg din prezentul regulament și prin evaluarea și promovarea convergenței bunelor practici în cadrul procedurilor de achiziții publice în ceea ce privește sistemele de IA. Întreprinderile mijlocii care până recent se încadrau în categoria de întreprinderi mici în sensul anexei la Recomandarea 2003/361/CE a Comisiei[44] ar trebui să aibă acces la măsurile de sprijin respective, deoarece este posibil ca aceste noi întreprinderi mijlocii să nu dispună uneori de resursele juridice și formarea necesare pentru a asigura respectarea și înțelegerea adecvată a prezentului regulament.

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

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

(145) Pentru a reduce la minimum riscurile la adresa punerii în aplicare care decurg din lipsa de cunoaștere și de cunoștințe de specialitate de pe piață, precum și pentru a facilita respectarea de către furnizori, cu precădere de către IMM-uri, inclusiv întreprinderile nou-înființate, 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 nivelul Uniunii sau la nivel național ar trebui să contribuie la punerea în aplicare a prezentului regulament. În cadrul misiunii și domeniilor lor de competență respective, platforma de IA la cerere, centrele europene de inovare digitală și instalațiile de testare și experimentare sunt în măsură să ofere, în special, sprijin tehnic și științific furnizorilor și organismelor notificate.

(146) În plus, având în vedere dimensiunea foarte mică a unor operatori și pentru a asigura proporționalitatea în ceea ce privește costurile inovării, este oportun să se permită microîntreprinderilor să îndeplinească într-o manieră simplificată una dintre obligațiile cele mai costisitoare, și anume aceea de a institui un sistem de management al calității, fapt 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. Comisia ar trebui să elaboreze orientări pentru a specifica elementele sistemului de management al calității care trebuie îndeplinite în această manieră simplificată de către microîntreprinderi.

(147) 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 oricăror acte legislative de armonizare relevante ale Uniunii și care îndeplinesc sarcini în contextul evaluării conformității produselor sau dispozitivelor reglementate de respectivele acte legislative de armonizare ale Uniunii. Acest lucru este valabil în special în ceea ce privește grupurile de experți, laboratoarele de expertiză și laboratoarele de referință în domeniul dispozitivelor medicale în temeiul Regulamentelor (UE) 2017/745 și (UE) 2017/746.

(148) Prezentul regulament ar trebui să instituie un cadru de guvernanță care să permită, pe de o parte, coordonarea și sprijinirea aplicării prezentului regulament la nivel național și, pe de altă parte, consolidarea capabilităților la nivelul Uniunii și integrarea părților interesate în domeniul IA. Punerea în aplicare și respectarea efectivă a prezentului regulament necesită un cadru de guvernanță care să permită coordonarea și consolidarea cunoștințelor de specialitate centrale la nivelul Uniunii. Oficiul pentru IA a fost instituit printr-o decizie a Comisiei[45] și are ca misiune să dezvolte cunoștințele de specialitate și capabilitățile Uniunii în domeniul IA și să contribuie la punerea în aplicare a dreptului Uniunii privind IA. Statele membre ar trebui să faciliteze sarcinile Oficiului pentru IA cu scopul de a sprijini dezvoltarea, la nivelul Uniunii, a cunoștințelor de specialitate și a capabilităților Uniunii și de a consolida funcționarea pieței unice digitale. În plus, ar trebui să fie instituit un comitet compus din reprezentanți ai statelor membre, un grup științific care să integreze comunitatea științifică și un forum consultativ pentru a furniza contribuții ale părților interesate pentru punerea în aplicare a prezentului regulament, la nivelul Uniunii și la nivel național. Dezvoltarea cunoștințelor de specialitate și a capabilităților Uniunii ar trebui să includă și valorificarea resurselor și cunoștințelor de specialitate existente, în special prin sinergii cu structurile create în contextul aplicării la nivelul Uniunii a altor acte legislative și al sinergiilor cu inițiativele conexe de la nivelul Uniunii, cum ar fi Întreprinderea comună EuroHPC și unitățile de testare și experimentare în domeniul IA din cadrul programului „Europa digitală”.

---

[45] Decizia Comisiei din 24.1.2024 de instituire a Oficiului european pentru inteligența artificială, C(2024) 390.

(149) Pentru a facilita o punere în aplicare armonioasă, efectivă și armonizată a prezentului regulament, ar trebui să fie instituit un comitet. Comitetul ar trebui să reflecte diferitele interese ale ecosistemului de IA și să fie alcătuit din reprezentanți ai statelor membre. Comitetul ar trebui să fie responsabil pentru o serie de sarcini consultative, inclusiv emiterea de avize, recomandări, consiliere sau furnizarea unor contribuții sub formă de orientări cu privire la aspecte legate de punerea în aplicare a prezentului regulament, inclusiv cu privire la aspecte de aplicare a legii, la specificații tehnice sau la standarde existente în ceea ce privește cerințele stabilite în prezentul regulament, precum și furnizarea de consiliere Comisiei și statelor lor membre și autorităților naționale competente ale acestora cu privire la chestiuni specifice legate de IA. Pentru a oferi o anumită flexibilitate statelor membre în ceea ce privește desemnarea reprezentanților lor în cadrul comitetului, 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 articolul 33 din regulamentul respectiv, 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 Uniunii care își desfășoară activitatea în contextul reglementărilor relevante ale dreptului Uniunii, inclusiv, în special, cu cele care își desfășoară activitatea în temeiul reglementărilor relevante ale dreptului Uniunii privind datele, produsele și serviciile digitale.

(150) Pentru a asigura implicarea părților interesate în punerea în aplicare și aplicarea prezentului regulament, ar trebui să fie instituit un forum consultativ care să furnizeze comitetului și Comisiei consiliere și cunoștințe de specialitate tehnice. Pentru a asigura o reprezentare a părților interesate variată și echilibrată între interesele comerciale și cele necomerciale și, în cadrul categoriei intereselor comerciale, în ceea ce privește IMM-urile și alte întreprinderi, forumul consultativ ar trebui să cuprindă, printre altele, industria, întreprinderile nou-înființate, IMM-urile, mediul academic, societatea civilă, inclusiv partenerii sociali, precum și Agenția pentru Drepturi Fundamentale, ENISA, Comitetul European de Standardizare (CEN), Comitetul European de Standardizare în Electrotehnică (CENELEC) și Institutul European de Standardizare în Telecomunicații (ETSI).

(151) Pentru a sprijini punerea în aplicare și respectarea prezentului regulament, în special activitățile de monitorizare ale Oficiului pentru IA în ceea ce privește modelele de IA de uz general, ar trebui să fie instituit un grup științific de experți independenți. Experții independenți din alcătuirea grupului științific ar trebui să fie selectați pe baza cunoștințelor de specialitate științifice sau tehnice actualizate în domeniul IA și ar trebui să își îndeplinească sarcinile cu imparțialitate și obiectivitate și să asigure confidențialitatea informațiilor și a datelor obținute în îndeplinirea sarcinilor și activităților lor. Pentru a permite consolidarea capacităților naționale necesare pentru aplicarea efectivă a prezentului regulament, statele membre ar trebui să poată solicita sprijin echipei de experți care formează grupul științific pentru activitățile lor de aplicare a legii.

(152) Pentru a sprijini o aplicare adecvată a normelor în ceea ce privește sistemele de IA și pentru a consolida capacitățile statelor membre, ar trebui să fie instituite și puse la dispoziția statelor membre structuri ale Uniunii de sprijin pentru testarea IA.

(153) Statele membre joacă un rol esențial în aplicarea și respectarea prezentului regulament. În acest sens, fiecare stat membru ar trebui să desemneze cel puțin o autoritate de notificare și cel puțin o autoritate de supraveghere a pieței în calitatea de 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. Pentru a spori eficiența organizațională din partea statelor membre și pentru a stabili un punct unic de contact cu publicul și cu alți omologi la nivelul statelor membre și al Uniunii, fiecare stat membru ar trebui să desemneze o autoritate de supraveghere a pieței care să acționeze ca punct unic de contact.

(154) Autoritățile naționale competente ar trebui să își exercite competențele în mod independent, imparțial și fără prejudecăți, garantând principiile obiectivității activităților și sarcinilor lor și asigurând aplicarea și punerea în aplicare a prezentului regulament. Membrii acestor autorități ar trebui să se abțină de la orice act incompatibil cu natura funcțiilor lor și ar trebui să facă obiectul normelor de confidențialitate în temeiul prezentului regulament.

(155) 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. După caz, monitorizarea ulterioară introducerii pe piață ar trebui să includă o analiză a interacțiunii cu alte sisteme de IA, inclusiv cu alte dispozitive și alt software. Monitorizarea ulterioară introducerii pe piață nu ar trebui să vizeze datele operaționale sensibile ale implementatorilor care sunt autorități de aplicare a legii. 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 în timp util. 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, și anume un incident sau o funcționare defectuoasă care duce la deces sau la daune grave pentru sănătate, la perturbări grave și ireversibile ale gestionării și funcționării infrastructurii critice, la încălcări ale obligațiilor în temeiul dreptului Uniunii menite să protejeze drepturile fundamentale sau la daune grave aduse bunurilor materiale sau mediului.

(156) Pentru a se asigura respectarea adecvată și efectivă a cerințelor și a obligațiilor prevăzute în prezentul regulament, și anume în legislația de armonizare a Uniunii, ar trebui să se aplice sistemul de supraveghere a pieței și de conformitate a produselor în ansamblul său, astfel cum a fost instituit prin Regulamentul (UE) 2019/1020. Autoritățile de supraveghere a pieței desemnate în temeiul prezentului regulament ar trebui să dispună de toate competențele de aplicare a dispozițiilor stabilite în prezentul regulament și în Regulamentul (UE) 2019/1020 și ar trebui să își exercite competențele și să își îndeplinească atribuțiile în mod independent, imparțial și fără prejudecăți. 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 organelor Uniunii care intră în domeniul de aplicare al prezentului regulament, este oportun ca Autoritatea Europeană pentru Protecția Datelor să fie desemnată drept autoritate 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.

(157) Prezentul regulament nu aduce atingere competențelor, sarcinilor, prerogativelor și independenței autorităților sau organismelor publice naționale relevante 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 să fie stabilită o procedură de salvgardare specifică pentru a se asigura respectarea dispozițiilor în domeniul IA, în mod adecvat și în timp util, în privința 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 interdicției anumitor practici prevăzută 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.

(158) Dreptul 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, în mod coerent, aplicarea și respectarea obligațiilor prevăzute în prezentul regulament și a normelor și cerințelor relevante ale actelor juridice ale Uniunii în domeniul serviciilor financiare, autoritățile competente responsabile cu supravegherea și aplicarea actelor juridice respective, în special autoritățile competente, astfel cum sunt definite în Regulamentul (UE) nr. 575/2013 al Parlamentului European și al Consiliului[46] și în Directivele 2008/48/CE[47], 2009/138/CE[48], 2013/36/UE[49], 2014/17/UE[50] și (UE) 2016/97[51] ale Parlamentului European și ale Consiliului, ar trebui să fie desemnate, în limitele competențelor lor respective, 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.

---

[46] Regulamentul (UE) nr. 575/2013 al Parlamentului European și al Consiliului din 26 iunie 2013 privind cerințele prudențiale pentru instituțiile de credit și societățile de investiții și de modificare a Regulamentului (UE) nr. 648/2012 (JO L 176, 27.6.2013, p. 1).

[47] Directiva 2008/48/CE a Parlamentului European și a Consiliului din 23 aprilie 2008 privind contractele de credit pentru consumatori și de abrogare a Directivei 87/102/CEE a Consiliului (JO L 133, 22.5.2008, p. 66).

[48] Directiva 2009/138/CE a Parlamentului European și a Consiliului din 25 noiembrie 2009 privind accesul la activitate și desfășurarea activității de asigurare și de reasigurare (Solvabilitate II) (JO L 335, 17.12.2009, p. 1).

[49] 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).

[50] Directiva 2014/17/UE a Parlamentului European și a Consiliului din 4 februarie 2014 privind contractele de credit oferite consumatorilor pentru bunuri imobile rezidențiale și de modificare a Directivelor 2008/48/CE și 2013/36/UE și a Regulamentului (UE) nr. 1093/2010 (JO L 60, 28.2.2014, p. 34).

[51] Directiva (UE) 2016/97 a Parlamentului European și a Consiliului din 20 ianuarie 2016 privind distribuția de asigurări (JO L 26, 2.2.2016, p. 19).

Autoritățile competente respective ar trebui să dețină toate competențele 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 dispozițiilor relevante ale dreptului Uniunii din domeniul serviciilor 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 instituit prin Regulamentul (UE) nr. 1024/2013 al Consiliului[52], 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, 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 să fie avute în vedere derogări limitate și în ceea ce privește sistemul de management al calității al furnizorilor și obligația de monitorizare impusă implementatorilor de sisteme de IA cu grad ridicat de risc, în măsura în care acestea se aplică instituțiilor de credit reglementate de Directiva 2013/36/UE. Același regim ar trebui să se aplice întreprinderilor de asigurare și reasigurare și holdingurilor de asigurare în temeiul Directivei 2009/138/CE, intermediarilor de asigurări în temeiul Directivei (UE) 2016/97, precum și altor tipuri de instituții financiare care fac obiectul cerințelor privind guvernanța internă, măsurile sau procesele interne instituite în temeiul dispozițiilor relevante ale dreptului Uniunii din domeniul serviciilor financiare pentru a asigura coerența și egalitatea de tratament în sectorul financiar.

---

52 Regulamentul (UE) nr. 1024/2013 al Consiliului din 15 octombrie 2013 de conferire a unor atribuții specifice Băncii Centrale Europene în ceea ce privește politicile legate de supravegherea prudențială a instituțiilor de credit (JO L 287, 29.10.2013, p. 63).

(159) Fiecare autoritate de supraveghere a pieței pentru sistemele de IA cu grad ridicat de risc din domeniul biometriei, astfel cum sunt enumerate într-o anexă la prezentul regulament, în măsura în care sistemele respective sunt utilizate în scopul aplicării legii, al migrației, al azilului și al gestionării controlului la frontiere sau al administrării justiției și al proceselor democratice, ar trebui să aibă competențe de investigare și corective efective, inclusiv cel puțin competența de a obține acces la toate datele cu caracter personal care sunt prelucrate și la toate informațiile necesare pentru îndeplinirea sarcinilor sale. Autoritățile de supraveghere a pieței ar trebui să își poată exercita competențele acționând cu deplină independență. Nicio limitare a accesului acestora la date operaționale sensibile în temeiul prezentului regulament nu ar trebui să aducă atingere competențelor care le sunt conferite prin Directiva (UE) 2016/680. Nicio excludere în ceea ce privește divulgarea de date către autoritățile naționale de protecție a datelor în temeiul prezentului regulament nu ar trebui să afecteze competențele actuale sau viitoare ale autorităților respective în afara domeniului de aplicare al prezentului regulament.

(160) Autoritățile de supraveghere a pieței și Comisia ar trebui să poată propune activități comune, inclusiv investigații comune, care să fie efectuate de autoritățile de supraveghere a pieței sau de autoritățile de supraveghere a pieței în colaborare cu Comisia și care au scopul de a promova conformitatea, de a identifica cazurile de neconformitate, de a sensibiliza și de a oferi orientări în legătură cu prezentul regulament în ceea ce privește anumite categorii de sisteme de IA cu grad ridicat de risc despre care se constată că prezintă un risc grav în două sau mai multe state membre. Activitățile comune de promovare a conformității ar trebui desfășurate în conformitate cu articolul 9 din Regulamentul (UE) 2019/1020. Oficiul pentru IA ar trebui să ofere sprijin sub formă de coordonare pentru investigațiile comune.

(161) Este necesar să se clarifice responsabilitățile și competențele la nivelul Uniunii și la nivel național în ceea ce privește sistemele de IA care au la bază modele de IA de uz general. Pentru a evita suprapunerea competențelor, în cazul în care un sistem de IA se bazează pe un model de IA de uz general, iar modelul și sistemul sunt furnizate de același furnizor, supravegherea ar trebui să aibă loc la nivelul Uniunii prin intermediul Oficiului pentru IA, care, în acest scop, ar trebui să dețină competențele unei autorități de supraveghere a pieței în sensul Regulamentului (UE) 2019/1020. În toate celelalte cazuri, responsabilitatea privind supravegherea sistemelor de IA rămâne în sarcina autorităților naționale de supraveghere a pieței. Cu toate acestea, pentru sistemele de IA de uz general care pot fi utilizate direct de către implementatori pentru cel puțin un scop clasificat ca prezentând un grad ridicat de risc, autoritățile de supraveghere a pieței ar trebui să coopereze cu Oficiul pentru IA pentru a efectua evaluări ale conformității și să informeze în consecință comitetul și alte autorități de supraveghere a pieței. În plus, autoritățile de supraveghere a pieței ar trebui să poată solicita asistență din partea Oficiului pentru IA în cazul în care autoritatea de supraveghere a pieței nu este în măsură să finalizeze o investigație cu privire la un sistem de IA cu grad ridicat de risc din cauza incapacității sale de a accesa anumite informații legate de modelul de IA de uz general care stă la baza sistemului de IA cu grad ridicat de risc. În astfel de cazuri, ar trebui să se aplice *mutatis mutandis* procedura privind asistența reciprocă transfrontalieră din capitolul VI din Regulamentul (UE) 2019/1020.

(162) Pentru a utiliza în mod optim cunoștințele de specialitate centralizate ale Uniunii și sinergiile de la nivelul Uniunii, competențele de supraveghere și de executare a obligațiilor care le revin furnizorilor de modele de IA de uz general ar trebui să fie deținute de Comisie. Oficiul pentru IA ar trebui să fie în măsură să întreprindă toate acțiunile necesare pentru a monitoriza punerea în aplicare efectivă a prezentului regulament în ceea ce privește modelele de IA de uz general. Acesta ar trebui să fie în măsură să investigheze posibilele încălcări ale normelor privind furnizorii de modele de IA de uz general, atât din proprie inițiativă, dând curs rezultatelor activităților sale de monitorizare, cât și la cererea autorităților de supraveghere a pieței, în conformitate cu condițiile stabilite în prezentul regulament. Pentru a sprijini desfășurarea în mod eficace de către Oficiul pentru IA a monitorizării, acesta ar trebui să prevadă posibilitatea ca furnizorii din aval să depună plângeri cu privire la posibile încălcări ale normelor privind furnizorii de sisteme și modele de IA de uz general.

(163) În vederea completării sistemelor de guvernanță pentru modelele de IA de uz general, grupul științific ar trebui să sprijine activitățile de monitorizare ale Oficiului pentru IA și poate, în anumite cazuri, să furnizeze Oficiului pentru IA alerte calificate care declanșează acțiuni subsecvente, de exemplu investigații. Acest lucru ar trebui să fie valabil atunci când grupul științific are motive să suspecteze că un model de IA de uz general prezintă un risc concret și identificabil la nivelul Uniunii. În plus, acest lucru ar trebui să fie valabil atunci când grupul științific are motive să suspecteze că un model de IA de uz general îndeplinește criteriile care ar conduce la o clasificare ca model de IA de uz general cu risc sistemic. Pentru ca grupul științific să dispună de informațiile necesare în îndeplinirea sarcinilor respective, ar trebui să existe un mecanism prin care acesta să poată solicita Comisiei să impună furnizorilor să ofere documente sau informații.

(164) Oficiul pentru IA ar trebui să poată lua măsurile necesare pentru a monitoriza punerea în aplicare efectivă și respectarea obligațiilor furnizorilor de modele de IA de uz general prevăzute în prezentul regulament. Oficiul pentru IA ar trebui să fie în măsură să investigheze posibilele încălcări în conformitate cu competențele prevăzute în prezentul regulament, inclusiv prin solicitarea unor documente și informații, prin desfășurarea de evaluări, precum și prin solicitarea luării de măsuri de către furnizorii de modele de IA de uz general. În desfășurarea evaluărilor, pentru a utiliza cunoștințe de specialitate cu caracter independent, Oficiul pentru IA ar trebui să poată implica experți independenți pentru a desfășura evaluările în numele său. Respectarea obligațiilor ar trebui să fie asigurată, printre altele, prin cereri de a lua măsuri adecvate, inclusiv măsuri de atenuare a riscurilor în cazul unor riscuri sistemice identificate, precum și prin restricționarea punerii la dispoziție pe piață, retragerea sau rechemarea modelului. Ca o garanție, în cazul în care aceasta este necesară dincolo de drepturile procedurale prevăzute în prezentul regulament, furnizorii de modele de IA de uz general ar trebui să beneficieze de drepturile procedurale prevăzute la articolul 18 din Regulamentul (UE) 2019/1020, care ar trebui să se aplice *mutatis mutandis*, fără a aduce atingere drepturilor procedurale mai specifice prevăzute în prezentul regulament.

(165) 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 IA conform unor principii etice și fiabile în Uniune. Furnizorii de sisteme de IA care nu prezintă un grad ridicat de risc ar trebui să fie încurajați să creeze coduri de conduită, inclusiv mecanisme de guvernanță conexe, menite să promoveze aplicarea parțială sau integrală, în mod voluntar, a cerințelor obligatorii aplicabile sistemelor de IA cu grad ridicat de risc, adaptate în funcție de scopul preconizat al sistemelor și de riscul mai scăzut implicat și ținând seama de soluțiile tehnice disponibile și de bunele practici din industrie, cum ar fi modelele și cardurile de date. Furnizorii și, după caz, implementatorii tuturor modelelor de IA și sistemelor de IA cu sau fără grad ridicat de risc ar trebui, de asemenea, să fie încurajați să aplice în mod voluntar cerințe suplimentare legate, de exemplu, de elementele Orientărilor Uniunii în materie de etică pentru o IA fiabilă, de durabilitatea mediului, de măsuri de alfabetizare în domeniul IA, de proiectarea și dezvoltarea sistemelor de IA ținând seama de incluziune și diversitate, inclusiv acordând atenție persoanelor vulnerabile și accesibilității pentru persoanele cu dizabilități, de participarea părților interesate în proiectarea și dezvoltarea sistemelor de IA, cu implicarea, după caz, a părților interesate relevante, cum ar fi întreprinderi și organizații ale societății civile, mediul academic, organizații de cercetare, sindicate și organizații de protecție a consumatorilor, precum și de diversitatea în cadrul echipelor de dezvoltare, inclusiv echilibrul de gen. Pentru a se asigura eficacitatea lor, codurile de conduită voluntare ar trebui să se bazeze pe obiective clare și pe indicatori-cheie de performanță pentru a măsura îndeplinirea obiectivelor respective. Acestea ar trebui, de asemenea, să fie dezvoltate într-un mod incluziv, după caz, cu implicarea părților interesate relevante, cum ar fi întreprinderi și organizații ale societății civile, mediul academic, organizații de cercetare, sindicate și organizații de protecție a consumatorilor. 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 și interoperabilitatea semantică și tehnică a diferitelor tipuri de date.

(166) 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 pentru sistemele de IA cu grad ridicat de risc să fie totuși sigure atunci când sunt introduse pe piață sau puse în funcțiune. Pentru a contribui la acest obiectiv, Regulamentul (UE) 2023/988 al Parlamentului European și a Consiliului[53] ar fi aplicat ca o „plasă de siguranță”.

(167) 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. Acestea ar trebui să își îndeplinească sarcinile și activitățile astfel încât să protejeze, în special, drepturile de proprietate intelectuală, informațiile comerciale confidențiale și secretele comerciale, punerea în aplicare efectivă a prezentului regulament, interesele de securitate publică și națională, integritatea procedurilor penale și administrative și integritatea informațiilor clasificate.

---

[53] Regulamentul (UE) 2023/988 al Parlamentului European și al Consiliului din 10 mai 2023 privind siguranța generală a produselor, de modificare a Regulamentului (UE) nr. 1025/2012 al Parlamentului European și al Consiliului și a Directivei (UE) 2020/1828 a Parlamentului European și a Consiliului și de abrogare a Directivei 2001/95/CE a Parlamentului European și a Consiliului și a Directivei 87/357/CEE a Consiliului (JO L 135, 23.5.2023, p. 1).

(168) Respectarea prezentului regulament ar trebui să fie asigurată prin impunerea de sancțiuni și alte măsuri de executare. Statele membre ar trebui să ia toate măsurile necesare pentru a se asigura că sunt puse în aplicare dispozițiile prezentului regulament, inclusiv prin stabilirea unor sancțiuni efective, proporționale și cu efect de descurajare în cazul încălcării acestora, și pentru a respecta principiul *ne bis in idem*. În scopul de a consolida și armoniza sancțiunile administrative pentru încălcarea prezentului regulament, ar trebui să fie definite limitele superioare pentru stabilirea amenzilor administrative pentru anumite încălcări specifice. Atunci când evaluează cuantumul amenzilor, statele membre ar trebui, în fiecare caz în parte, să țină seama de toate circumstanțele relevante ale situației specifice, acordând atenția cuvenită, în special, naturii, gravității și duratei încălcării și consecințelor acesteia, precum și dimensiunii furnizorului, în special în cazul în care furnizorul este un IMM, inclusiv o întreprindere nou-înființată. 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.

(169) Respectarea obligațiilor impuse furnizorilor de modele de IA de uz general în temeiul prezentului regulament ar trebui să fie asigurată, printre altele, prin amenzi. În acest scop, ar trebui să fie stabilite, de asemenea, niveluri adecvate ale amenzilor pentru încălcarea obligațiilor respective, inclusiv pentru nerespectarea măsurilor impuse de Comisie în conformitate cu prezentul regulament, sub rezerva unor termene de prescripție adecvate, în conformitate cu principiul proporționalității. Toate deciziile luate de Comisie în temeiul prezentului regulament fac obiectul controlului jurisdicțional al Curții de Justiție a Uniunii Europene în conformitate cu TFUE, incluzând competența nelimitată a Curții de Justiție cu privire la sancțiuni în temeiul articolului 261 din TFUE.

(170) Dreptul Uniunii și dreptul intern prevăd deja căi de atac efective pentru persoanele fizice și juridice ale căror drepturi și libertăți sunt afectate în mod negativ de utilizarea sistemelor de IA. Fără a aduce atingere căilor de atac respective, orice persoană fizică sau juridică care are motive să considere că a avut loc o încălcare a prezentului regulament ar trebui să aibă dreptul de a depune o plângere la autoritatea relevantă de supraveghere a pieței.

(171) Persoanele afectate ar trebui să aibă dreptul de a obține o explicație atunci când decizia implementatorului este bazată în principal pe rezultatele anumitor sisteme de IA cu grad ridicat de risc care intră în domeniul de aplicare al prezentului regulament și în cazul în care decizia respectivă produce efecte juridice sau afectează în mod similar în mod semnificativ persoanele respective într-o manieră pe care acestea o consideră ca având un impact negativ asupra sănătății, siguranței sau drepturilor fundamentale ale acestora. Explicația respectivă ar trebui să fie clară și semnificativă și să ofere un temei pentru exercitarea drepturilor de către persoanele afectate. Dreptul de a obține o explicație nu ar trebui să se aplice în cazul utilizării unor sisteme de IA care fac obiectul unor excepții sau restricții care decurg din dreptul Uniunii sau din dreptul intern și ar trebui să se aplice numai în măsura în care acest drept nu este deja prevăzut în dreptul Uniunii.

(172) Persoanele care acționează în calitate de avertizori de integritate cu privire la încălcările prezentului regulament ar trebui să fie protejate în temeiul dreptului Uniunii. În ceea ce privește raportarea încălcărilor prezentului regulament și protecția persoanelor care raportează astfel de încălcări ar trebui, prin urmare, să se aplice Directiva (UE) 2019/1937 a Parlamentului European și a Consiliului[54].

---

[54] Directiva (UE) 2019/1937 a Parlamentului European și a Consiliului din 23 octombrie 2019 privind protecția persoanelor care raportează încălcări ale dreptului Uniunii (JO L 305, 26.11.2019, p. 17).

(173) 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 să fie delegată Comisiei pentru a modifica condițiile în care un sistem de IA nu este considerat ca având un grad ridicat de risc, lista sistemelor de IA cu grad ridicat de risc, dispozițiile privind documentația tehnică, conținutul declarației de conformitate UE, dispozițiile privind procedurile de evaluare a conformității, 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 pe evaluarea documentației tehnice, pragul, valorile de referință și indicatorii din cadrul normelor pentru clasificarea modelelor de IA de uz general cu risc sistemic, inclusiv prin completarea valorilor de referință și indicatorilor respectivi, criteriile pentru desemnarea modelelor de IA de uz general cu risc sistemic, documentația tehnică pentru furnizorii de modele de IA de uz general și informațiile privind transparența pentru furnizorii de modele de IA de uz general. 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[55]. 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.

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

(174) Având în vedere evoluțiile tehnologice rapide și cunoștințele de specialitate tehnice necesare pentru aplicarea eficientă a prezentului regulament, Comisia ar trebui să evalueze și să revizuiască prezentul regulament până la ... [cinci ani de la data intrării în vigoare a prezentului regulament] și, ulterior, o dată la patru ani și să raporteze Parlamentului European și Consiliului în acest sens. În plus, ținând seama de implicațiile pentru domeniul de aplicare al prezentului regulament, Comisia ar trebui să efectueze o evaluare a necesității de a modifica, o dată pe an, lista sistemelor de IA cu grad ridicat de risc și lista practicilor interzise. În plus, până la ... [patru ani de la data intrării în vigoare a prezentului regulament] și, ulterior, o dată la patru ani, Comisia ar trebui să evalueze necesitatea de a modifica lista rubricilor de domeniu cu grad ridicat de risc din anexa la prezentul regulament, sistemele de IA care intră în domeniul de aplicare al obligațiilor de transparență, eficacitatea sistemului de supraveghere și de guvernanță și progresele înregistrate în ceea ce privește elaborarea de documente de standardizare privind dezvoltarea eficientă din punct de vedere energetic a modelelor de IA de uz general, inclusiv necesitatea unor măsuri sau acțiuni suplimentare și să raporteze Parlamentului European și Consiliului în acest sens. În cele din urmă, până la ... [patru ani de la data intrării în vigoare a prezentului regulament] și, ulterior, o dată la trei ani, Comisia ar trebui să evalueze impactul și eficacitatea codurilor de conduită voluntare în ceea ce privește încurajarea aplicării cerințelor prevăzute pentru sistemele de IA cu grad ridicat de risc în cazul altor sisteme de IA decât cele cu grad ridicat de risc și, eventual, a altor cerințe suplimentare pentru sistemele de IA respective.

(175) În vederea asigurării unor condiții uniforme pentru punerea în aplicare a prezentului regulament, ar trebui să fie conferite competențe de executare Comisiei. Respectivele competențe ar trebui să fie exercitate în conformitate cu Regulamentul (UE) nr. 182/2011 al Parlamentului European și al Consiliului[56].

(176) Întrucât obiectivul prezentului regulament, și anume de a îmbunătăți funcționarea pieței interne și de a promova adoptarea IA centrate pe factorul uman și fiabile, asigurând în același timp un nivel ridicat de protecție a sănătății, a siguranței și a drepturilor fundamentale consacrate în Cartă, inclusiv a democrației, a statului de drept și a mediului împotriva efectelor dăunătoare ale sistemelor de IA din Uniune, și sprijinind inovarea, nu poate fi realizat în mod satisfăcător de către statele membre și, având în vedere amploarea sau efectele acțiunii sale, poate fi realizat mai bine la nivelul Uniunii, aceasta din urmă poate adopta măsuri, în conformitate cu principiul subsidiarității, astfel cum se prevede 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.

---

[56] 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).

(177) 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 acestuia, 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 că, în acest sens, conceptul de modificare semnificativă ar trebui să fie 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, în temeiul prezentului regulament. În mod excepțional și având în vedere răspunderea publică, operatorii de sisteme de IA care fac parte din sistemele informatice la scară largă instituite prin actele juridice care sunt enumerate într-o anexă la prezentul regulament și operatorii de sisteme de IA cu grad ridicat de risc care sunt destinate a fi utilizate de autoritățile publice ar trebui să ia măsurile necesare pentru a se conforma cerințelor prezentului regulament până la sfârșitul anului 2030 și, respectiv, până la ... [șase ani de la data intrării în vigoare a prezentului regulament].

(178) Furnizorii de sisteme de IA cu grad ridicat de risc sunt încurajați să înceapă să se conformeze, în mod voluntar, obligațiilor relevante aferente prezentului regulament încă din perioada de tranziție.

(179) Prezentul regulament ar trebui să se aplice de la ... [doi ani de la data intrării în vigoare a prezentului regulament]. Cu toate acestea, ținând seama de riscul inacceptabil asociat utilizării IA în anumite moduri, interdicțiile și dispozițiile cu caracter general din prezentul regulament ar trebui să se aplice deja de la ... [șase luni de la data intrării în vigoare a prezentului regulament]. Deși efectul deplin al interdicțiilor respective este corelat cu instituirea guvernanței și cu aplicarea prezentului regulament, aplicarea anticipată a interdicțiilor este importantă pentru a se ține seama de riscurile inacceptabile și pentru a produce efecte asupra altor proceduri, cum ar fi în dreptul civil. În plus, infrastructura legată de guvernanță și de sistemul de evaluare a conformității ar trebui să fie operațională înainte de ... [doi ani de la data intrării în vigoare a prezentului regulament]; prin urmare, dispozițiile privind organismele notificate și structura de guvernanță ar trebui să se aplice de la ... [12 luni de la data intrării în vigoare a prezentului regulament]. Având în vedere ritmul rapid al progreselor tehnologice și al adoptării modelelor de IA de uz general, ar trebui ca obligațiile furnizorilor de modele de IA de uz general să se aplice de la ... [12 luni de la data intrării în vigoare a prezentului regulament]. Codurile de bune practici ar trebui să fie gata până la ... [nouă luni de la data intrării în vigoare a prezentului regulament], pentru a permite furnizorilor să demonstreze conformitatea în timp util. Oficiul pentru IA ar trebui să se asigure că normele și procedurile de clasificare sunt actualizate în funcție de evoluțiile tehnologice. 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 efectiv până la data aplicării prezentului regulament. Prin urmare, dispozițiile privind sancțiunile ar trebui să se aplice de la ...[12 luni de la data intrării în vigoare a prezentului regulament].

(180) Autoritatea Europeană pentru Protecția Datelor și Comitetul european pentru protecția datelor au fost consultate în conformitate cu articolul 42 alineatele (1) și (2) din Regulamentul (UE) 2018/1725 și au emis avizul lor comun la 18 iunie 2021,

ADOPTĂ PREZENTUL REGULAMENT:

Capitolul I
Dispoziții generale

Articolul 1

Obiectul

(1) Scopul prezentului regulament este de a îmbunătăți funcționarea pieței interne, de a promova adoptarea inteligenței artificiale (IA) centrate pe factorul uman și fiabile, asigurând în același timp un nivel ridicat de protecție a sănătății, a siguranței și a drepturilor fundamentale consacrate în Cartă, inclusiv a democrației, a statului de drept și a mediului împotriva efectelor dăunătoare ale sistemelor de IA din Uniune, și sprijinind inovarea.

(2) Prezentul regulament stabilește:

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

(b) interdicții privind anumite practici în domeniul IA;

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

(d) norme armonizate de transparență pentru anumite sisteme de IA;

(e) norme armonizate privind introducerea pe piață a modelelor de IA de uz general;

(f) norme privind monitorizarea pieței, supravegherea pieței, guvernanța și aplicarea prezentului regulament;

(g) măsuri de susținere a inovării, cu un accent deosebit pe IMM-uri, inclusiv pe întreprinderile nou-înființate.

Articolul 2

Domeniul de aplicare

(1) Prezentul regulament se aplică pentru:

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

(b) implementatorii de sisteme de IA care își au sediul sau se află pe teritoriul Uniunii;

(c) furnizorii și implementatorii de sisteme de IA care își au sediul sau se află într-o țară terță, în cazul în care rezultatele produse de sistemele de IA 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, care nu sunt stabiliți în Uniune;

(g) persoanele afectate care se află în Uniune.

(2) În cazul sistemelor de IA clasificate ca sisteme de IA prezentând un grad ridicat de risc în conformitate cu articolul 6 alineatul (1), legate de produse care fac obiectul actelor legislative de armonizare ale Uniunii care figurează în anexa I secțiunea B, se aplică numai articolul 6 alineatul (1), articolele 102-109 și articolul 112. Articolul 57 se aplică numai în măsura în care cerințele pentru sistemele de IA cu grad ridicat de risc prevăzute în temeiul prezentului regulament au fost integrate în respectivele acte legislative de armonizare ale Uniunii.

(3) Prezentul regulament nu se aplică domeniilor care nu intră în sfera de cuprindere a dreptului Uniunii și, în orice caz, nu afectează competențele statelor membre în materie de securitate națională, indiferent de tipul de entitate însărcinată de statele membre să îndeplinească sarcinile legate de competențele respective.

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 modificări exclusiv în scopuri militare, de apărare sau de securitate națională, indiferent de tipul de entitate care desfășoară activitățile respective.

Prezentul regulament nu se aplică sistemelor de IA care nu sunt introduse pe piață sau puse în funcțiune în Uniune, în cazul în care rezultatul este utilizat în Uniune exclusiv în scopuri 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 sfera de cuprindere a prezentului regulament în temeiul alineatului (1), în cazul în care respectivele autorități sau organizații utilizează sisteme de IA în cadrul cooperării sau acordurilor internaționale pentru aplicarea legii și pentru cooperarea judiciară cu Uniunea sau cu unul sau mai multe state membre, cu condiția ca o astfel de țară terță sau organizație internațională să ofere garanții adecvate în ceea ce privește protecția drepturilor și libertăților fundamentale ale persoanelor.

(5) Prezentul regulament nu aduce atingere aplicării dispozițiilor privind răspunderea furnizorilor de servicii intermediare cuprinse în capitolul II din Regulamentul (UE) 2022/2065.

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

(7) Dreptul Uniunii privind protecția datelor cu caracter personal, a vieții private și a confidențialității comunicațiilor se aplică datelor cu caracter personal prelucrate în legătură cu drepturile și obligațiile prevăzute în prezentul regulament. Prezentul regulament nu afectează Regulamentul (UE) 2016/679 sau (UE) 2018/1725 ori Directiva 2002/58/CE sau (UE) 2016/680, fără a aduce atingere articolului 10 alineatul (5) și articolului 59 din prezentul regulament.

(8) Prezentul regulament nu se aplică niciunei activități de cercetare, testare sau dezvoltare privind sisteme de IA sau modele de IA, înainte ca acestea să fie introduse pe piață sau puse în funcțiune. Astfel de activități se desfășoară în conformitate cu dreptul aplicabil al Uniunii. Testarea în condiții reale nu face obiectul excluderii menționate.

(9) Prezentul regulament nu aduce atingere normelor prevăzute de alte acte juridice ale Uniunii referitoare la protecția consumatorilor și la siguranța produselor.

(10) Prezentul regulament nu se aplică obligațiilor implementatorilor persoane fizice care utilizează sisteme de IA în cursul unei activități strict personale, fără caracter profesional.

(11) Prezentul regulament nu împiedică Uniunea sau statele membre să mențină sau să introducă acte cu putere de lege și acte administrative care sunt mai favorabile lucrătorilor privind protejarea drepturilor acestora în ceea ce privește utilizarea sistemelor de IA de către angajatori sau să încurajeze ori să permită aplicarea unor contracte colective de muncă care sunt mai favorabile lucrătorilor.

(12) Prezentul regulament nu se aplică sistemelor de IA lansate sub licențe libere și cu sursă deschisă, cu excepția cazului în care acestea sunt introduse pe piață sau puse în funcțiune ca sisteme de IA cu grad ridicat de risc sau ca sisteme de IA care intră sub incidența articolului 5 sau a articolului 50.

Articolul 3

Definiții

În sensul prezentului regulament, se aplică următoarele definiții:

1. „sistem de IA” înseamnă un sistem bazat pe o mașină care este conceput să funcționeze cu diferite niveluri de autonomie și care poate prezenta adaptabilitate după implementare, și care, urmărind obiective explicite sau implicite, deduce, din datele de intrare pe care le primește, modul de generare a unor rezultate precum previziuni, conținut, recomandări sau decizii care pot influența mediile fizice sau virtuale;

2. „risc” înseamnă combinația dintre probabilitatea producerii unui prejudiciu și gravitatea acestuia;

3. „furnizor” înseamnă o persoană fizică sau juridică, o autoritate publică, o agenție sau un alt organism care dezvoltă un sistem de IA sau un model de IA de uz general sau care comandă dezvoltarea unui sistem de IA sau a unui model de IA de uz general și îl introduce pe piață sau pune în funcțiune sistemul de IA sub propriul nume sau propria marcă comercială, contra cost sau gratuit;

4. „implementator” înseamnă o persoană fizică sau juridică, autoritate publică, agenție sau alt organism care utilizează un sistem de IA aflat sub autoritatea sa, cu excepția cazului în care sistemul de IA este utilizat în cursul unei activități personale, fără caracter profesional;

5. „reprezentant autorizat” înseamnă o persoană fizică sau juridică aflată sau stabilită în Uniune care a primit și a acceptat un mandat scris din partea unui furnizor al unui sistem de IA sau al unui model de IA de uz general pentru a exercita și, respectiv, a îndeplini, în numele său, obligațiile și procedurile stabilite prin prezentul regulament;

6. „importator” înseamnă o persoană fizică sau juridică aflată sau stabilită în Uniune care introduce pe piață un sistem de IA care poartă numele sau marca unei persoane fizice sau juridice stabilite într-o țară terță;

7. „distribuitor” înseamnă o 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 furnizor, fabricant de produse, implementator, reprezentant autorizat, importator sau distribuitor;

9. „introducere pe piață” înseamnă prima punere la dispoziție a unui sistem de IA sau a unui model de IA de uz general pe piața Uniunii;

10. „punere la dispoziție pe piață” înseamnă furnizarea unui sistem de IA sau a unui model de IA de uz general 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 implementatorului sau pentru uz propriu în Uniune, în scopul său preconizat;

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, inclusiv cu alte sisteme de IA;

14. „componentă de siguranță” înseamnă o componentă a unui produs sau a unui sistem de IA care îndeplinește o funcție de siguranță pentru produsul sau sistemul de IA 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 implementatorul, 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 implementatorilor;

17. „retragere a unui sistem de IA” înseamnă orice măsură care are drept scop împiedicarea punerii 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 îndeplini scopul preconizat;

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

20. „evaluare a conformității” înseamnă procesul prin care se demonstrează dacă au fost îndeplinite sau nu cerințele prevăzute în capitolul III secțiunea 2 referitoare la un sistem de IA cu grad ridicat de risc;

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 notificat în conformitate cu prezentul regulament și cu alte acte legislative relevante de armonizare ale Uniunii;

23. „modificare substanțială” înseamnă o modificare a unui sistem de IA după introducerea sa pe piață sau punerea sa în funcțiune, care nu este prevăzută sau planificată în evaluarea inițială a conformității realizată de furnizor și în urma căreia este afectată conformitatea sistemului de IA cu cerințele prevăzute în capitolul III secțiunea 2 sau care conduce la o modificare a scopului preconizat pentru care a fost evaluat sistemul de IA;

24. „marcaj CE” înseamnă un marcaj prin care un furnizor indică faptul că un sistem de IA este în conformitate cu cerințele prevăzute în capitolul III secțiunea 2 și în alte acte legislative de armonizare aplicabile ale Uniunii care prevăd aplicarea acestui marcaj;

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. „standard armonizat” înseamnă un standard armonizat, în sensul definiției de la articolul 2 punctul 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 validare” 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 subadaptarea sau supraadaptarea;

31. „set de date de validare” înseamnă un set de date separat sau o parte a setului de date de antrenament, sub forma unei divizări fixe sau variabile;

32. „date de testare” înseamnă datele utilizate pentru a furniza o evaluare independentă a sistemului de IA, în scopul de a confirma performanța preconizată a sistemului respectiv înainte de introducerea sa pe piață sau de punerea sa în funcțiune;

33. „date de intrare” înseamnă datele furnizate unui sistem de IA sau dobândite direct de acesta, pe baza cărora sistemul produce un rezultat;

34. „date biometrice” înseamnă datele cu caracter personal rezultate dintr-o prelucrare tehnică specifică, referitoare la caracteristicile fizice, fiziologice sau comportamentale ale unei persoane fizice, cum ar fi imaginile faciale sau datele dactiloscopice;

35. „identificare biometrică” înseamnă recunoașterea automată a caracteristicilor fizice, fiziologice, comportamentale sau psihologice ale omului în scopul stabilirii identității unei persoane fizice prin compararea datelor biometrice ale persoanei respective cu datele biometrice ale persoanelor stocate într-o bază de date;

36. „verificare biometrică” înseamnă verificarea automată, pe baza unei comparații între două seturi de date, inclusiv autentificarea, a identității persoanelor fizice prin compararea datelor biometrice ale acestora cu datele biometrice furnizate anterior;

37. „categorii speciale de date cu caracter personal” înseamnă categoriile 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;

38. „date operaționale sensibile” înseamnă date operaționale legate de activități de prevenire, depistare, investigare sau urmărire penală a infracțiunilor a căror divulgare ar putea pune în pericol integritatea unor proceduri penale;

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

40. „sistem de clasificare biometrică” înseamnă un sistem de IA al cărui scop este de a încadra persoanele fizice în categorii specifice pe baza datelor lor biometrice, cu excepția cazului în care acesta este auxiliar unui alt serviciu comercial și strict necesar din motive tehnice obiective;

41. „sistem de identificare biometrică la distanță” înseamnă un sistem de IA al cărui scop este de a identifica persoanele fizice, fără implicarea activă a acestora, de obicei la distanță, prin compararea datelor biometrice ale unei persoane cu datele biometrice conținute într-o bază de date de referință;

42. „sistem de identificare biometrică la distanță în timp real” înseamnă un sistem de identificare biometrică la distanță în care atât capturarea datelor biometrice, cât și compararea și identificarea au loc fără întârzieri semnificative, incluzând nu numai identificarea instantanee, ci și întârzieri scurte limitate pentru a se evita eludarea;

43. „sistem de identificare biometrică la distanță ulterioară” înseamnă un alt sistem de identificare biometrică la distanță decât sistemul de identificare biometrică la distanță în timp real;

44. „spațiu accesibil publicului” înseamnă orice loc fizic aflat în proprietate publică sau privată, accesibil unui număr nedeterminat de persoane fizice, indiferent dacă se pot aplica anumite condiții de acces și indiferent de potențiale restricții de capacitate;

45. „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 sancțiunilor penale, 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 sancțiunilor penale, inclusiv al protejării împotriva amenințărilor la adresa securității publice și al prevenirii acestora;

46. „aplicarea 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 sancțiunilor penale, inclusiv pentru protejarea împotriva amenințărilor la adresa securității publice și prevenirea acestora;

47. „Oficiul pentru IA” înseamnă funcția Comisiei de a contribui la punerea în aplicare, monitorizarea și supravegherea sistemelor de IA și a modelelor de IA de uz general și la guvernanța IA, prevăzută în Decizia din 24 ianuarie 2024 a Comisiei; trimiterile din prezentul regulament la Oficiul pentru IA se interpretează ca trimiteri la Comisie;

48. „autoritate națională competentă” înseamnă o autoritate de notificare sau o autoritate de supraveghere a pieței; în ceea ce privește sistemele de IA puse în funcțiune sau utilizate de instituțiile, agențiile, oficiile și organele Uniunii, mențiunile referitoare la autoritățile naționale competente sau la autoritățile de supraveghere a pieței din prezentul regulament se interpretează ca mențiuni referitoare la Autoritatea Europeană pentru Protecția Datelor;

49. „incident grav” înseamnă un incident sau funcționarea necorespunzătoare a unui sistem de IA care, direct sau indirect, conduce la oricare dintre următoarele:

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

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

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

(d) daune grave aduse bunurilor sau mediului;

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

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

52. „creare de profiluri” înseamnă creare de profiluri în sensul definiției de la articolul 4 punctul 4 din Regulamentul (UE) 2016/679;

53. „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;

54. „plan privind spațiul de testare” înseamnă un document convenit între furnizorul participant și autoritatea competentă care descrie obiectivele, condițiile, calendarul, metodologia și cerințele pentru activitățile desfășurate în spațiul de testare;

55. „spațiu de testare în materie de reglementare în domeniul IA” înseamnă un cadru controlat instituit de o autoritate 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 privind spațiul de testare, pentru o perioadă limitată de timp, sub supraveghere reglementară;

56. „alfabetizare în domeniul IA” înseamnă competențele, cunoștințele și înțelegerea care le permit furnizorilor, implementatorilor și persoanelor afectate, ținând seama de drepturile și obligațiile lor respective în contextul prezentului regulament, să implementeze sistemele de IA în cunoștință de cauză și să conștientizeze oportunitățile și riscurile pe care le implică IA, precum și prejudiciile pe care le pot aduce;

57. „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 și nu se consideră introducere pe piață sau punere în funcțiune a sistemului de IA în sensul prezentului regulament, dacă sunt îndeplinite toate condițiile prevăzute la articolul 57 sau 60;

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

59. „consimțământ în cunoștință de cauză” înseamnă exprimarea liberă, specifică, neechivocă 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;

60. „deepfake” înseamnă o imagine ori un conținut audio sau video generat sau manipulat de IA care prezintă o asemănare cu persoane, obiecte, locuri sau alte entități ori evenimente existente și care ar crea unei persoane impresia falsă că este autentic sau adevărat;

61. „încălcare pe scară largă” înseamnă orice acțiuni sau omisiuni contrare dreptului Uniunii care protejează interesele persoanelor fizice și care:

(a) au adus sau ar putea aduce prejudicii intereselor colective ale persoanelor care își au reședința în cel puțin două state membre diferite de statul membru în care:

(i) au fost inițiate sau au avut loc acțiunile sau omisiunile în cauză;

(ii) se află sau este stabilit furnizorul în cauză sau, după caz, reprezentantul său autorizat; sau

(iii) este stabilit implementatorul, atunci când încălcarea este comisă de implementator;

(b) au adus, aduc sau sunt susceptibile să aducă prejudicii intereselor colective ale persoanelor și au caracteristici comune, cum ar fi aceeași practică ilegală, încălcarea aceluiași interes, care survin în același timp, fiind comise de același operator, în cel puțin trei state membre;

62. „infrastructură critică” înseamnă infrastructură critică în sensul definiției de la articolul 2 punctul 4 din Directiva (UE) 2022/2557;

63. „model de IA de uz general” înseamnă un model de IA, inclusiv în cazul în care un astfel de model de IA este antrenat cu un volum mare de date care utilizează autosupravegherea la scară largă, care prezintă o generalitate semnificativă și este capabil să îndeplinească în mod competent o gamă largă de sarcini distincte, indiferent de modul în care este introdus pe piață și care poate fi integrat într-o varietate de sisteme sau aplicații din aval, cu excepția modelelor de IA care sunt utilizate pentru activități de cercetare, dezvoltare sau creare de prototipuri înainte de introducerea pe piață;

64. „capabilități cu impact ridicat” înseamnă capabilități care corespund capabilităților înregistrate în cele mai avansate modele de IA de uz general sau depășesc capabilitățile respective;

65. „risc sistemic” înseamnă un risc specific capabilităților cu impact ridicat ale modelelor de IA de uz general, având un impact semnificativ asupra pieței Uniunii ca urmare a amplorii acestora sau a efectelor negative reale sau previzibile în mod rezonabil asupra sănătății publice, siguranței, securității publice, drepturilor fundamentale sau asupra societății în ansamblu, care poate fi propagat la scară largă de-a lungul lanțului valoric;

66. „sistem de IA de uz general” înseamnă un sistem de IA care se bazează pe un model de IA de uz general și care are capabilitatea de a deservi o varietate de scopuri, atât pentru utilizare directă, cât și pentru integrarea în alte sisteme de IA;

67. „operație în virgulă mobilă” înseamnă orice operație matematică sau atribuire care implică numere în virgulă mobilă, care sunt o subcategorie a numerelor reale și sunt reprezentate de regulă în informatică printr-un număr întreg cu precizie fixă multiplicat cu o bază fixă având un exponent număr întreg;

68. „furnizor din aval” înseamnă un furnizor al unui sistem de IA, inclusiv al unui sistem de IA de uz general, care integrează un model de IA, indiferent dacă modelul de IA este furnizat de furnizorul însuși și integrat vertical sau dacă acesta este furnizat de o altă entitate pe baza unor relații contractuale.

Articolul 4

Alfabetizarea în domeniul IA

Furnizorii și implementatorii de sisteme de IA iau măsuri pentru a asigura, în cea mai mare măsură posibilă, un nivel suficient de alfabetizare în domeniul IA a personalului lor și a altor persoane care se ocupă cu operarea și utilizarea sistemelor de IA în numele lor, ținând seama de cunoștințele tehnice, experiența, educația și formarea lor și de contextul în care urmează să fie folosite sistemele de IA și luând în considerare persoanele sau grupurile de persoane în legătură cu care urmează să fie folosite sistemele de IA.

Capitolul II
Practici interzise în domeniul IA

Articolul 5

Practici interzise în domeniul IA

(1) Sunt interzise următoarele practici în domeniul IA:

(a) introducerea pe piață, punerea în funcțiune sau utilizarea unui sistem de IA care utilizează tehnici subliminale ce nu pot fi percepute în mod conștient de o persoană sau tehnici intenționat manipulatoare sau înșelătoare, cu scopul sau efectul de a denatura în mod semnificativ comportamentul unei persoane sau al unui grup de persoane prin împiedicarea apreciabilă a capacității acestora de a lua o decizie în cunoștință de cauză, determinându-le astfel să ia o decizie pe care altfel nu ar fi luat-o, într-un mod care aduce sau este susceptibil în mod rezonabil să aducă prejudicii semnificative persoanei respective, unei alte persoane sau unui grup de persoane;

(b) introducerea pe piață, punerea în funcțiune sau utilizarea unui sistem de IA care exploatează oricare dintre vulnerabilitățile unei persoane fizice sau ale unui anumit grup de persoane asociate vârstei, unei dizabilități sau unei situații sociale sau economice specifice, cu scopul sau efectul de a denatura în mod semnificativ comportamentul persoanei respective sau al unei persoane care aparține grupului respectiv într-un mod care aduce sau este susceptibil în mod rezonabil să aducă prejudicii semnificative persoanei respective sau unei alte persoane;

(c) introducerea pe piață, punerea în funcțiune sau utilizarea unor sisteme de IA pentru evaluarea sau clasificarea persoanelor fizice sau a grupurilor de persoane pe o anumită perioadă de timp, pe baza comportamentului lor social sau a caracteristicilor personale sau de personalitate cunoscute, deduse sau preconizate, cu un punctaj 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) introducerea pe piață, punerea în funcțiune în acest scop specific sau utilizarea unui sistem de IA pentru efectuarea de evaluări ale riscurilor persoanelor fizice cu scopul de a evalua sau de a prevedea riscul ca o persoană fizică să comită o infracțiune, exclusiv pe baza creării profilului unei persoane fizice sau pe baza evaluării trăsăturilor și caracteristicilor sale de personalitate; această interdicție nu se aplică sistemelor de IA utilizate pentru a sprijini evaluarea umană a implicării unei persoane într-o activitate infracțională, care se bazează deja pe fapte obiective și verificabile legate direct de o activitate infracțională;

(e) introducerea pe piață, punerea în funcțiune în acest scop specific sau utilizarea unor sisteme de IA care creează sau extind bazele de date de recunoaștere facială prin extragerea fără scop precis a imaginilor faciale de pe internet sau de pe înregistrările TVCI;

(f) introducerea pe piață, punerea în funcțiune în acest scop specific sau utilizarea unor sisteme de IA pentru a deduce emoțiile unei persoane fizice în sfera locului de muncă și a instituțiilor de învățământ, cu excepția cazurilor în care utilizarea sistemului de IA este destinată a fi instituită sau introdusă pe piață din motive medicale sau de siguranță;

(g) introducerea pe piață sau punerea în funcțiune în acest scop specific sau utilizarea de sisteme de clasificare biometrică care clasifică în mod individual persoanele fizice pe baza datelor lor biometrice pentru a deduce sau a intui rasa, opiniile politice, apartenența la un sindicat, convingerile religioase sau filozofice, viața sexuală sau orientarea sexuală ale persoanelor respective; această interdicție nu se referă la etichetarea sau filtrarea seturilor de date biometrice obținute în mod legal, cum ar fi imaginile, pe baza datelor biometrice sau la clasificarea datelor biometrice în domeniul aplicării legii;

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

(i) căutarea în mod specific a anumitor victime ale răpirii, traficului de persoane sau exploatării sexuale a persoanelor, precum și căutarea persoanelor dispărute;

(ii) prevenirea unei amenințări specifice, substanțiale și iminente care vizează viața sau siguranța fizică a persoanelor fizice sau a unei amenințări reale și prezente sau reale și previzibile de atac terorist;

(iii) localizarea sau identificarea unei persoane suspectate de săvârșirea unei infracțiuni, în scopul desfășurării unei investigații penale sau al urmăririi penale sau al executării unor sancțiuni penale pentru infracțiuni, menționate în anexa II și pasibile, în statul membru în cauză, de o pedeapsă privativă de libertate sau o măsură de siguranță privativă de libertate pentru o perioadă maximă de cel puțin patru ani;

Litera (h) de la primul paragraf nu aduce atingere articolului 9 din Regulamentul (UE) 2016/679 privind prelucrarea datelor biometrice în alte scopuri decât aplicarea legii.

(2) Sistemele de identificare biometrică la distanță în timp real în spațiile accesibile publicului în scopul aplicării legii pentru oricare dintre obiectivele menționate la alineatul (1) primul paragraf litera (h) se utilizează în scopurile prevăzute la alineatul (1) litera (h) numai pentru a confirma identitatea persoanei vizate în mod specific, ținându-se seama de următoarele elemente:

(a) natura situației care determină posibila utilizare, în special gravitatea, probabilitatea și amploarea prejudiciului care ar fi cauzat dacă sistemul nu ar fi utilizat;

(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 aplicării legii pentru oricare dintre obiectivele menționate la alineatul (1) primul paragraf litera (h) de la prezentul articol respectă garanțiile și condițiile necesare și proporționale în ceea ce privește utilizarea în conformitate cu dreptul intern care autorizează utilizarea sistemelor respective, în special în ceea ce privește limitările temporale, geografice și legate de persoane. Utilizarea sistemului de identificare biometrică la distanță în timp real în spațiile accesibile publicului este autorizată numai dacă autoritatea de aplicare a legii a finalizat o evaluare a impactului asupra drepturilor fundamentale, astfel cum se prevede la articolul 27, și a înregistrat sistemul în baza de date a UE, în conformitate cu articolul 49. Cu toate acestea, în cazuri de urgență justificate în mod corespunzător, utilizarea sistemelor respective poate fi inițiată fără înregistrarea în baza de date a UE, cu condiția ca înregistrarea respectivă să fie finalizată fără întârzieri nejustificate.

(3) În sensul alineatului (1) primul paragraf litera (h) și al alineatului (2), fiecare utilizare în scopul aplicării legii a unui sistem de identificare biometrică la distanță în timp real în spațiile accesibile publicului face obiectul unei autorizații prealabile acordate de o autoritate judiciară sau de o autoritate administrativă independentă a cărei decizie are efect obligatoriu din statul membru în care urmează să aibă loc utilizarea; autorizația respectivă este emisă pe baza unei cereri motivate și în conformitate cu normele detaliate de drept intern menționate la alineatul (5). 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, cel târziu în termen de 24 de ore. În cazul în care o astfel de autorizație este refuzată, utilizarea sistemului este oprită cu efect imediat și toate datele, precum și rezultatele și produsele obținute în cadrul utilizării respective sunt înlăturate și șterse imediat.

Autoritatea judiciară competentă sau o autoritate administrativă independentă a cărei decizie are efect obligatoriu 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) primul paragraf litera (h), astfel cum a fost identificat în cerere și, în special, rămâne limitată la ceea ce este strict necesar din punctul de vedere al perioadei de timp, precum și al sferei de aplicare geografică și personală. Atunci când ia o decizie cu privire la cerere, autoritatea respectivă ia în considerare elementele menționate la alineatul (2). Nicio decizie care produce un efect juridic negativ asupra unei persoane nu poate fi luată exclusiv pe baza unui rezultat al sistemului de identificare biometrică la distanță în timp real.

(4) Fără a aduce atingere alineatului (3), fiecare utilizare a unui sistem de identificare biometrică la distanță în timp real în spațiile accesibile publicului în scopul aplicării legii este notificată autorității relevante de supraveghere a pieței și autorității naționale pentru protecția datelor, în conformitate cu normele naționale menționate la alineatul (5). Notificarea conține cel puțin informațiile specificate la alineatul (6) și nu include date operaționale sensibile.

(5) 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 aplicării legii, în limitele și condițiile enumerate la alineatul (1) primul paragraf litera (h) și la alineatele (2) și (3). Statul membru în cauză stabilește în dreptul său intern normele detaliate necesare pentru solicitarea, eliberarea și exercitarea, precum și pentru supravegherea autorizațiilor menționate la alineatul (3) și pentru raportarea cu privire la acestea. Normele respective specifică, de asemenea, pentru care dintre obiectivele enumerate la alineatul (1) primul paragraf litera (h), inclusiv pentru care dintre infracțiunile menționate la litera (h) punctul (iii) de la alineatul respectiv, pot fi autorizate autoritățile competente să utilizeze respectivele sisteme în scopul aplicării legii. Statele membre notifică normele respective Comisiei în termen de cel mult 30 de zile de la adoptarea acestora. Statele membre pot introduce, în conformitate cu dreptul Uniunii, legi mai restrictive privind utilizarea sistemelor de identificare biometrică la distanță.

(6) Autoritățile naționale de supraveghere a pieței și autoritățile naționale de protecție a datelor din statele membre care au fost notificate cu privire la utilizarea sistemelor de identificare biometrică la distanță în timp real în spațiile accesibile publicului în scopul aplicării legii în temeiul alineatului (4) prezintă Comisiei rapoarte anuale cu privire la utilizarea respectivă. În acest scop, Comisia furnizează statelor membre și autorităților naționale de supraveghere a pieței și de protecție a datelor un model, inclusiv informații privind numărul deciziilor luate de autoritățile judiciare competente sau de o autoritate administrativă independentă a cărei decizie are efect obligatoriu, în ceea ce privește cererile de autorizare în conformitate cu alineatul (3), precum și rezultatul cererilor respective.

(7) Comisia publică rapoarte anuale privind utilizarea sistemelor de identificare biometrică la distanță în timp real în spațiile accesibile publicului în scopul aplicării legii, pe baza datelor agregate din statele membre din cadrul rapoartelor anuale menționate la alineatul (6). Rapoartele anuale respective nu includ date operaționale sensibile ale activităților conexe de aplicare a legii.

(8) Prezentul articol nu afectează interdicțiile care se aplică în cazul în care o practică în materie de IA încalcă alte dispoziții din dreptul Uniunii.

Capitolul III

Sisteme de IA cu grad ridicat de risc

SECȚIUNEA 1

CLASIFICAREA SISTEMELOR DE IA CA PREZENTÂND UN RISC RIDICAT

Articolul 6

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

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

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

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

(2) Sistemele de IA menționate în anexa III sunt considerate, pe lângă sistemele de IA cu grad ridicat de risc menționate la alineatul (1), ca prezentând un grad ridicat de risc.

(3) Prin derogare de la alineatul (2), un sistem de IA menționat în anexa III nu poate fi considerat ca prezentând un grad ridicat de risc dacă nu prezintă un risc semnificativ de a aduce prejudicii sănătății, siguranței sau drepturilor fundamentale ale persoanelor fizice, inclusiv prin faptul că nu influențează în mod semnificativ rezultatul procesului decizional.

Primul paragraf se aplică în cazul în care oricare dintre următoarele condiții este îndeplinită:

(a) sistemul de IA este destinat să îndeplinească o sarcină procedurală restrânsă;

(b) sistemul de IA este destinat să îmbunătățească rezultatul unei activități umane finalizate anterior;

(c) sistemul de IA este destinat să depisteze modelele decizionale sau abaterile de la modelele decizionale anterioare și nu este menit să înlocuiască sau să influențeze evaluarea umană finalizată anterior, fără o revizuire umană adecvată; sau

(d) sistemul de IA este destinat să îndeplinească o sarcină pregătitoare pentru o evaluare relevantă în scopul cazurilor de utilizare enumerate în anexa III.

În pofida primului paragraf, un sistem de IA menționat în anexa III este întotdeauna considerat ca prezentând un grad ridicat de risc dacă creează profiluri ale persoanelor fizice.

(4) Orice furnizor care consideră că un sistem de IA menționat în anexa III nu prezintă un grad ridicat de risc documentează evaluarea sa înainte ca sistemul respectiv să fie introdus pe piață sau pus în funcțiune. Furnizorul respectiv este supus obligației de înregistrare prevăzute la articolul 49 alineatul (2). La cererea autorităților naționale competente, furnizorul pune la dispoziție dovezile documentare în sprijinul evaluării.

(5) După consultarea Comitetului european pentru inteligența artificială (denumit în continuare „comitetul”) și în termen de cel mult ... [18 luni de la data intrării în vigoare a prezentului regulament], Comisia furnizează orientări care precizează modalitățile privind punerea în aplicare practică a prezentului articol, în conformitate cu articolul 96, împreună cu o listă cuprinzătoare de exemple practice de cazuri de utilizare a sistemelor de IA care prezintă un grad ridicat de risc și a celor care nu prezintă un grad ridicat de risc.

(6) Comisia este împuternicită să adopte acte delegate în conformitate cu articolul 97 pentru a modifica alineatul (3) al doilea paragraf de la prezentul articol prin adăugarea de noi condiții față de cele prevăzute la dispoziția menționată sau prin modificarea acestora, în cazul în care există dovezi concrete și fiabile ale existenței unor sisteme de IA care intră în domeniul de aplicare al anexei III, dar care nu prezintă un risc semnificativ de a aduce prejudicii sănătății, siguranței sau drepturilor fundamentale ale persoanelor fizice.

(7) Comisia adoptă acte delegate în conformitate cu articolul 97 pentru a modifica alineatul (3) al doilea paragraf de la prezentul articol prin eliminarea oricăreia dintre condițiile prevăzute la dispoziția menționată, în cazul în care există dovezi concrete și fiabile că acest lucru este necesar în scopul menținerii nivelului de protecție a sănătății, a siguranței și a drepturilor fundamentale prevăzut în prezentul regulament.

(8) Orice modificare a condițiilor prevăzute la alineatul (3) al doilea paragraf, adoptată în conformitate cu alineatele (6) și (7) de la prezentul articol, nu reduce nivelul general de protecție a sănătății, a siguranței și a drepturilor fundamentale prevăzut în prezentul regulament și asigură corelarea cu actele delegate adoptate în temeiul articolului 7 alineatul (1) și ține seama de evoluțiile pieței și ale tehnologiei.

Articolul 7

Modificări ale anexei III

(1) Comisia este împuternicită să adopte acte delegate în conformitate cu articolul 97 pentru a modifica anexa III prin adăugarea de cazuri de utilizare a sistemelor de IA cu grad ridicat de risc sau prin modificarea unor astfel de cazuri dacă sunt îndeplinite cumulativ următoarele două condiții:

(a) sistemele de IA sunt destinate a fi utilizate în oricare dintre domeniile enumerate în anexa III;

(b) sistemele de IA prezintă un risc de a aduce prejudicii sănătății și siguranței sau un risc de impact negativ asupra drepturilor fundamentale, iar riscul respectiv este echivalent sau mai mare în raport cu 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 condiția prevăzută la alineatul (1) litera (b), 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) natura și volumul datelor prelucrate și utilizate de sistemul de IA, în special dacă sunt prelucrate categorii speciale de date cu caracter personal;

(d) măsura în care sistemul de IA acționează în mod autonom și posibilitatea ca o persoană să anuleze o decizie sau recomandări care atrag un potențial prejudiciu;

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

(f) 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 numeroase persoane sau de a afecta în mod disproporționat un anumit grup de persoane;

(g) măsura în care persoanele care sunt 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;

(h) măsura în care există un dezechilibru de putere sau persoanele care sunt potențial prejudiciate sau afectate de impactul negativ se află într-o poziție vulnerabilă în raport cu implementatorul unui sistem de IA, în special din cauza statutului, a autorității, a cunoștințelor, a circumstanțelor economice sau sociale sau a vârstei;

(i) măsura în care rezultatul produs cu implicarea unui sistem de IA este ușor de corectat sau reversibil, avându-se în vedere soluțiile tehnice disponibile pentru corectare sau reversare și dat fiind că rezultatele care au un impact negativ asupra sănătății, siguranței sau drepturilor fundamentale nu sunt considerate ca fiind ușor de corectat sau reversibile;

(j) amploarea și probabilitatea beneficiilor implementării sistemului de IA pentru persoane fizice, grupuri sau societate în general, inclusiv îmbunătățirile posibile ale siguranței produselor;

(k) măsura în care dreptul existent al 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.

(3) Comisia este împuternicită să adopte acte delegate în conformitate cu articolul 97 pentru a modifica lista din anexa III prin eliminarea de sisteme de IA cu grad ridicat de risc în cazul în care sunt îndeplinite cumulativ următoarele două condiții:

(a) sistemul 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.

SECȚIUNEA 2

CERINȚE PENTRU SISTEMELE DE IA CU GRAD RIDICAT DE RISC

Articolul 8

Respectarea cerințelor

(1) Sistemele de IA cu grad ridicat de risc respectă cerințele stabilite în prezenta secțiune, ținând seama de scopul lor preconizat, precum și de stadiul de avansare general recunoscut al IA și al tehnologiilor conexe IA. Sistemul de gestionare a riscurilor menționat la articolul 9 este luat în considerare atunci când se asigură respectarea cerințelor respective.

(2) În cazul în care un produs conține un sistem de IA căruia i se aplică cerințele prezentului regulament, precum și cerințele din legislația de armonizare a Uniunii care figurează în anexa I secțiunea A, furnizorii au responsabilitatea de a se asigura că produsul lor respectă pe deplin toate cerințele aplicabile impuse de legislația aplicabilă de armonizare a Uniunii. Pentru a asigura conformitatea sistemelor de IA cu grad ridicat de risc menționate la alineatul (1) cu cerințele prevăzute în prezenta secțiune și pentru a asigura coerența, a evita suprapunerile și a reduce la minimum sarcinile suplimentare, furnizorii au posibilitatea de a integra, după caz, procesele de testare și raportare necesare, informațiile și documentația pe care le furnizează cu privire la produsul lor în documentația și procedurile deja existente și sunt impuse în temeiul legislației de armonizare a Uniunii care figurează în anexa I secțiunea A.

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 derulat pe parcursul întregului ciclu de viață al unui sistem de IA cu grad ridicat de risc, necesitând în mod periodic actualizarea și revizuirea sistematică. Acesta cuprinde următoarele etape:

(a) identificarea și analiza riscurilor cunoscute și previzibile în mod rezonabil pe care sistemul de IA cu grad ridicat de risc le poate prezenta pentru sănătate, siguranță sau drepturile fundamentale atunci când sistemul de IA cu grad ridicat de risc este utilizat în conformitate cu scopul preconizat;

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

(c) evaluarea altor riscuri care ar putea apărea pe baza analizei datelor colectate din sistemul de monitorizare ulterioară introducerii pe piață menționat la articolul 72;

(d) adoptarea unor măsuri adecvate și specifice de gestionare a riscurilor, concepute pentru a combate riscurile identificate în temeiul literei (a).

(3) Prezentul articol 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.

(4) 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 prezenta secțiune, 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.

(5) Măsurile de gestionare a riscurilor menționate la alineatul (2) litera (d) sunt de așa natură încât riscul rezidual relevant asociat fiecărui pericol, precum și riscul rezidual global al sistemelor de IA cu grad ridicat de risc să fie considerate a fi 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), în măsura în care acest lucru este fezabil din punct de vedere tehnic 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 pentru combaterea riscurilor care nu pot fi eliminate;

(c) furnizarea informațiilor necesare în temeiul articolului 13 și, după caz, formarea implementatorilor.

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 și formării preconizate din partea implementatorului, precum și contextului prezumtiv în care urmează să fie utilizat sistemul.

(6) Sistemele de IA cu grad ridicat de risc sunt testate în scopul identificării celor mai adecvate măsuri specifice de gestionare a riscurilor. Testarea asigură faptul că sistemele de IA cu grad ridicat de risc funcționează într-un mod coerent cu scopul preconizat și că sunt conforme cu cerințele stabilite în prezenta secțiune.

(7) Procedurile de testare pot include testarea în condiții reale, în conformitate cu articolul 60.

(8) 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 a acestora. 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.

(9) La punerea în aplicare a sistemului de gestionare a riscurilor descris la alineatele (1)-(7), furnizorii analizează dacă, având în vedere scopul său preconizat, sistemul de IA cu grad ridicat de risc este susceptibil să aibă un impact negativ asupra persoanelor cu vârsta sub 18 ani și, după caz, asupra altor grupuri vulnerabile.

(10) 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 altor dispoziții relevante din dreptul Uniunii, aspectele descrise la alineatele (1)-(9) pot face parte din procedurile de gestionare a riscurilor stabilite în temeiul legislației respective sau pot fi combinate cu acestea.

Articolul 10

Datele și guvernanța datelor

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

(2) Seturile de date de antrenament, de validare și de testare fac obiectul unor practici de guvernanță și gestionare a datelor adecvate scopului preconizat al sistemului de IA cu grad ridicat de risc. Practicile respective se referă în special la:

(a) opțiunile de proiectare relevante;

(b) procesele de colectare a datelor și originea datelor, iar în cazul datelor cu caracter personal, scopul inițial al colectării datelor;

(c) operațiunile relevante de prelucrare în vederea pregătirii datelor, cum ar fi adnotarea, etichetarea, curățarea, actualizarea, îmbogățirea și agregarea;

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

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

(f) examinarea în vederea identificării unor posibile prejudecăți care sunt susceptibile să afecteze sănătatea și siguranța persoanelor, să aibă un impact negativ asupra drepturilor fundamentale sau să conducă la o discriminare interzisă în temeiul dreptului Uniunii, în special în cazul în care datele de ieșire influențează datele de intrare pentru operațiunile viitoare;

(g) măsuri adecvate pentru detectarea, prevenirea și atenuarea posibilelor prejudecăți identificate în conformitate cu litera (f);

(h) identificarea lacunelor sau a deficiențelor relevante în materie de date care împiedică conformitatea cu prezentul regulament și a modului în care acestea pot fi abordate.

(3) Seturile de date de antrenament, de validare și de testare sunt relevante, suficient de reprezentative, și pe cât posibil, fără erori și complete, având în vedere scopul preconizat. 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. Caracteristicile respective ale seturilor de date pot fi îndeplinite la nivelul seturilor de date individuale sau la nivelul unei combinații a acestora.

(4) Seturile de date iau în considerare, în măsura impusă de scopul preconizat, caracteristicile sau elementele specifice cadrului geografic, contextual, 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 detectarea și corectarea prejudecăților în legătură cu sistemele de IA cu grad ridicat de risc în conformitate cu alineatul (2) literele (f) și (g) de la prezentul articol, furnizorii de astfel de sisteme pot prelucra în mod excepțional categoriile speciale de date cu caracter personal, sub rezerva unor garanții adecvate pentru drepturile și libertățile fundamentale ale persoanelor fizice. În plus față de dispozițiile prevăzute de Regulamentele (UE) 2016/679 și (UE) 2018/1725 și de Directiva (UE) 2016/680, pentru ca o astfel de prelucrare să aibă loc, trebuie să fie respectate toate condițiile următoare:

(a) depistarea și corectarea prejudecăților nu poate fi realizată în mod eficace prin prelucrarea altor date, inclusiv a datelor sintetice sau anonimizate;

(b) categoriile speciale de date cu caracter personal fac obiectul unor limitări tehnice privind reutilizarea datelor cu caracter personal și al unor măsuri avansate de securitate și de protecție a vieții private, inclusiv pseudonimizarea;

(c) categoriile speciale de date cu caracter personal fac obiectul unor măsuri prin care să se asigure că datele cu caracter personal prelucrate sunt securizate și protejate, sub rezerva unor garanții adecvate, inclusiv controale stricte și documentarea accesului, pentru a se evita utilizarea necorespunzătoare și pentru a se asigura că numai persoanele autorizate cu obligații de confidențialitate corespunzătoare au acces la aceste date cu caracter personal;

(d) categoriile speciale de date cu caracter personal nu trebuie să fie transmise, transferate sau accesate în alt mod de către alte părți;

(e) categoriile speciale de date cu caracter personal sunt șterse după corectarea prejudecăților sau după ce datele cu caracter personal au ajuns la sfârșitul perioadei lor de păstrare, în funcție de care dintre acestea survine mai întâi;

(f) evidențele activităților de prelucrare în temeiul Regulamentelor (UE) 2016/679 și (UE) 2018/1725 și al Directivei (UE) 2016/680 includ motivele pentru care a fost strict necesară prelucrarea unor categorii speciale de date cu caracter personal pentru a depista și a corecta prejudecățile și motivele pentru care acest obiectiv nu putea fi realizat prin prelucrarea altor date.

(6) Pentru dezvoltarea sistemelor de IA cu grad ridicat de risc care nu utilizează tehnici care implică antrenarea de modele de IA, 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 prezenta secțiune și să furnizeze autorităților naționale competente și organismelor notificate 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. IMM-urile, inclusiv întreprinderile nou-înființate, pot furniza într-o manieră simplificată elementele documentației tehnice specificate în anexa IV. În acest scop, Comisia stabilește un formular simplificat de documentație tehnică care vizează nevoile întreprinderilor mici și ale microîntreprinderilor. În cazul în care IMM-urile, inclusiv întreprinderile nou-înființate, optează să furnizeze informațiile solicitate în anexa IV într-o manieră simplificată, acestea utilizează formularul menționat la prezentul alineat. Organismele notificate acceptă formularul în scopul evaluării conformității.

(2) În cazul în care este introdus pe piață sau pus în funcțiune un sistem de IA cu grad ridicat de risc legat de un produs care face obiectul actelor legislative de armonizare ale Uniunii care figurează în anexa I secțiunea A, se întocmește o singură documentație tehnică ce conține toate informațiile prevăzute la alineatul (1), precum și informațiile necesare în temeiul respectivelor acte juridice.

(3) Comisia este împuternicită să adopte acte delegate în conformitate cu articolul 97 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 prezenta secțiune.

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) de-a lungul duratei de viață a sistemului.

(2) Pentru a asigura un nivel de trasabilitate a funcționării sistemului de IA cu grad ridicat de risc care să fie adecvat scopului preconizat al sistemului, capabilitățile de jurnalizare permit înregistrarea evenimentelor relevante pentru:

(a) identificarea situațiilor care pot avea ca rezultat faptul că sistemul de IA cu grad ridicat de risc prezintă un risc în sensul articolului 79 alineatul (1) sau care pot conduce la o modificare substanțială;

(b) facilitarea monitorizării ulterioare introducerii pe piață menționate la articolul 72; și

(c) monitorizarea funcționării sistemelor de IA cu grad ridicat de risc menționate la articolul 26 alineatul (5).

(3) În cazul sistemelor de IA cu grad ridicat de risc menționate în anexa III punctul 1 litera (a), capabilitățile de jurnalizare furnizează 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 în raport 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 implementatorilor

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

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

(3) Instrucțiunile de utilizare conțin cel puțin următoarele informații:

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

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

(i) scopul său preconizat;

(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 său preconizat sau în condiții de utilizare necorespunzătoare previzibilă în mod rezonabil, care poate conduce la riscurile pentru sănătate și siguranță sau pentru drepturile fundamentale menționate la articolul 9 alineatul (2);

(iv) după caz, capabilitățile și caracteristicile tehnice ale sistemului de IA cu grad ridicat de risc de a furniza informații relevante pentru explicarea rezultatelor sale;

(v) după caz, performanțele sale în ceea ce privește anumite persoane sau grupuri de persoane în legătură cu care este destinat să fie utilizat sistemul;

(vi) 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 cu grad ridicat de risc;

(vii) după caz, informații care să le permită implementatorilor să interpreteze rezultatele sistemului de IA cu grad ridicat de risc și să le utilizeze în mod corespunzător;

(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 cu grad ridicat de risc de către implementatori;

(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) după caz, o descriere a mecanismelor incluse în sistemul de IA cu grad ridicat de risc care să permită implementatorilor să colecteze, să stocheze și să interpreteze în mod corespunzător fișierele de jurnalizare în conformitate cu articolul 12.

Articolul 14

Supravegherea umană

(1) Sistemele de IA cu grad ridicat de risc sunt proiectate și dezvoltate astfel încât, prin includerea de instrumente adecvate de interfață om-mașină, să poată fi supravegheate în mod eficace de către persoane fizice în perioada în care sunt utilizate.

(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 previzibilă în mod rezonabil, în special în cazurile în care astfel de riscuri persistă în pofida aplicării altor cerințe prevăzute în prezenta secțiune.

(3) Măsurile de supraveghere sunt proporționale cu riscurile specifice, cu nivelul de autonomie și cu contextul utilizării sistemului de IA cu grad ridicat de risc și se asigură fie prin unul dintre următoarele tipuri de măsuri, fie prin ambele:

(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 implementator.

(4) În scopul punerii în aplicare a alineatelor (1), (2) și (3), sistemul de IA cu grad ridicat de risc este pus la dispoziția implementatorului astfel încât persoanelor fizice cărora li se încredințează supravegherea umană să li se permită, în funcție de următoarele și proporțional cu acestea:

(a) să înțeleagă în mod corespunzător capacitățile și limitările relevante ale sistemului de IA cu grad ridicat de risc și să fie în măsură să monitorizeze în mod corespunzător funcționarea acestuia, inclusiv în vederea depistării și abordării anomaliilor, disfuncționalităților și performanțelor neașteptate;

(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 (prejudecăți legate de automatizare), în special în cazul sistemelor de IA cu grad ridicat de risc utilizate pentru a furniza informații sau recomandări pentru deciziile care urmează să fie luate de persoanele fizice;

(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 anume, 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 care să permită sistemului să se oprească în condiții de siguranță.

(5) În cazul sistemelor de IA cu grad ridicat de risc menționate în anexa III punctul 1 litera (a), măsurile menționate la alineatul (3) de la prezentul articol sunt de așa natură încât să asigure că, în plus, implementatorul nu ia nicio măsură sau decizie pe baza identificării care rezultă din sistem, cu excepția cazului în care identificarea respectivă a fost verificată și confirmată separat de cel puțin două persoane fizice care au competența, pregătirea și autoritatea necesare.

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 aplicării legii sau în domeniul imigrației, al controlului la frontiere ori 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 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) Pentru a aborda aspectele tehnice ale modului de măsurare a nivelurilor adecvate de acuratețe și robustețe prevăzute la alineatul (1) și orice alți indicatori de performanță relevanți, Comisia, în cooperare cu părți interesate și organizații relevante precum autoritățile din domeniul metrologiei și al etalonării încurajează, după caz, elaborarea de valori de referință și metodologii de măsurare.

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

(4) Sistemele de IA cu grad ridicat de risc sunt cât mai reziliente posibil 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. Se iau măsuri tehnice și organizatorice în acest sens.

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

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 ca eventuale rezultate distorsionate de prejudecăți să influențeze datele de intrare pentru operațiunile viitoare (bucle de feedback) și să se asigure că orice astfel de bucle de feedback sunt abordate în mod corespunzător prin măsuri de atenuare adecvate.

(5) Sistemele de IA cu grad ridicat de risc sunt reziliente în ceea ce privește încercările unor părți terțe neautorizate de a le modifica utilizarea, rezultatele 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 relevante și riscurilor.

Soluțiile tehnice pentru abordarea vulnerabilităților specifice ale IA includ, după caz, măsuri de prevenire, depistare, răspuns, soluționare și control în privința atacurilor ce vizează manipularea setului de date de antrenament (otrăvirea datelor) sau a componentelor preantrenate utilizate la antrenament (otrăvirea modelelor), a datelor de intrare concepute să determine modelul de IA să facă o greșeală (exemple contradictorii sau eludarea modelelor), a atacurilor la adresa confidențialității sau a defectelor modelului.

SECȚIUNEA 3

OBLIGAȚIILE FURNIZORILOR ȘI IMPLEMENTATORILOR 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 secțiunea 2;

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

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

(d) păstrează documentația menționată la articolul 18;

(e) atunci când acestea se află sub controlul lor, păstrează fișierele de jurnalizare generate automat de sistemele lor de IA cu grad ridicat de risc menționate la articolul 19;

(f) 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;

(g) elaborează o declarație de conformitate UE în conformitate cu articolul 47;

(h) aplică marcajul CE pe sistemul de IA cu grad ridicat de risc sau, în cazul în care acest lucru nu este posibil, pe ambalajul sau în documentația sa însoțitoare, pentru a indica conformitatea cu prezentul regulament, în conformitate cu articolul 48;

(i) respectă obligațiile de înregistrare menționate la articolul 49 alineatul (1);

(j) iau măsurile corective necesare și furnizează informațiile prevăzute la articolul 20;

(k) la cererea motivată a unei autorități naționale competente, demonstrează conformitatea sistemului de IA cu grad ridicat de risc cu cerințele prevăzute în secțiunea 2;

(l) se asigură că sistemul de IA cu grad ridicat de risc respectă cerințele de accesibilitate, în conformitate cu Directivele (UE) 2016/2102 și (UE) 2019/882.

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 trebuie utilizate pentru proiectarea, controlul proiectării și verificarea proiectării sistemului de IA cu grad ridicat de risc;

(c) tehnicile, procedurile și acțiunile sistematice care trebuie 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 trebuie aplicate și, în cazul în care standardele armonizate relevante nu sunt aplicate integral sau nu vizează toate cerințele relevante prevăzute în secțiunea 2, mijloacele care trebuie utilizate pentru a se asigura că sistemul de IA cu grad ridicat de risc respectă cerințele respective;

(f) sisteme și proceduri pentru gestionarea datelor, inclusiv obținerea datelor, 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) instituirea, implementarea și întreținerea unui sistem de monitorizare ulterioară introducerii pe piață, în conformitate cu articolul 72;

(i) procedurile legate de raportarea unui incident grav în conformitate cu articolul 73;

(j) gestionarea comunicării cu autoritățile naționale competente, cu alte autorități relevante, inclusiv cu cele 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. Furnizorii respectă, indiferent de situație, gradul de precizie și nivelul de protecție necesare pentru a asigura conformitatea cu prezentul regulament a sistemelor lor de IA cu grad ridicat de risc.

(3) Furnizorii de sisteme de IA cu grad ridicat de risc care fac obiectul unor obligații în ceea ce privește sistemele de management al calității sau o funcție echivalentă a acestora în temeiul dreptului sectorial relevant al Uniunii pot include aspectele descrise la alineatul (1) ca parte din sistemele de management al calității stabilite în temeiul dreptului respectiv.

(4) În cazul furnizorilor care sunt instituții financiare supuse unor cerințe privind guvernanța internă, măsurile sau procesele interne în temeiul dreptului Uniunii din domeniul serviciilor financiare, se consideră că obligația de instituire a unui sistem de management al calității, cu excepția alineatului (1) literele (g), (h) și (i) de la prezentul articol, este îndeplinită prin respectarea normelor privind măsurile sau procesele de guvernanță internă în temeiul dreptului relevant al Uniunii din domeniul serviciilor financiare. În acest scop, se ține seama de toate standardele armonizate menționate la articolul 40.

Articolul 18

Păstrarea evidențelor

(1) Pentru o perioadă de 10 ani după introducerea pe piață sau punerea în funcțiune a sistemului de IA cu grad ridicat de risc, furnizorul păstrează 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 47.

(2) 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.

(3) Furnizorii care sunt instituții financiare supuse unor cerințe privind guvernanța internă, măsurile sau procesele lor interne în temeiul dreptului Uniunii din domeniul serviciilor financiare păstrează documentația tehnică ca parte a documentației păstrate în temeiul dreptului relevant al Uniunii din domeniul serviciilor financiare.

Articolul 19

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 de IA cu grad ridicat de risc ale acestora, în măsura în care astfel de fișiere de jurnalizare se află sub controlul lor. Fără a aduce atingere dreptului Uniunii sau dreptului intern aplicabil, fișiere de jurnalizare se păstrează pentru o perioadă adecvată scopului preconizat al sistemului de IA cu grad ridicat de risc, 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 lor internă, măsurile sau procesele lor interne în temeiul dreptului Uniunii din domeniul serviciilor financiare păstrează fișierele de jurnalizare generate automat de sistemele lor de IA cu grad ridicat de risc ca parte a documentației păstrate în temeiul dreptului relevant din domeniul serviciilor financiare.

Articolul 20

Măsuri corective și obligația de informare

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

(2) În cazul în care sistemul de IA cu grad ridicat de risc prezintă un risc în sensul articolului 79 alineatul (1), iar furnizorul ia cunoștință de riscul respectiv, acesta investighează imediat cauzele, în colaborare cu implementatorul care efectuează raportarea, după caz, și informează autoritățile de supraveghere a pieței competente pentru sistemul de IA cu grad ridicat de risc în cauză și, după caz, organismul notificat care a eliberat un certificat pentru sistemul de IA cu grad ridicat de risc respectiv în conformitate cu articolul 44, în special cu privire la natura neconformității și la orice măsură corectivă relevantă întreprinsă.

Articolul 21

Cooperarea cu autoritățile competente

(1) La cererea motivată a unei autorități competente, furnizorii de sisteme de IA cu grad ridicat de risc furnizează autorității respective toate informațiile și documentația necesare pentru a demonstra conformitatea sistemului de IA cu grad ridicat de risc cu cerințele prevăzute în secțiunea 2, într-o limbă care poate fi ușor înțeleasă de către autoritatea respectivă și care este una dintre limbile oficiale ale instituțiilor Uniunii, astfel cum sunt indicate de statul membru în cauză.

(2) La cererea motivată a unei autorități competente, furnizorii acordă, de asemenea, autorității competente solicitante, după caz, acces la fișierele de jurnalizare generate automat ale sistemului de IA cu grad ridicat de risc menționate la articolul 12 alineatul (1), în măsura în care respectivele fișiere de jurnalizare se află sub controlul lor.

(3) Toate informațiile obținute de autoritățile competente în temeiul prezentului articol sunt tratate în conformitate cu obligațiile de confidențialitate prevăzute la articolul 78.

Articolul 22

Reprezentanții autorizați ai furnizorilor de sisteme de IA cu grad ridicat de risc

(1) Înainte de a-și pune la dispoziție sistemele de IA cu grad ridicat de risc pe piața Uniunii, furnizorii stabiliți în țări terțe desemnează, prin mandat scris, un reprezentant autorizat care este stabilit în Uniune.

(2) Furnizorul permite reprezentantului său autorizat să îndeplinească sarcinile prevăzute în mandatul primit de la furnizor.

(3) Reprezentantul autorizat îndeplinește sarcinile prevăzute în mandatul primit de la furnizor. Acesta furnizează autorităților de supraveghere a pieței, la cerere, o copie a mandatului, într-una din limbile oficiale ale instituțiilor Uniunii, astfel cum este indicată de autoritatea competentă. În sensul prezentului regulament, mandatul îl autorizează pe reprezentantul autorizat să îndeplinească următoarele sarcini:

(a) să verifice dacă au fost întocmite declarația de conformitate UE menționată la articolul 47 și documentația tehnică menționată la articolul 11 și dacă furnizorul a desfășurat o procedură corespunzătoare de evaluare a conformității;

(b) să păstreze la dispoziția autorităților competente și a autorităților sau organismelor naționale menționate la articolul 74 alineatul (10), 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 care a desemnat reprezentantul autorizat, o copie a declarației de conformitate UE menționată la articolul 47, documentația tehnică și, dacă este cazul, certificatul eliberat de organismul notificat;

(c) să furnizeze unei autorități competente, pe baza unei cereri motivate, toate informațiile și documentația, inclusiv cele menționate la litera (b) de la prezentul paragraf, necesare pentru a demonstra conformitatea unui sistem de IA cu grad ridicat de risc cu cerințele prevăzute în secțiunea 2, inclusiv accesul la fișierele de jurnalizare, astfel cum sunt 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;

(d) să coopereze cu autoritățile competente, în urma unei cereri motivate, cu privire la orice acțiune întreprinsă de acestea din urmă în legătură cu sistemul de IA cu grad ridicat de risc, în special pentru a reduce și a atenua riscurile prezentate de sistemul de IA cu grad ridicat de risc;

(e) după caz, să respecte obligațiile de înregistrare menționate la articolul 49 alineatul (1) sau, dacă înregistrarea este efectuată chiar de furnizor, să se asigure că informațiile menționate la secțiunea A punctul 3 din anexa VIII sunt corecte.

Mandatul împuternicește reprezentantul autorizat să fie contactat, în afara sau în locul furnizorului, de către autoritățile competente, cu referire la toate aspectele legate de asigurarea conformității cu prezentul regulament.

(4) Reprezentantul autorizat își reziliază mandatul dacă consideră sau are motive să considere că furnizorul acționează contrar obligațiilor care îi revin în temeiul prezentului regulament. Într-un astfel de caz, el informează imediat autoritatea relevantă de supraveghere a pieței, precum și, după caz, organismul notificat relevant, cu privire la rezilierea mandatului și la motivele acesteia.

Articolul 23

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 sistemul este în conformitate cu prezentul regulament, verificând dacă:

(a) procedura relevantă de evaluare a conformității menționată la articolul 43 a fost efectuată de furnizorul sistemului de IA cu grad ridicat de risc;

(b) furnizorul a întocmit documentația tehnică în conformitate cu articolul 11 și cu anexa IV;

(c) sistemul poartă marcajul CE necesar și este însoțit de declarația de conformitate UE menționată la articolul 47 și de instrucțiunile de utilizare;

(d) furnizorul a desemnat un reprezentant autorizat în conformitate cu articolul 22 alineatul (1).

(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 ori însoțit de o documentație falsificată, acesta nu introduce sistemul respectiv pe piață înainte de a fi adus în conformitate. În cazul în care sistemul de IA cu grad ridicat de risc prezintă un risc în sensul articolului 79 alineatul (1), importatorul informează în acest sens furnizorul sistemului, reprezentanții autorizați și autoritățile de supraveghere a pieței.

(3) Importatorii indică numele lor, denumirea lor comercială înregistrată sau marca lor înregistrată și adresa la care pot fi contactați în privința sistemului de IA cu grad ridicat de risc și pe ambalajul acestuia sau în documentele care îl însoțesc, dacă este cazul.

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

(5) Importatorii păstrează, timp de 10 ani de la introducerea pe piață sau punerea în funcțiune a sistemului de IA cu grad ridicat de risc, o copie a certificatului eliberat de organismul notificat, după caz, a instrucțiunilor de utilizare și a declarației de conformitate UE menționată la articolul 47.

(6) Importatorii furnizează autorităților competente relevante, pe baza unei cereri motivate, toate informațiile și documentația necesare, inclusiv cele menționate la alineatul (5), pentru a demonstra conformitatea unui sistem de IA cu grad ridicat de risc cu cerințele prevăzute în secțiunea 2, într-o limbă care poate fi ușor înțeleasă de acestea. În acest scop, aceștia se asigură, de asemenea, că documentația tehnică poate fi pusă la dispoziția autorităților respective.

(7) Importatorii cooperează cu autoritățile competente relevante cu privire la orice acțiune întreprinsă de autoritățile respective în legătură cu un sistem de IA cu grad ridicat de risc introdus pe piață de importatori, în special pentru a reduce sau a atenua riscurile prezentate de acesta.

Articolul 24

Obligațiile distribuitorilor

(1) Înainte de a pune la dispoziție pe piață un sistem de IA cu grad ridicat de risc, distribuitorii verifică dacă acesta poartă marcajul CE necesar, dacă este însoțit de o copie a declarației de conformitate UE menționată la articolul 47 și de instrucțiunile de utilizare și dacă furnizorul și importatorul sistemului respectiv, după caz, au respectat obligațiile lor respective prevăzute la articolul 16 literele (b) și (c) și la articolul 23 alineatul (3).

(2) În cazul în care un distribuitor consideră sau are motive să considere, pe baza informațiilor pe care le deține, că un sistem de IA cu grad ridicat de risc nu este în conformitate cu cerințele prevăzute în secțiunea 2, acesta nu pune la dispoziție pe piață sistemul de IA cu grad ridicat de risc înainte ca sistemul să fie adus în conformitate cu cerințele respective. În plus, în cazul în care sistemul de IA cu grad ridicat de risc prezintă un risc în sensul articolului 79 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, condițiile de depozitare sau de transport, după caz, nu periclitează conformitatea sistemului cu cerințele prevăzute în secțiunea 2.

(4) Un distribuitor care consideră sau are motive să considere, pe baza informațiilor pe care le deține, 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 secțiunea 2 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 79 alineatul (1), distribuitorul informează imediat în acest sens furnizorul sau importatorul sistemului și autoritățile competente pentru sistemul de IA cu grad ridicat de risc în cauză, oferind informații detaliate, în special despre neconformitate și orice măsură corectivă întreprinsă.

(5) Pe baza unei cereri motivate a unei autorități competente relevante, distribuitorii unor sisteme de IA cu grad ridicat de risc furnizează autorității respective toate informațiile și documentația referitoare la acțiunile lor în temeiul alineatelor (1)-(4), necesare pentru a demonstra conformitatea respectivelor sisteme cu grad ridicat de risc cu cerințele prevăzute în secțiunea 2.

(6) Distribuitorii cooperează cu autoritățile competente relevante cu privire la orice acțiune întreprinsă de autoritățile respective în legătură cu un sistem de IA cu grad ridicat de risc pus la dispoziție pe piață de distribuitori, în special pentru a reduce sau a atenua riscul prezentat de acesta.

Articolul 25

Responsabilitățile de-a lungul lanțului valoric al IA

(1) Se consideră că orice distribuitor, importator, implementator sau altă parte terță este furnizor al unui sistem de IA cu grad ridicat de risc în sensul prezentului regulament și este supus obligațiilor care îi 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 dispozițiilor contractuale care prevăd o repartizare diferită a obligațiilor;

(b) modifică substanțial un sistem de IA cu grad ridicat de risc care a fost deja introdus pe piață sau a fost deja pus în funcțiune, astfel încât acesta rămâne un sistem de IA cu grad ridicat de risc în temeiul articolului 6;

(c) modifică scopul preconizat al un sistem de IA, inclusiv al unui sistem IA de uz general, care nu a fost clasificat ca prezentând un grad ridicat de risc și a fost deja introdus pe piață sau pus în funcțiune, astfel încât sistemul de IA în cauză devine un sistem IA cu grad ridicat de risc în conformitate cu articolul 6.

(2) În cazul în care se produc circumstanțele menționate la alineatul (1), furnizorul care a introdus inițial pe piață sau a pus în funcțiune sistemul de IA nu mai este considerat furnizorul respectivului sistem de IA în sensul prezentului regulament. Acest furnizor inițial cooperează îndeaproape cu noii furnizori și pune la dispoziție informațiile necesare și oferă accesul tehnic și alte tipuri de asistență preconizate în mod rezonabil care sunt necesare pentru îndeplinirea obligațiilor prevăzute în prezentul regulament, în special în ceea ce privește respectarea cerințelor privind evaluarea conformității sistemelor de IA cu grad ridicat de risc. Prezentul alineat nu se aplică în cazurile în care furnizorul inițial a specificat în mod clar că sistemul său de IA nu trebuie transformat într-un sistem de IA cu grad ridicat de risc și, prin urmare, nu intră sub incidența obligației de a preda documentația.

(3) În cazul sistemelor de IA cu grad ridicat de risc care sunt componente de siguranță ale unor produse cărora li se aplică actele legislative de armonizare ale Uniunii care figurează în anexa I secțiunea A, fabricantul 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:

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

(b) 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.

(4) Furnizorul unui sistem de IA cu grad ridicat de risc și partea terță care furnizează un sistem de IA, instrumente, servicii, componente sau procese care sunt utilizate sau integrate într-un sistem de IA cu grad ridicat de risc specifică, printr-un acord scris, pe baza stadiului de avansare general recunoscut al tehnologiei, informațiile, capabilitățile, accesul tehnic și alte tipuri de asistență necesare pentru a permite furnizorului sistemului de IA cu grad ridicat de risc să respecte întru totul obligațiile prevăzute în prezentul regulament. Prezentul alineat nu se aplică terților care pun la dispoziția publicului instrumente, servicii, procese sau componente, în afara modelelor de IA de uz general, sub licență liberă și deschisă.

Oficiul pentru IA poate elabora și recomanda un model voluntar de clauze pentru contractele dintre furnizorii de sisteme de IA cu grad ridicat de risc și părțile terțe care furnizează instrumente, servicii, componente sau procese care sunt utilizate sau integrate în sistemele de IA cu grad ridicat de risc. Atunci când elaborează modelul voluntar de clauze, Oficiul pentru IA ia în considerare eventualele cerințe contractuale aplicabile în anumite sectoare sau situații economice. Modelul voluntar de clauze se publică și este disponibil gratuit într-un format electronic ușor de utilizat.

(5) Alineatele (2) și (3) nu aduc atingere necesității de a respecta și de a proteja drepturile de proprietate intelectuală și informațiile comerciale confidențiale sau secretele comerciale în conformitate cu dreptul Uniunii și cu dreptul intern.

Articolul 26

Obligațiile implementatorilor de sisteme de IA cu grad ridicat de risc

(1) Implementatorii sistemelor de IA cu grad ridicat de risc iau măsuri tehnice și organizatorice corespunzătoare pentru a oferi siguranța că utilizează astfel de sisteme în conformitate cu instrucțiunile de utilizare care însoțesc sistemele, în temeiul alineatelor (3) și (6).

(2) Implementatorii încredințează supravegherea umană unor persoane fizice care au competența, formarea și autoritatea necesare, precum și sprijinul necesar.

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

(4) Fără a aduce atingere alineatelor (1) și (2), în măsura în care exercită controlul asupra datelor de intrare, implementatorul se asigură că datele de intrare sunt relevante și suficient de reprezentative în raport cu scopul preconizat al sistemului de IA cu grad ridicat de risc.

(5) Implementatorii monitorizează funcționarea sistemului de IA cu grad ridicat de risc pe baza instrucțiunilor de utilizare și, atunci când este cazul, informează furnizorii în conformitate cu articolul 72. În cazul în care au motive să considere că utilizarea sistemului de IA cu grad ridicat de risc în conformitate cu instrucțiunile poate conduce la situația în care sistemul de IA respectiv prezintă un risc în sensul articolului 79 alineatul (1), implementatorii informează fără întârzieri nejustificate furnizorul sau distribuitorul și autoritatea relevantă de supraveghere a pieței și suspendă utilizarea sistemului respectiv. De asemenea, în cazul în care au identificat un incident grav, implementatorii informează imediat mai întâi furnizorul, și apoi importatorul sau distribuitorul și autoritățile relevante de supraveghere a pieței cu privire la incidentul respectiv. În cazul în care implementatorul nu poate comunica cu furnizorul, articolul 73 se aplică mutatis mutandis. Această obligație nu vizează datele operaționale sensibile ale implementatorilor sistemelor de IA care sunt autorități de aplicare a legii.

În cazul implementatorilor care sunt instituții financiare supuse unor cerințe privind guvernanța internă, măsurile sau procesele interne în temeiul dreptului Uniunii din domeniul serviciilor 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 dreptului relevant din domeniul serviciilor financiare.

(6) Implementatorii sistemelor de IA cu grad ridicat de risc păstrează fișierele de jurnalizare generate automat de respectivele sisteme de IA cu grad ridicat de risc, în măsura în care aceste fișiere de jurnalizare se află sub controlul lor pentru o perioadă adecvată scopului preconizat al sistemului de IA cu grad ridicat de risc, 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.

Implementatorii care sunt instituții financiare supuse unor cerințe privind guvernanța internă, măsurile sau procesele interne în temeiul dreptului Uniunii din domeniul serviciilor financiare păstrează fișierele de jurnalizare ca parte a documentației păstrate în temeiul dreptului relevant al Uniunii din domeniul serviciilor financiare.

(7) Înainte de a pune în funcțiune sau de a utiliza un sistem de IA cu grad ridicat de risc la locul de muncă, implementatorii care sunt angajatori informează reprezentanții lucrătorilor și lucrătorii afectați că vor fi implicați în utilizarea sistemului de IA cu grad ridicat de risc. Informațiile respective sunt furnizate, după caz, în conformitate cu normele și procedurile prevăzute în dreptul și practicile de la nivelul Uniunii și de la nivel național privind informarea lucrătorilor și a reprezentanților acestora.

(8) Implementatorii sistemelor de IA cu grad ridicat de risc care sunt autorități publice sau instituții, organe, oficii sau agenții ale Uniunii respectă obligațiile de înregistrare menționate la articolul 49. În cazul în care constată că sistemul de IA cu grad ridicat de risc pe care intenționează să îl utilizeze nu a fost înregistrat în baza de date a UE menționată la articolul 71, implementatorii respectivi nu utilizează sistemul respectiv și informează furnizorul sau distribuitorul.

(9) După caz, implementatorii de sisteme de IA cu grad ridicat de risc utilizează informațiile furnizate în temeiul articolului 13 din prezentul regulament 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.

(10) Fără a aduce atingere Directivei (UE) 2016/680, în cadrul unei investigații pentru căutarea în mod specific a unei persoane suspectate sau condamnate de a fi comis o infracțiune, implementatorul unui sistem de IA cu grad ridicat de risc pentru identificarea biometrică la distanță ulterioară solicită o autorizație, *ex ante* sau fără întârzieri nejustificate și în termen de cel mult 48 de ore, din partea unei autorități judiciare sau a unei autorități administrative a cărei decizie are efect obligatoriu și face obiectul controlului jurisdicțional, pentru utilizarea sistemului respectiv, cu excepția cazului în care este utilizat pentru identificarea inițială a unui potențial suspect pe baza unor fapte obiective și verificabile legate direct de infracțiune. Fiecare utilizare se limitează la ceea ce este strict necesar pentru investigarea unei anumite infracțiuni.

În cazul în care autorizația solicitată în temeiul primului paragraf este respinsă, utilizarea sistemului de identificare biometrică la distanță ulterioară legat de autorizația solicitată respectivă se oprește cu efect imediat, iar datele cu caracter personal legate de utilizarea sistemului de IA cu grad ridicat de risc pentru care a fost solicitată autorizația se șterg.

În niciun caz, un astfel de sistem de IA cu grad ridicat de risc pentru identificarea biometrică la distanță ulterioară nu se utilizează într-un mod nedirecționat în scopul aplicării legii, dacă nu implică nicio legătură cu o infracțiune, cu o procedură penală, cu o amenințare reală și prezentă sau reală și previzibilă vizând o infracțiune sau căutarea unei anumite persoane dispărute. Se asigură faptul că autoritățile de aplicare a legii nu pot lua nicio decizie care produce un efect juridic negativ asupra unei persoane exclusiv pe baza rezultatelor unor astfel de sisteme de identificare biometrică la distanță ulterioară.

Prezentul alineat nu aduce atingere dispozițiilor de la articolul 9 din Regulamentul (UE) 2016/679 și de la articolul 10 din Directiva (UE) 2016/680 privind prelucrarea datelor biometrice.

Indiferent de scop sau de implementator, fiecare utilizare a acestor sisteme de IA cu grad ridicat de risc este documentată în dosarul relevant al poliției și este pusă la dispoziția autorității relevante de supraveghere a pieței și a autorității naționale pentru protecția datelor, la cerere, exceptând divulgarea datelor operaționale sensibile legate de aplicarea legii. Prezentul paragraf nu aduce atingere competențelor conferite autorităților de supraveghere de Directiva (UE) 2016/680.

Implementatorii prezintă autorităților relevante de supraveghere a pieței și autorităților naționale pentru protecția datelor rapoarte anuale cu privire la utilizarea sistemelor de identificare biometrică la distanță ulterioară, exceptând divulgarea datelor operaționale sensibile legate de aplicarea legii. Rapoartele pot fi agregate pentru a cuprinde mai multe implementări.

Statele membre pot introduce, în conformitate cu dreptul Uniunii, legi mai restrictive privind utilizarea sistemelor de identificare biometrică la distanță ulterioară.

(11) Fără a afecta dispozițiile de la articolul 50 din prezentul regulament, implementatorii de sisteme de IA cu grad ridicat de risc menționate în anexa III, care iau decizii sau contribuie la luarea deciziilor referitoare la persoane fizice, informează persoanele fizice că fac obiectul utilizării sistemului de IA cu grad ridicat de risc. În cazul sistemelor de IA cu grad ridicat de risc utilizate în scopul aplicării legii, se aplică articolul 13 din Directiva (UE) 2016/680.

(12) Implementatorii cooperează cu autoritățile competente relevante pentru orice acțiune întreprinsă de respectivele autorități în legătură cu sistemul de IA cu grad ridicat de risc pentru a pune în aplicare prezentul regulament.

Articolul 27

Evaluarea impactului sistemelor de IA cu grad ridicat de risc asupra drepturilor fundamentale

(1) Înainte de a implementa un sistem de IA cu grad ridicat de risc, astfel cum este menționat la articolul 6 alineatul (2), cu excepția sistemelor de IA cu grad ridicat de risc destinate a fi utilizate în domeniul menționat la punctul 2 din anexa III, implementatorii care sunt organisme de drept public sau entități private care furnizează servicii publice și implementatorii de sisteme de IA cu grad ridicat de risc menționate la punctul 5 literele (b) și (c) din anexa III efectuează o evaluare a impactului asupra drepturilor fundamentale pe care îl poate produce utilizarea unor astfel de sisteme. În acest scop, implementatorii efectuează o evaluare care constă în:

(a) o descriere a proceselor implementatorului în care sistemele de IA cu grad ridicat de risc urmează a fi utilizate în conformitate cu scopul lor preconizat;

(b) o descriere a perioadei de timp pentru care se intenționează utilizarea fiecărui sistem de IA cu grad ridicat de risc, precum și a frecvenței utilizării respective;

(c) categoriile de persoane fizice și grupurile susceptibile a fi afectate de utilizarea sa în contextul specific;

(d) riscurile specifice de prejudicii susceptibile a avea un impact asupra categoriilor de persoane fizice sau a grupurilor de persoane identificate în temeiul literei (c) de la prezentul alineat, ținând seama de informațiile comunicate de furnizor în temeiul articolului 13;

(e) o descriere a punerii în aplicare a măsurilor de supraveghere umană, în conformitate cu instrucțiunile de utilizare;

(f) măsurile care trebuie să fie luate în cazul în care riscurile respective se materializează, inclusiv mecanismele de guvernanță internă și mecanismele de tratare a plângerilor.

(2) Obligația prevăzută la alineatul (1) se aplică primei utilizări a sistemului de IA cu grad ridicat de risc. În cazuri similare, implementatorul poate să se bazeze pe evaluări ale impactului asupra drepturilor fundamentale efectuate anterior sau pe evaluări existente efectuate de furnizor. În cazul în care consideră că, în timpul utilizării sistemului de IA cu grad ridicat de risc, oricare dintre elementele enumerate la alineatul (1) s-a schimbat sau nu mai este actualizat, implementatorul ia măsurile necesare pentru a actualiza informațiile.

(3) După efectuarea evaluării menționate la alineatul (1) de la prezentul articol, implementatorul notifică autorității de supraveghere a pieței rezultatele sale, transmițând modelul completat menționat la alineatul (5) de la prezentul articol ca parte a notificării. În cazul menționat la articolul 46 alineatul (1), implementatorii pot fi scutiți de această obligație de notificare.

(4) În cazul în care oricare dintre obligațiile prevăzute la prezentul articol este deja respectată ca urmare a evaluării impactului asupra protecției datelor efectuate în temeiul articolului 35 din Regulamentul (UE) 2016/679 sau al articolului 27 din Directiva (UE) 2016/680, evaluarea impactului asupra drepturilor fundamentale menționată la alineatul (1) de la prezentul articol completează respectiva evaluare a impactului asupra protecției datelor.

(5) Oficiul pentru IA elaborează un model de chestionar, inclusiv prin intermediul unui instrument automatizat, pentru a-i ajuta pe implementatori să își respecte obligațiile care le revin în temeiul prezentului articol într-un mod simplificat.

SECȚIUNEA 4

AUTORITĂȚILE DE NOTIFICARE ȘI ORGANISMELE NOTIFICATE

Articolul 28

Autoritățile de notificare

(1) Fiecare stat membru desemnează sau instituie cel puțin o autoritate de notificare responsabilă cu instituirea și efectuarea procedurilor necesare pentru evaluarea, desemnarea și notificarea organismelor de evaluare a conformității și pentru monitorizarea acestora. Procedurile respective se elaborează în cooperare între autoritățile de notificare ale tuturor statelor membre.

(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 și organizate și funcționează 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 nici 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 pe care le obțin, în conformitate cu articolul 78.

(7) Autoritățile de notificare au la dispoziție un număr adecvat de membri competenți ai personalului în vederea îndeplinirii corespunzătoare a sarcinilor lor. Membrii competenți ai personalului dețin cunoștințele de specialitate necesare, după caz, pentru funcția pe care o îndeplinesc, în domenii precum tehnologiile informației, IA și drept, inclusiv supravegherea drepturilor fundamentale.

Articolul 29

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 tipurilor de sisteme 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 31.

Se adaugă orice document valabil referitor la desemnările existente ale organismului notificat solicitant în temeiul oricăror alte acte legislative de armonizare ale 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 31.

(4) În cazul organismelor notificate care sunt desemnate în temeiul oricăror alte acte legislative de armonizare ale 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) de la prezentul articol 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 31.

Articolul 30

Procedura de notificare

(1) Autoritățile de notificare pot notifica numai organismele de evaluare a conformității care îndeplinesc cerințele prevăzute la articolul 31.

(2) Autoritățile de notificare înștiințează Comisia și celelalte state membre prin intermediul instrumentului de notificare electronică dezvoltat și administrat de Comisie cu privire la fiecare organism de evaluare a conformității menționat la alineatul (1).

(3) Notificarea menționată la alineatul (2) de la prezentul articol include detalii complete privind activitățile de evaluare a conformității, modulul sau modulele de evaluare a conformității și tipurile de sisteme de IA în cauză, precum și atestarea relevantă a competenței. În cazul în care notificarea nu se bazează pe un certificat de acreditare menționat la articolul 29 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 31.

(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 29 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 29 alineatul (3).

(5) În cazul în care se ridică obiecții, Comisia inițiază fără întârziere consultații cu statele membre relevante și cu organismul de evaluare a conformității. În lumina acestora, Comisia decide dacă autorizația este justificată. Comisia comunică decizia luată statului membru în cauză și organismului relevant de evaluare a conformității.

Articolul 31

Cerințe cu privire la organismele notificate

(1) Un organism notificat este instituit în temeiul dreptului intern al unui stat membru și are personalitate juridică.

(2) Organismele notificate îndeplinesc cerințele organizatorice, de management al calității, de resurse și în materie de procese care sunt necesare pentru îndeplinirea sarcinilor lor, precum și cerințele adecvate în materie de securitate cibernetică.

(3) Structura organizațională, alocarea responsabilităților, liniile de raportare și funcționarea organismelor notificate asigură încrederea în performanța acestora 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 sistemele de IA cu grad ridicat de risc evaluate, precum și de orice concurent al furnizorului. Acest lucru nu împiedică utilizarea sistemelor de IA cu grad ridicat de risc evaluate care sunt necesare pentru operațiunile organismului de evaluare a conformității sau utilizarea sistemelor respective de IA cu grad ridicat de risc în scopuri personale.

(5) Nici organismul de evaluare a conformității, personalul său de conducere de nivel superior, nici personalul responsabil cu îndeplinirea sarcinilor acestuia de evaluare a conformității nu sunt direct implicați în proiectarea, dezvoltarea, comercializarea sau utilizarea sistemelor de IA cu grad ridicat de risc și nici nu reprezintă părțile implicate în respectivele activități. Aceștia nu se implică în nicio activitate susceptibilă de a le afecta imparțialitatea sau integritatea în ceea ce privește activitățile de evaluare a conformității pentru care sunt notificați. Această dispoziție se aplică în special serviciilor de consultanță.

(6) 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.

(7) Organismele notificate dispun de proceduri documentate care să asigure că personalul, comitetele, filialele, subcontractanții lor, precum și orice organism asociat sau membru al personalului organismelor externe respectă, în conformitate cu articolul 78, confidențialitatea informațiilor care le parvin în timpul derulării activităților de evaluare a conformității, cu excepția cazurilor în care divulgarea acestora este impusă 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.

(8) Organismele notificate dispun de proceduri pentru desfășurarea activităților, care să țină seama în mod corespunzător de dimensiunile unui furnizor, de sectorul în care acesta își desfășoară activitatea, de structura sa și de gradul de complexitate al sistemului de IA în cauză.

(9) 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 stabilite, în conformitate cu dreptul intern, sau în care însuși statul membru respectiv este direct responsabil pentru evaluarea conformității.

(10) Organismele notificate sunt capabile să își îndeplinească toate sarcinile în temeiul prezentului regulament cu cel mai înalt grad de integritate profesională și cu competența necesară în domeniul specific, indiferent dacă sarcinile respective sunt realizate de organismele notificate înseși sau în numele și pe răspunderea acestora.

(11) Organismele notificate dispun de suficiente competențe interne pentru a putea evalua în mod efectiv 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 tipurile relevante de sisteme de IA, de date și de calculul datelor, precum și în ceea ce privește cerințele prevăzute în secțiunea 2.

(12) 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.

Articolul 32

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 31, în măsura în care standardele armonizate aplicabile vizează aceste cerințe.

Articolul 33

Filiale ale organismelor notificate și subcontractare

(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 31 și informează autoritatea de notificare în acest sens.

(2) Organismele notificate preiau întreaga responsabilitate pentru sarcinile îndeplinite de orice subcontractant sau filială.

(3) Activitățile pot fi subcontractate sau îndeplinite de o filială doar cu acordul furnizorului. Organismele notificate pun la dispoziția publicului o listă a filialelor acestora.

(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 cinci ani de la data încetării subcontractării.

Articolul 34

Obligații operaționale ale organismelor notificate

(1) Organismele notificate verifică conformitatea sistemelor de IA cu grad ridicat de risc în conformitate cu procedurile de evaluare a conformității prevăzute la articolul 43.

(2) Organismele notificate evită sarcinile inutile pentru furnizori atunci când aceștia își desfășoară activitățile și țin seama în mod corespunzător de dimensiunile furnizorilor, de sectorul în care aceștia își desfășoară activitatea, de structura acestora și de gradul de complexitate al sistemului de IA cu grad ridicat de risc în cauză, în special în vederea reducerii la minimum a sarcinilor administrative și a costurilor de asigurare a conformității pentru microîntreprinderi și întreprinderile mici în sensul Recomandării 2003/361/CE. Organismul notificat respectă totuși gradul de precizie și nivelul de protecție impuse 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 28 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 prezenta secțiune.

Articolul 35

Numerele de identificare și listele organismelor notificate

(1) Comisia atribuie un număr unic de identificare fiecărui organism notificat, chiar și în cazul în care un organism este notificat în temeiul mai multor acte ale Uniunii.

(2) Comisia pune la dispoziția publicului lista organismelor notificate în temeiul prezentului regulament, incluzând numerele de identificare ale acestora 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 30 alineatul (2).

(2) Procedurile prevăzute la articolele 29 și 30 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 (3)-(9).

(3) 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 cel puțin un an înainte de încetarea activităților. Certificatele organismului notificat pot rămâne valabile pentru o perioadă 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 cu grad ridicat de risc care fac obiectul respectivelor certificate. Acest din urmă organism notificat efectuează o evaluare completă a sistemelor de IA cu grad ridicat de risc în cauză până la finalul respectivei perioade de nouă luni, înainte de emiterea de noi certificate pentru aceste sisteme. În cazul în care organismul notificat și-a încetat activitatea, autoritatea de notificare retrage desemnarea.

(4) În cazul în care o autoritate de notificare are motive suficiente să considere că un organism notificat nu mai îndeplinește cerințele prevăzute la articolul 31 sau că acesta nu își îndeplinește obligațiile, autoritatea de notificare respectivă investighează fără întârziere chestiunea, cu cea mai mare diligență. În acest context, aceasta informează organismul notificat în cauză cu privire la obiecțiile ridicate și îi oferă posibilitatea de a-și face cunoscute punctele de vedere. În cazul în care ajunge la concluzia că organismul notificat nu mai îndeplinește cerințele prevăzute la articolul 31 sau că nu își îndeplinește obligațiile, autoritatea de notificare restricționează, suspendă sau retrage desemnarea, 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.

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

(6) În caz de restricționare, suspendare sau retragere a unei desemnări, 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 de supravegherea pieței, la cererea acestora.

(7) 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 aduse desemnării;

(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 menținerea conformității sistemelor de IA cu grad ridicat de risc de 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; autoritățile respective iau măsurile corespunzătoare, acolo unde este necesar, pentru evitarea unui risc potențial pentru sănătate, siguranță sau drepturile fundamentale.

(8) Cu excepția certificatelor eliberate în mod necorespunzător și în cazul în care o desemnare a fost suspendată sau restricționată, certificatele rămân valabile în una dintre 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 pentru acțiunile de remediere a 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 capabilitatea de a continua să monitorizeze și să rămână responsabil de certificatele existente pe care le-a emis pe perioada suspendării sau a restricționării; în cazul în care autoritatea de notificare stabilește că organismul notificat nu are capabilitatea de a gestiona certificatele existente pe care le-a emis, furnizorul sistemului care face obiectul certificatului confirmă în scris autorităților naționale competente ale statului membru în care își are sediul social, în termen de trei luni de la suspendare sau restricționare, 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 restricționării.

(9) 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) autoritatea națională competentă din statul membru în care furnizorul sistemului de IA cu grad ridicat de risc care face obiectul certificatului își are sediul social a confirmat că nu există niciun risc pentru sănătate, siguranță sau drepturile fundamentale asociat sistemelor de IA cu grad ridicat de risc în cauză; și

(b) un alt organism notificat a confirmat în scris că își va asuma responsabilitatea imediat pentru respectivele sisteme de IA și își încheie evaluarea în termen de 12 luni de la retragerea desemnării.

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

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

Articolul 37

Contestarea competenței organismelor notificate

(1) Dacă este necesar, Comisia investighează toate cazurile în care există motive de îndoială cu privire la competența unui organism notificat sau la îndeplinirea în continuare de către un organism notificat a cerințelor prevăzute la articolul 31 și a responsabilităților sale aplicabile.

(2) Autoritatea de notificare furnizează Comisiei, la cerere, toate informațiile relevante referitoare la notificarea sau menținerea competenței organismului notificat în cauză.

(3) Comisia se asigură că toate informațiile sensibile obținute în cursul investigațiilor sale în temeiul prezentului articol sunt tratate în mod confidențial în conformitate cu articolul 78.

(4) În cazul în care constată că un organism notificat nu îndeplinește sau nu mai îndeplinește cerințele pentru a fi notificat, Comisia informează statul membru notificator în consecință și îi solicită acestuia să ia măsurile corective necesare, inclusiv suspendarea sau retragerea notificării, dacă este necesar. În cazul în care statul membru nu ia măsurile corective necesare, Comisia poate, prin intermediul unui act de punere în aplicare, să suspende, să restricționeze sau să retragă desemnarea. Actul de punere în aplicare respectiv se adoptă în conformitate cu procedura de examinare menționată la articolul 98 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) Fiecare autoritate de notificare se asigură că organismele notificate de aceasta participă la activitatea unui grup menționat la alineatul (1), în mod direct sau prin intermediul unor reprezentanți desemnați.

(3) Comisia se ocupă de organizarea unor schimburi de cunoștințe și bune practici între autoritățile de notificare.

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 31 sau să asigure un nivel de conformitate echivalent.

SECȚIUNEA 5

STANDARDE, EVALUAREA CONFORMITĂȚII, CERTIFICATE, ÎNREGISTRARE

Articolul 40

Standarde armonizate și documente de standardizare

(1) Sistemele de IA cu grad ridicat de risc sau modelele 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* în conformitate cu Regulamentul (UE) nr. 1025/2012, sunt considerate a fi în conformitate cu cerințele stabilite în secțiunea 2 din prezentul capitol sau, după caz, cu obligațiile prevăzute în capitolul V secțiunile 2 și 3 din prezentul regulament, în măsura în care standardele respective vizează cerințele sau obligațiile respective.

(2) În conformitate cu articolul 10 din Regulamentul (UE) nr. 1025/2012, Comisia emite, fără întârzieri nejustificate, solicitări de standardizare care vizează toate cerințele prevăzute în secțiunea 2 din prezentul capitol și, după caz, solicitări de standardizare care vizează obligațiile prevăzute în capitolul V secțiunile 2 și 3 din prezentul regulament. De asemenea, în cadrul solicitărilor de standardizare se cere furnizarea de documente privind procesele de raportare și documentare pentru a îmbunătăți performanța în materie de resurse a sistemelor de IA, cum ar fi reducerea consumului de energie și de alte resurse pentru sistemul de IA cu grad ridicat de risc pe parcursul ciclului său de viață, precum și privind dezvoltarea eficientă din punct de vedere energetic a modelelor de IA de uz general. Atunci când elaborează o solicitare de standardizare, Comisia consultă comitetul și părțile interesate relevante, inclusiv forumul consultativ.

Atunci când adresează o solicitare de standardizare organizațiilor de standardizare europene, Comisia precizează că standardele trebuie să fie clare și coerente inclusiv cu standardele elaborate în diferitele sectoare pentru produsele care fac obiectul legislației existente de armonizare a Uniunii care figurează în anexa I, având drept scop să asigure faptul că sistemele de IA cu grad ridicat de risc sau modelele de IA de uz general introduse pe piață sau puse în funcțiune în Uniune îndeplinesc cerințele sau obligațiile relevante prevăzute în prezentul regulament.

Comisia solicită organizațiilor de standardizare europene să furnizeze dovezi ale tuturor eforturilor depuse pentru a îndeplini obiectivele menționate la primul și al doilea paragraf de la prezentul alineat, în conformitate cu articolul 24 din Regulamentul (UE) nr. 1025/2012.

(3) Participanții la procesul de standardizare urmăresc să promoveze investițiile și inovarea în IA, inclusiv prin sporirea securității juridice, precum și competitivitatea și creșterea pieței Uniunii, să contribuie la consolidarea cooperării la nivel mondial în materie de standardizare, ținând seama de standardele internaționale existente în domeniul IA care sunt în concordanță cu valorile, drepturile fundamentale și interesele Uniunii, și să consolideze guvernanța multipartită, asigurând o reprezentare echilibrată a intereselor și participarea efectivă a tuturor părților interesate relevante, în conformitate cu articolele 5, 6 și 7 din Regulamentul (UE) nr. 1025/2012.

Articolul 41

Specificații comune

(1) Comisia poate să adopte acte de punere în aplicare de stabilire a specificațiilor comune pentru cerințele prevăzute în secțiunea 2 din prezentul capitol sau, după caz, pentru obligațiile prevăzute în secțiunile 2 și 3 din capitolul V, în cazul în care sunt îndeplinite următoarele condiții:

(a) Comisia a solicitat, în temeiul articolului 10 alineatul (1) din Regulamentul (UE) nr. 1025/2012, uneia sau mai multor organizații de standardizare europene să elaboreze un standard armonizat pentru cerințele prevăzute în secțiunea 2 din prezentul capitol sau, după caz, pentru obligațiile prevăzute în secțiunile 2 și 3 din capitolul V, și:

(i) solicitarea nu a fost acceptată de niciuna dintre organizațiile de standardizare europene; sau

(ii) nu sunt prezentate standarde armonizate care să răspundă solicitării respective în termenul stabilit în conformitate cu articolul 10 alineatul (1) din Regulamentul (UE) nr. 1025/2012; sau

(iii) standardele armonizate relevante nu abordează suficient preocupările legate de drepturile fundamentale; sau

(iv) standardele armonizate nu sunt conforme cu solicitarea; și

(b) nicio referință la standardele armonizate care vizează cerințele prevăzute în secțiunea 2 din prezentul capitol sau, după caz, obligațiile prevăzute în secțiunile 2 și 3 din capitolul V, nu a fost publicată în *Jurnalul Oficial al Uniunii Europene* în conformitate cu Regulamentul (UE) nr. 1025/2012, și nu se preconizează publicarea niciunei astfel de referințe într-un termen rezonabil.

La redactarea specificațiilor comune, Comisia consultă forumul consultativ menționat la articolul 67.

Actele de punere în aplicare menționate la primul paragraf de la prezentul alineat se adoptă în conformitate cu procedura de examinare menționată la articolul 98 alineatul (2).

(2) 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, sunt îndeplinite condițiile de la alineatul (1).

(3) Sistemele de IA cu grad ridicat de risc sau modelele de IA de uz general care sunt în conformitate cu specificațiile comune menționate la alineatul (1) sau cu părți ale acestora sunt considerate a fi în conformitate cu cerințele prevăzute în secțiunea 2 din prezentul capitol sau, după caz, a respecta obligațiile prevăzute în secțiunile 2 și 3 din capitolul V, în măsura în care respectivele specificații comune vizează cerințele sau obligațiile respective.

(4) În cazul în care un standard armonizat este adoptat de o organizație de standardizare europeană și este propus Comisiei pentru ca referința sa să fie publicată în *Jurnalul Oficial al Uniunii Europene*, Comisia evaluează standardul armonizat în conformitate cu Regulamentul (UE) nr. 1025/2012. Atunci când referința unui standard armonizat este publicată în *Jurnalul Oficial al Uniunii Europene*, Comisia abrogă actele de punere în aplicare menționate la alineatul (1) sau acele părți ale lor care vizează aceleași cerințe menționate la secțiunea 2 din prezentul capitol sau, după caz, aceleași obligații prevăzute în secțiunile 2 și 3 din capitolul V.

(5) În cazul în care furnizorii de sisteme de IA cu grad ridicat de risc sau de modele de IA de uz general nu respectă specificațiile comune menționate la alineatul (1), aceștia trebuie să dovedească în mod corespunzător faptul că au adoptat soluții tehnice care îndeplinesc cerințele menționate în secțiunea 2 din prezentul capitol sau, după caz, care respectă obligațiile prevăzute în secțiunile 2 și 3 din capitolul V la un nivel cel puțin echivalent cu acestea.

(6) În cazul în care un stat membru consideră că o specificație comună nu îndeplinește în totalitate cerințele prevăzute în secțiunea 2 sau, după caz, nu respectă în totalitate obligațiile prevăzute în secțiunile 2 și 3 din capitolul V, acesta informează Comisia în acest sens, furnizând o explicație detaliată. 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, contextual sau funcțional specific în care sunt destinate să fie utilizate sunt considerate a respecta cerințele relevante prevăzute la articolul 10 alineatul (4).

(2) Sistemele de IA cu grad ridicat de risc care au fost certificate sau pentru care a fost emisă o declarație de conformitate în cadrul unui sistem de securitate cibernetică în temeiul Regulamentului (UE) 2019/881, iar referințele aferente au fost publicate în *Jurnalul Oficial al Uniunii Europene*, sunt considerate a respecta 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 vizează 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 secțiunea 2, furnizorul a aplicat standardele armonizate menționate la articolul 40 sau, după caz, specificațiile comune menționate la articolul 41, furnizorul optează pentru una dintre următoarele proceduri de evaluare a conformității:

(a) controlul intern, menționat în anexa VI; sau

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

Pentru a demonstra conformitatea unui sistem de IA cu grad ridicat de risc cu cerințele prevăzute în secțiunea 2, furnizorul urmează procedura de evaluare a conformității prevăzută în anexa VII în următoarele cazuri:

(a) standardele armonizate menționate la articolul 40 nu există, iar specificațiile comune menționate la articolul 41 nu sunt disponibile;

(b) furnizorul nu a aplicat sau a aplicat doar o parte din standardul armonizat;

(c) specificațiile comune menționate la litera (a) există, dar furnizorul nu le-a aplicat;

(d) unul sau mai multe dintre standardele armonizate menționate la litera (a) au fost publicate cu o restricție și numai în partea standardului care a fost restricționată.

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 de IA cu grad ridicat de risc este destinat să fie pus în funcțiune de către autoritățile de aplicare a legii, de imigrație sau de azil, sau de către instituțiile, organele, oficiile sau agențiile Uniunii, autoritatea de supraveghere a pieței menționată la articolul 74 alineatul (8) sau (9), 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, 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 de armonizare ale Uniunii care figurează în anexa I secțiunea A, furnizorul urmează procedura de evaluare a conformității relevantă, astfel cum se prevede în actele juridice respective. Cerințele prevăzute în secțiunea 2 din prezentul capitol 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 secțiunea 2, cu condiția ca respectarea de către organismele notificate respective a cerințelor prevăzute la articolul 31 alineatele (4), (10) și (11) să fi fost evaluată în contextul procedurii de notificare în temeiul respectivelor acte juridice.

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

(4) Sistemele de IA cu grad ridicat de risc care au făcut deja obiectul unei proceduri de evaluare a conformității sunt supuse la o nouă procedură de evaluare a conformității în cazul unei modificări substanțiale, indiferent dacă sistemul modificat este destinat să fie distribuit mai departe sau dacă implementatorul actual continuă să utilizeze sistemul modificat.

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

(5) Comisia este împuternicită să adopte acte delegate în conformitate cu articolul 97 în scopul modificării anexelor VI și VII prin actualizarea acestora având în vedere progresele tehnice.

(6) Comisia este împuternicită să adopte acte delegate în conformitate cu articolul 97 pentru a modifica alineatele (1) și (2) de la prezentul articol cu scopul de a supune sistemele 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 unor 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, siguranță și protecția drepturilor fundamentale pe care le prezintă astfel de sisteme, precum și de disponibilitatea capacităților și a resurselor adecvate în cadrul 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 relevante din statul membru în care este stabilit organismul notificat.

(2) Certificatele sunt valabile pe perioada pe care o indică, care nu depășește cinci ani pentru sistemele de IA vizate de anexa I și patru ani pentru sistemele de IA vizate de anexa III. La solicitarea furnizorului, valabilitatea unui certificat poate fi prelungită pentru perioade suplimentare, fiecare dintre acestea nedepășind cinci ani pentru sistemele de IA vizate de anexa I și patru ani pentru sistemele de IA vizate de anexa III, pe baza unei reevaluări în conformitate cu procedurile aplicabile de evaluare a conformității. Orice supliment la un certificat rămâne valabil, cu condiția ca certificatul pe care îl completează să fie valabil.

(3) În cazul în care un organism notificat constată că un sistem de IA nu mai îndeplinește cerințele prevăzute în secțiunea 2, 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 măsuri corective adecvate întreprinse de furnizorul sistemului într-un termen adecvat stabilit de organismul notificat. Organismul notificat comunică motivele deciziei sale.

Se pune la dispoziție o cale de atac împotriva deciziilor organismelor notificate, inclusiv privind certificatele de conformitate eliberate.

Articolul 45

Obligații de informare care revin organismelor notificate

(1) Organismele notificate informează autoritatea de notificare în legătură cu:

(a) orice certificate de evaluare a documentației tehnice ale Uniunii, orice suplimente la certificatele respective și orice 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 lor și orice altă activitate realizată, inclusiv activități transfrontaliere și subcontractare.

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

(a) aprobări ale sistemelor de management al calității pe care le-a refuzat, suspendat sau retras și, la cerere, aprobări ale sistemelor de management al calității pe care le-a eliberat;

(b) certificatele de evaluare a documentației tehnice ale Uniunii sau orice suplimente 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 vizează aceleași tipuri de sisteme de IA, informații relevante privind aspecte legate de rezultatele negative ale evaluărilor conformității și, la cerere, de rezultatele pozitive ale evaluărilor conformității.

(4) Organismele notificate păstrează confidențialitatea informațiilor pe care le obțin, în conformitate cu articolul 78.

Articolul 46

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 sau de protecție a activelor industriale și de infrastructură esențiale. Autorizația respectivă se acordă pentru o perioadă limitată, 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.

(2) 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. În cazul în care autorizația menționată la alineatul (1) este refuzată, utilizarea sistemului de IA cu grad ridicat de risc este oprită cu efect imediat și toate rezultatele și produsele obținute în cadrul unei astfel de utilizări sunt înlăturate imediat.

(3) 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 secțiunea 2. Autoritatea de supraveghere a pieței informează Comisia și celelalte state membre cu privire la orice autorizație eliberată în temeiul alineatelor (1) și (2). Această obligație nu vizează datele operaționale sensibile legate de activitățile autorităților de aplicare a legii.

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

(5) În cazul în care, în termen de 15 zile calendaristice de la primirea notificării menționate la alineatul (3), sunt ridicate obiecții de către un stat membru împotriva unei autorizații eliberate de o autoritate de supraveghere a pieței dintr-un alt stat membru sau în cazul în care Comisia consideră că autorizația este contrară dreptului Uniunii sau că concluzia statelor membre cu privire la conformitatea sistemului, astfel cum se menționează la alineatul (3), este nefondată, Comisia inițiază fără întârziere consultări cu statul membru relevant. Operatorii în cauză sunt consultați și au posibilitatea de a-și prezenta punctele de vedere. În considerarea acestora, Comisia decide dacă autorizația este justificată. Comisia comunică decizia sa statelor membre în cauză și operatorilor relevanți.

(6) În cazul în care Comisia consideră că autorizația este nejustificată, aceasta este retrasă de către autoritatea de supraveghere a pieței din statul membru în cauză.

(7) Pentru sistemele de IA cu grad ridicat de risc legate de produsele care fac obiectul actelor legislative de armonizare ale Uniunii menționate în anexa I secțiunea A, se aplică numai derogări de la procedurile de evaluare a conformității stabilite în respectivele acte legislative de armonizare ale Uniunii.

Articolul 47

Declarația de conformitate UE

(1) Furnizorul întocmește o declarație de conformitate UE elaborată într-un format prelucrabil automat, cu semnătură fizică sau electronică pentru fiecare sistem de IA cu grad ridicat de risc 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 cu grad ridicat de risc. Declarația de conformitate UE identifică sistemul de IA cu grad ridicat de risc 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 secțiunea 2. 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 statele membre în care se introduce pe piață sau 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 în legătură cu toate actele legislative ale Uniunii aplicabile sistemului de IA cu grad ridicat de risc. Declarația conține toate informațiile necesare pentru identificarea actelor legislative de armonizare ale Uniunii cu care are legătură declarația.

(4) Prin redactarea declarației de conformitate UE, furnizorul își asumă responsabilitatea pentru conformitatea cu cerințele prevăzute în secțiunea 2. Furnizorul actualizează în permanență declarația de conformitate UE, după caz.

(5) Comisia este împuternicită să adopte acte delegate în conformitate cu articolul 97 pentru a modifica anexa V prin actualizarea conținutului declarației de conformitate UE prevăzute în anexa menționată, pentru a introduce elemente care devin necesare având în vedere progresele tehnice.

Articolul 48

Marcajul CE

(1) Marcajul CE face obiectul principiilor generale prevăzute la articolul 30 din Regulamentul (CE) nr. 765/2008.

(2) În cazul sistemelor de IA cu grad ridicat de risc furnizate digital se utilizează un marcaj CE digital numai dacă poate fi accesat cu ușurință prin intermediul interfeței de la care este accesat sistemul respectiv sau printr-un cod ușor accesibil, prelucrabil automat, sau prin alte mijloace electronice.

(3) Marcajul CE se aplică în mod vizibil, lizibil și indelebil pe sistemele de IA cu grad ridicat de risc. 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 sau pe documentele de însoțire, după caz.

(4) 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. Numărul de identificare al organismului notificat se aplică chiar de către organism sau, la instrucțiunile acestuia, de către furnizor sau reprezentantul autorizat al furnizorului. De asemenea, numărul de identificare se indică în orice material promoțional care menționează că sistemul de IA cu grad ridicat de risc îndeplinește cerințele aferente marcajului CE.

(5) În cazul în care sistemele de IA cu grad ridicat de risc fac obiectul altor acte legislative ale Uniunii care prevăd de asemenea aplicarea marcajului CE, acesta indică faptul că sistemele de IA cu grad ridicat de risc îndeplinesc și cerințele celorlalte acte legislative.

Articolul 49
Înregistrare

(1) Înainte de a introduce pe piață sau de a pune în funcțiune un sistem de IA cu grad ridicat de risc care figurează în anexa III, cu excepția sistemelor de IA cu grad ridicat de risc menționate în anexa III punctul 2, furnizorul și, după caz, reprezentantul autorizat se înregistrează pe sine, alături de sistemul lor în baza de date a UE menționată la articolul 71.

(2) Înainte de a introduce pe piață sau de a pune în funcțiune un sistem de IA pentru care furnizorul a concluzionat că nu prezintă un grad ridicat de risc în conformitate cu articolul 6 alineatul (3), furnizorul respectiv sau, după caz, reprezentantul autorizat se înregistrează pe sine, alături de sistemul respectiv în baza de date a UE menționată la articolul 71.

(3) Înainte de a pune în funcțiune sau de a utiliza un sistem de IA cu grad ridicat de risc care figurează în anexa III, cu excepția sistemelor de IA cu grad ridicat de risc care figurează în anexa III punctul 2, implementatorii care sunt autorități publice, instituții, organe, oficii sau agenții ale Uniunii ori persoane care acționează în numele acestora se înregistrează, selectează sistemul și înregistrează utilizarea acestuia în baza de date a UE menționată la articolul 71.

(4) Pentru sistemele de IA cu grad ridicat de risc menționate la punctele 1, 6 și 7 din anexa III, în domeniul aplicării legii, al migrației, al azilului și al gestionării controlului la frontiere, înregistrarea menționată la alineatele (1), (2) și (3) de la prezentul articol se realizează în cadrul unei secțiuni securizate, care nu este accesibilă publicului, a bazei de date a UE menționate la articolul 71 și include numai următoarele informații, după caz, menționate la:

(a) secțiunea A punctele 1-10 din anexa VIII, cu excepția punctelor 6, 8 și 9;

(b) secțiunea B punctele 1-5, 8 și 9 din anexa VIII;

(c) secțiunea C punctele 1-3 din anexa VIII;

(d) punctele 1, 2, 3 și 5 din anexa IX.

Numai Comisia și autoritățile naționale menționate la articolul 74 alineatul (8) au acces la secțiunile restricționate respective ale bazei de date a UE care figurează la primul paragraf de la prezentul alineat.

(5) Sistemele de IA cu grad ridicat de risc menționate la punctul 2 din anexa III se înregistrează la nivel național.

Capitolul IV

Obligații de transparență pentru furnizorii și implementatorii anumitor sisteme de IA

Articolul 50

Obligații de transparență pentru furnizorii și implementatorii anumitor sisteme de IA

(1) Furnizorii se asigură că sistemele de IA destinate să interacționeze direct cu persoane fizice sunt proiectate și dezvoltate astfel încât persoanele fizice în cauză 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 rezonabil de bine informată, de atentă și de avizată, ținând seama de circumstanțele și contextul de utilizare. Această obligație nu se aplică sistemelor de IA autorizate prin lege pentru a depista, a preveni, a investiga sau 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) Furnizorii de sisteme de IA, inclusiv de sisteme de IA de uz general, care generează conținut sintetic în format audio, imagine, video sau text, se asigură că rezultatele sistemului de IA sunt marcate într-un format prelucrabil automat și detectabile ca fiind generate sau manipulate artificial. Furnizorii se asigură că soluțiile lor tehnice sunt eficace, interoperabile, solide și fiabile, în măsura în care acest lucru este fezabil din punct de vedere tehnic, ținând seama de particularitățile și limitările diferitelor tipuri de conținut, de costurile de punere în aplicare și de stadiul de avansare general recunoscut al tehnologiei, astfel cum poate fi reflectat în standardele tehnice relevante. Această obligație nu se aplică în măsura în care sistemele de IA îndeplinesc o funcție de asistare pentru editarea standard sau nu modifică în mod substanțial datele de intrare furnizate de implementator sau semantica acestora sau în cazul în care sunt autorizate prin lege să depisteze, să prevină, să investigheze sau să urmărească penal infracțiunile.

(3) Implementatorii unui sistem de recunoaștere a emoțiilor sau ai unui sistem de clasificare biometrică informează persoanele fizice expuse sistemului respectiv cu privire la funcționarea acestuia și prelucrează datele cu caracter personal în conformitate cu Regulamentele (UE) 2016/679 și (UE) 2018/1725 și cu Directiva (UE) 2016/680, după caz. Această obligație nu se aplică sistemelor de IA utilizate pentru clasificarea biometrică și recunoașterea emoțiilor, care sunt autorizate prin lege să depisteze, să prevină sau să investigheze infracțiunile, sub rezerva unor garanții adecvate pentru drepturile și libertățile terților și în conformitate cu dreptul Uniunii.

(4) Implementatorii unui sistem de IA care generează sau manipulează imagini, conținuturi audio sau video care constituie deepfake-uri dezvăluie faptul că respectivul conținut a fost generat sau manipulat artificial. Această obligație nu se aplică în cazul în care utilizarea este autorizată prin lege pentru depistarea, prevenirea, investigarea sau urmărirea penală a infracțiunilor. În cazul în care conținutul face parte dintr-o operă sau dintr-un program de o vădită natură artistică, creativă, satirică, fictivă sau analogă, obligațiile de transparență prevăzute la prezentul alineat se limitează la divulgarea existenței unui astfel de conținut generat sau manipulat într-un mod adecvat, care să nu împiedice afișarea sau receptarea operei.

Implementatorii unui sistem de IA care generează sau manipulează texte publicate cu scopul de a informa publicul cu privire la chestiuni de interes public dezvăluie faptul că textul a fost generat sau manipulat artificial. Această obligație nu se aplică în cazul în care utilizarea este autorizată prin lege pentru a depista, a preveni, a investiga sau a urmări penal infracțiunile sau în cazul în care conținutul generat de IA a fost supus unui proces de verificare editorială sau revizuire umană și responsabilitatea editorială pentru publicarea conținutului este deținută de o persoană fizică sau juridică.

(5) Informațiile menționate la alineatele (1)-(4) sunt furnizate persoanelor fizice în cauză într-un mod clar și distinct, cel târziu în momentul primei interacțiuni sau al primei expuneri. Informațiile trebuie să respecte cerințele de accesibilitate aplicabile.

(6) Alineatele (1)-(4) nu aduc atingere cerințelor și obligațiilor prevăzute în capitolul III și nici altor obligații de transparență pentru implementatorii de sisteme de IA prevăzute în dreptul Uniunii sau în dreptul intern.

(7) Oficiul pentru IA încurajează și facilitează elaborarea de coduri de bune practici la nivelul Uniunii pentru a facilita punerea în aplicare efectivă a obligațiilor privind depistarea și etichetarea conținutului generat sau manipulat artificial. Comisia poate să adopte acte de punere în aplicare pentru a aproba respectivele coduri de bune practici în conformitate cu procedura prevăzută la articolul 56 alineatul (6). În cazul în care consideră că codul nu este adecvat, Comisia poate să adopte un act de punere în aplicare care să precizeze normele comune pentru punerea în aplicare a obligațiilor respective, în conformitate cu procedura de examinare prevăzută la articolul 98 alineatul (2).

Capitolul V
Modele de IA de uz general

SECȚIUNEA 1
NORME DE CLASIFICARE

Articolul 51

Clasificarea modelelor de IA de uz general ca modele de IA de uz general cu risc sistemic

(1) Un model de IA de uz general este clasificat drept model de IA de uz general cu risc sistemic dacă îndeplinește oricare dintre următoarele condiții:

(a) are capabilități cu impact ridicat evaluate pe baza unor instrumente și metodologii tehnice adecvate, inclusiv a unor indicatori și valori de referință;

(b) pe baza unei decizii a Comisiei, *ex officio* sau în urma unei alerte calificate din partea grupului științific, are capabilități sau un impact echivalente cu cele prevăzute la litera (a), având în vedere criteriile stabilite în anexa XIII.

(2) Se consideră că un model de IA de uz general are capabilități cu impact ridicat în temeiul alineatului (1) litera (a) atunci când volumul cumulat de calcul utilizat pentru antrenarea sa măsurat în operații în virgulă mobilă este mai mare de 10^{25}.

(3) Comisia adoptă acte delegate în conformitate cu articolul 97 pentru a modifica pragurile care figurează la alineatele (1) și (2) de la prezentul articol, precum și pentru a completa valorile de referință și indicatorii având în vedere evoluțiile tehnologice constante, cum ar fi îmbunătățirile algoritmice sau eficiența sporită a hardware-ului, atunci când este necesar, astfel încât pragurile respective să reflecte stadiul cel mai avansat al tehnologiei.

Articolul 52

Procedură

(1) În cazul în care un model de IA de uz general îndeplinește condiția menționată la articolul 51 alineatul (1) litera (a), furnizorul relevant informează Comisia fără întârziere și, în orice caz, în termen de două săptămâni de la îndeplinirea cerinței respective sau de la data la care se constată faptul că va fi îndeplinită. Notificarea respectivă include informațiile necesare pentru a demonstra că a fost îndeplinită cerința relevantă. În cazul în care ia cunoștință de un model de IA de uz general care prezintă riscuri sistemice cu privire la care nu a fost notificată, Comisia poate decide să îl desemneze drept model prezentând risc sistemic.

(2) Furnizorul unui model de IA de uz general care îndeplinește condiția menționată la articolul 51 alineatul (1) litera (a) poate prezenta, odată cu notificarea sa, argumente suficient de întemeiate pentru a demonstra că, în mod excepțional, deși îndeplinește cerința respectivă, modelul de IA de uz general nu prezintă riscuri sistemice, având în vedere caracteristicile sale specifice și, prin urmare, nu ar trebui să fie clasificat drept model de IA de uz general cu risc sistemic.

(3) În cazul în care concluzionează că argumentele prezentate în temeiul alineatului (2) nu sunt suficient de întemeiate, iar furnizorul relevant nu a fost în măsură să demonstreze că modelul de IA de uz general nu prezintă riscuri sistemice, având în vedere caracteristicile sale specifice, Comisia respinge argumentele respective, iar modelul de IA de uz general este considerat un model de IA de uz general cu risc sistemic.

(4) Comisia poate desemna un model de IA de uz general ca prezentând riscuri sistemice, *ex officio* sau în urma unei alerte calificate din partea comitetului științific în temeiul articolului 90 alineatul (1) litera (a), pe baza criteriilor stabilite în anexa XIII.

Comisia este împuternicită să adopte acte delegate în conformitate cu articolul 97 pentru a modifica anexa XIII prin precizarea și actualizarea criteriilor prevăzute în anexa menționată.

(5) La cererea motivată a unui furnizor al cărui model a fost desemnat drept model de IA de uz general cu risc sistemic în temeiul alineatului (4), Comisia ia în considerare cererea și poate decide să reevalueze dacă modelul de IA de uz general poate fi considerat în continuare ca prezentând riscuri sistemice pe baza criteriilor prevăzute în anexa XIII. O astfel de cerere conține motive obiective, detaliate și noi care au survenit după decizia de desemnare. Furnizorii pot solicita reevaluarea cel mai devreme la șase luni de la decizia de desemnare. În cazul în care, în urma reevaluării sale, Comisia decide să mențină desemnarea drept model de IA de uz general cu risc sistemic, furnizorii pot solicita reevaluarea cel mai devreme la șase luni de la decizia respectivă.

(6) Comisia se asigură că se publică o listă a modelelor de IA de uz general cu risc sistemic și actualizează lista respectivă, fără a aduce atingere necesității de a respecta și de a proteja drepturile de proprietate intelectuală și informațiile comerciale confidențiale sau secretele comerciale în conformitate cu dreptul Uniunii și cu dreptul intern.

SECȚIUNEA 2

OBLIGAȚIILE FURNIZORILOR DE MODELE DE IA DE UZ GENERAL

Articolul 53

Obligațiile furnizorilor de modele de IA de uz general

(1) Furnizorii de sisteme de IA de uz general:

(a) realizează și actualizează documentația tehnică a modelului, inclusiv procesul vizând antrenarea și testarea sa, precum și rezultatele evaluării sale, care conțin cel puțin informațiile prevăzute în anexa XI în scopul de a le furniza, la cerere, Oficiului pentru IA și autorităților naționale competente;

(b) elaborează, actualizează și pun la dispoziție informații și documentație destinate furnizorilor de sisteme de IA care intenționează să integreze modelul de IA de uz general în sistemele lor de IA. Fără a aduce atingere necesității de a respecta și de a proteja drepturile de proprietate intelectuală și informațiile comerciale confidențiale sau secretele comerciale în conformitate cu dreptul Uniunii și cu dreptul intern, informațiile și documentația:

(i) le permit furnizorilor de sisteme de IA să înțeleagă bine capabilitățile și limitările modelului de IA de uz general și să respecte obligațiile care le revin în temeiul prezentului regulament; și

(ii) conțin cel puțin elementele prevăzute în anexa XII;

(c) pun în aplicare o politică vizând respectarea dreptului Uniunii privind drepturile de autor și drepturile conexe și, în special, identificarea și respectarea, inclusiv pe baza stadiului cel mai avansat al tehnologiei, a unei rezervări a drepturilor exprimate în temeiul articolului 4 alineatul (3) din Directiva (UE) 2019/790;

(d) elaborează și pun la dispoziția publicului un rezumat suficient de detaliat cu privire la conținutul utilizat pentru antrenarea modelului de IA de uz general, în conformitate cu un model furnizat de Oficiul pentru IA.

(2) Obligațiile prevăzute la alineatul (1) literele (a) și (b) nu se aplică furnizorilor de modele de IA care sunt lansate sub licență liberă și deschisă permițând accesul, utilizarea, modificarea și distribuția modelelor respective și ai căror parametri, inclusiv ponderile și informațiile privind arhitectura modelelor și utilizarea acestora, sunt puși la dispoziția publicului. Această excepție nu se aplică modelelor de IA de uz general cu risc sistemic.

(3) Furnizorii de modele de IA de uz general cooperează, după caz, cu Comisia și cu autoritățile naționale competente în exercitarea competențelor și a prerogativelor lor în temeiul prezentului regulament.

(4) Furnizorii de modele de IA de uz general se pot baza pe coduri de bune practici în sensul articolului 56 pentru a demonstra respectarea obligațiilor prevăzute la alineatul (1) de la prezentul articol, până la publicarea unui standard armonizat. Respectarea standardelor europene armonizate oferă furnizorilor prezumția de conformitate, în măsura în care standardele respective vizează obligațiile respective. Furnizorii de modele de IA de uz general care nu aderă la un cod de bune practici aprobat sau nu respectă un standard european armonizat demonstrează existența unor mijloace alternative adecvate de conformitate spre a fi evaluate de Comisie.

(5) În scopul facilitării respectării anexei XI, în special a punctului 2 literele (d) și (e), Comisia este împuternicită să adopte acte delegate în conformitate cu articolul 97 pentru a detalia metodologiile de măsurare și de calculare, astfel încât documentațiile să poată fi comparabile și verificabile.

(6) Comisia este împuternicită să adopte acte delegate în conformitate cu articolul 97 alineatul (2) pentru a modifica anexele XI și XII având în vedere evoluțiile tehnologice constante.

(7) Orice informații sau documentație obținute în temeiul prezentului articol, inclusiv secretele comerciale, sunt tratate în conformitate cu obligațiile de confidențialitate prevăzute la articolul 78.

Articolul 54

Reprezentanții autorizați ai furnizorilor de modele de IA de uz general

(1) Înainte de a pune la dispoziție un model de IA de uz general pe piața Uniunii, furnizorii stabiliți în țări terțe desemnează, prin mandat scris, un reprezentant autorizat stabilit în Uniune.

(2) Furnizorul permite reprezentantului său autorizat să îndeplinească sarcinile prevăzute în mandatul primit de la furnizor.

(3) Reprezentantul autorizat îndeplinește sarcinile prevăzute în mandatul primit de la furnizor. Acesta furnizează Oficiului pentru IA, la cerere, o copie a mandatului, într-una din limbile oficiale ale instituțiilor Uniunii. În sensul prezentului regulament, mandatul îl împuternicește pe reprezentantul autorizat să îndeplinească următoarele sarcini:

(a) să verifice dacă a fost întocmită documentația tehnică specificată în anexa XI și dacă au fost îndeplinite de către furnizor toate obligațiile menționate la articolul 53 și, după caz, la articolul 55;

(b) să păstreze la dispoziția Oficiului pentru IA și a autorităților naționale competente o copie a documentației tehnice specificate în anexa XI pentru o perioadă de 10 ani după introducerea pe piață a modelului de IA de uz general, precum și datele de contact ale furnizorului care a desemnat reprezentantul autorizat;

(c) să furnizeze Oficiului pentru IA, în urma unei cereri motivate, toate informațiile și documentația, inclusiv cele menționate la litera (b), necesare pentru a demonstra respectarea de către furnizor a obligațiilor prevăzute în prezentul capitol;

(d) să coopereze cu Oficiul pentru IA și cu autoritățile competente, în urma unei cereri motivate, cu privire la orice acțiune întreprinsă de acestea în legătură cu un model de IA de uz general, inclusiv atunci când modelul este integrat în sistemele de IA introduse pe piață sau puse în funcțiune în Uniune.

(4) Mandatul împuternicește reprezentantul autorizat să fie contactat, pe lângă furnizor sau în locul acestuia, de către Oficiul pentru IA sau autoritățile competente, cu referire la toate aspectele legate de asigurarea conformității cu prezentul regulament.

(5) Reprezentantul autorizat își reziliază mandatul dacă consideră sau are motive să considere că furnizorul acționează contrar obligațiilor care îi revin în temeiul prezentului regulament. Într-un astfel de caz, el informează imediat Oficiul pentru IA cu privire la rezilierea mandatului și la motivele acesteia.

(6) Obligația prevăzută la prezentul articol nu se aplică furnizorilor de modele de IA de uz general care sunt lansate sub licență liberă și cu sursă deschisă permițând accesul, utilizarea, modificarea și distribuția modelelor respective și ai căror parametri, inclusiv ponderile și informațiile privind arhitectura modelelor și utilizarea acestora, sunt puși la dispoziția publicului, cu excepția cazului în care modelele de IA de uz general prezintă riscuri sistemice.

SECȚIUNEA 3

OBLIGAȚIILE FURNIZORILOR DE MODELE DE IA DE UZ GENERAL CU RISC SISTEMIC

Articolul 55

Obligațiile furnizorilor de modele de IA de uz general cu risc sistemic

(1) Pe lângă obligațiile enumerate la articolele 53 și 54, furnizorii de modele de IA de uz general cu risc sistemic:

(a) efectuează evaluarea modelelor în conformitate cu protocoale și instrumente standardizate care reflectă stadiul de avansare al tehnologiei, inclusiv prin efectuarea de testări contradictorii ale modelelor și documentarea acestora, în vederea identificării și atenuării riscurilor sistemice;

(b) evaluează și atenuează posibilele riscuri sistemice la nivelul Uniunii, inclusiv sursele acestora, care pot decurge din dezvoltarea, introducerea pe piață sau utilizarea unor modele de IA de uz general cu risc sistemic;

(c) urmăresc, documentează și raportează fără întârzieri nejustificate Oficiului pentru IA și, după caz, autorităților naționale competente, informații relevante cu privire la incidentele grave și la posibilele măsuri corective pentru a le aborda;

(d) asigură un nivel adecvat de protecție a securității cibernetice pentru modelele de IA de uz general cu risc sistemic și pentru infrastructura fizică a modelelor.

(2) Furnizorii de modele de IA de uz general cu risc sistemic se pot baza pe coduri de bune practici în sensul articolului 56 pentru a demonstra respectarea obligațiilor prevăzute la alineatul (1) de la prezentul articol, până la publicarea unui standard armonizat. Respectarea standardelor europene armonizate oferă furnizorilor prezumția de conformitate, în măsura în care standardele respective vizează obligațiile respective. Furnizorii de modele de IA de uz general cu risc sistemic care nu aderă la un cod de bune practici aprobat sau nu respectă un standard european armonizat demonstrează existența unor mijloace alternative adecvate de conformitate, spre a fi evaluate de Comisie.

(3) Orice informații sau documentație obținute în temeiul prezentului articol, inclusiv secretele comerciale, sunt tratate în conformitate cu obligațiile de confidențialitate prevăzute la articolul 78.

SECȚIUNEA 4

CODURI DE BUNE PRACTICI

Articolul 56

Coduri de bune practici

(1) Oficiul pentru IA încurajează și facilitează elaborarea de coduri de bune practici la nivelul Uniunii pentru a contribui la aplicarea corespunzătoare a prezentului regulament, ținând seama de abordările internaționale.

(2) Oficiul pentru IA și comitetul urmăresc să se asigure că codurile de bune practici vizează cel puțin obligațiile prevăzute la articolele 53 și 55, inclusiv următoarele aspecte:

(a) mijloacele de asigurare a faptului că informațiile menționate la articolul 53 alineatul (1) literele (a) și (b) sunt actualizate având în vedere evoluțiile tehnologice și ale pieței;

(b) nivelul adecvat de detaliere a rezumatului cu privire la conținutul utilizat pentru antrenare;

(c) identificarea tipului și naturii riscurilor sistemice la nivelul Uniunii, inclusiv a surselor acestora, după caz;

(d) măsurile, procedurile și modalitățile pentru evaluarea și gestionarea riscurilor sistemice la nivelul Uniunii, inclusiv documentația aferentă, care sunt proporționale cu riscurile, iau în considerare gravitatea și probabilitatea acestora, precum și provocările specifice legate de abordarea acestor riscuri, având în vedere modurile posibile în care astfel de riscuri pot apărea și se pot materializa de-a lungul lanțului valoric al IA.

(3) Oficiul pentru IA poate invita toți furnizorii de modele de IA de uz general, precum și autoritățile naționale competente relevante, să participe la elaborarea de coduri de bune practici. Organizațiile societății civile, industria, mediul academic și alte părți interesate relevante, cum ar fi furnizorii din aval și experții independenți, pot sprijini procesul.

(4) Oficiul pentru IA și comitetul urmăresc să se asigure că codurile de bune practici stabilesc în mod clar obiectivele lor specifice, conțin angajamente sau măsuri, inclusiv indicatori-cheie de performanță, după caz, pentru a asigura realizarea obiectivelor respective și că acestea țin seama în mod corespunzător de nevoile și interesele tuturor părților interesate, inclusiv ale persoanelor afectate, la nivelul Uniunii.

(5) Oficiul pentru IA urmărește să se asigure că participanții la codurile de bune practici raportează periodic Oficiului pentru IA cu privire la punerea în aplicare a angajamentelor și a măsurilor luate și a rezultatelor acestora, inclusiv astfel cum sunt măsurate în raport cu indicatorii-cheie de performanță, după caz. Indicatorii-cheie de performanță și obligațiile de raportare reflectă diferențele de dimensiune și de capacitate dintre diferiții participanți.

(6) Oficiul pentru IA și comitetul monitorizează și evaluează periodic îndeplinirea obiectivelor codurilor de bune practici de către participanți și contribuția acestora la aplicarea corespunzătoare a prezentului regulament. Oficiul pentru IA și comitetul evaluează dacă codurile de bune practici vizează obligațiile prevăzute la articolele 53 și 55 și monitorizează și evaluează periodic îndeplinirea obiectivelor lor. Acestea publică evaluarea caracterului adecvat al codurilor de bune practici.

Comisia poate, prin intermediul unui act de punere în aplicare, să aprobe un cod de bune practici și îi poate conferi o valabilitate generală în cadrul Uniunii. Actul de punere în aplicare respectiv se adoptă în conformitate cu procedura de examinare menționată la articolul 98 alineatul (2).

(7) Oficiul pentru IA poate invita toți furnizorii de modele de IA de uz general să adere la codurile de bune practici. Pentru furnizorii de modele de IA de uz general care nu prezintă riscuri sistemice, aderarea respectivă se poate limita la obligațiile prevăzute la articolul 53, cu excepția cazului în care aceștia își declară în mod explicit interesul de a adera la codul integral.

(8) De asemenea, Oficiul pentru IA încurajează și facilitează, după caz, revizuirea și adaptarea codurilor de bune practici, în special în lumina standardelor emergente. Oficiul pentru IA contribuie la evaluarea standardelor disponibile.

(9) Codurile de bune practici sunt pregătite cel târziu până la ... [nouă luni de la data intrării în vigoare a prezentului regulament]. Oficiul pentru IA face demersurile necesare, inclusiv prin invitarea furnizorilor în temeiul alineatului (7).

În cazul în care, până la ... [12 luni de la data intrării în vigoare], nu poate fi finalizat un cod de bune practici sau în cazul în care Oficiul pentru IA consideră, în urma evaluării sale în temeiul alineatului (6) de la prezentul articol, că acesta nu este adecvat, Comisia poate prevedea, prin intermediul unor acte de punere în aplicare, norme comune pentru punerea în aplicare a obligațiilor prevăzute la articolele 53 și 55, inclusiv aspectele prevăzute la alineatul (2) de la prezentul articol. Actele de punere în aplicare respective se adoptă în conformitate cu procedura de examinare menționată la articolul 98 alineatul (2).

Capitolul VI
Măsuri de sprijinire a inovării

Articolul 57

Spațiile de testare în materie de reglementare în domeniul IA

(1) Statele membre se asigură că autoritățile lor competente instituie cel puțin un spațiu de testare în materie de reglementare în domeniul IA la nivel național, care este operațional până la ... [24 de luni de la data intrării în vigoare a prezentului regulament]. Spațiul de testare respectiv poate fi instituit, de asemenea, împreună cu autoritățile competente din alte state membre. Comisia poate oferi sprijin tehnic, consiliere și instrumente pentru instituirea și exploatarea spațiilor de testare în materie de reglementare în domeniul IA.

Obligația prevăzută la primul paragraf poate fi îndeplinită și prin participarea la un spațiu de testare existent, în măsura în care această participare asigură un nivel echivalent de acoperire națională pentru statele membre participante.

(2) De asemenea, pot fi instituite spații de testare suplimentare în materie de reglementare în domeniul IA la nivel regional sau local sau împreună cu autoritățile competente din alte state membre.

(3) Autoritatea Europeană pentru Protecția Datelor poate, de asemenea, să instituie un spațiu de testare în materie de reglementare în domeniul IA pentru instituțiile, organele, oficiile și agențiile Uniunii și poate să exercite rolurile și sarcinile autorităților naționale competente în conformitate cu prezentul capitol.

(4) Statele membre se asigură că autoritățile competente menționate la alineatele (1) și (2) alocă resurse suficiente pentru a se conforma prezentului articol în mod eficace și în timp util. După caz, autoritățile naționale competente cooperează cu alte autorități relevante și pot permite implicarea altor actori din ecosistemul de IA. Prezentul articol nu aduce atingere altor spații de testare în materie de reglementare instituite în temeiul dreptului Uniunii sau al dreptului intern. Statele membre asigură un nivel adecvat de cooperare între autoritățile care supraveghează aceste alte spații de testare și autoritățile naționale competente.

(5) Spațiile de testare în materie de reglementare în domeniul IA instituite în temeiul alineatului (1) prevăd un mediu controlat care promovează inovarea și facilitează dezvoltarea, antrenare, testarea și validarea sistemelor de IA inovatoare pentru o perioadă limitată de timp înainte de introducerea lor pe piață sau de punerea lor în funcțiune în temeiul unui plan specific privind spațiul de testare convenit între furnizori sau furnizorii potențiali și autoritatea competentă. Astfel de spații de testare pot include testarea în condiții reale supravegheată în spațiul de testare.

(6) Autoritățile competente oferă, după caz, orientări, supraveghere și sprijin în cadrul spațiului de testare în materie de reglementare în domeniul IA în vederea identificării riscurilor, în special în ceea ce privește drepturile fundamentale, sănătatea și siguranța, în vederea testării, precum și în vederea unor măsuri de atenuare și a asigurării eficacității acestora în ceea ce privește obligațiile și cerințele prezentului regulament și, după caz, ale altor dispoziții din dreptul Uniunii și dreptul intern care fac obiectul supravegherii în cadrul spațiului de testare.

(7) Autoritățile competente oferă furnizorilor și potențialilor furnizori care participă la spațiul de testare în materie de reglementare în domeniul IA orientări privind așteptările în materie de reglementare și modul de îndeplinire a cerințelor și a obligațiilor prevăzute în prezentul regulament.

La cererea furnizorului sau a potențialului furnizor al sistemului de IA, autoritatea competentă furnizează o dovadă scrisă a activităților desfășurate cu succes în spațiul de testare. Autoritatea competentă furnizează, de asemenea, un raport de ieșire care detaliază activitățile desfășurate în spațiul de testare, precum și realizările și rezultatele învățării aferente. Furnizorii pot utiliza o astfel de documentație pentru a demonstra că respectă prezentul regulament prin intermediul procesului de evaluare a conformității sau al activităților relevante de supraveghere a pieței. În acest sens, rapoartele de ieșire și dovezile scrise furnizate de autoritatea națională competentă sunt luate în considerare în mod pozitiv de către autoritățile de supraveghere a pieței și de către organismele notificate, în vederea accelerării procedurilor de evaluare a conformității într-o măsură rezonabilă.

(8) Sub rezerva dispozițiilor privind confidențialitatea de la articolul 78 și cu acordul furnizorului sau al potențialului furnizor, Comisia 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 furnizorul sau potențialul furnizor, cât și autoritatea națională competentă își dau acordul în mod explicit, raportul de ieșire poate fi pus la dispoziția publicului prin intermediul platformei unice de informare menționate la prezentul articol.

(9) Instituirea spațiilor de testare în materie de reglementare în domeniul IA urmărește să contribuie la următoarele obiective:

(a) îmbunătățirea securității juridice pentru a asigura conformitatea normativă cu prezentul regulament sau, după caz, cu alte dispoziții aplicabile din dreptul Uniunii și din dreptul intern;

(b) sprijinirea schimbului de bune practici prin cooperarea cu autoritățile implicate în spațiul de testare în materie de reglementare în domeniul IA;

(c) stimularea inovării și a competitivității și facilitarea dezvoltării unui ecosistem de IA;

(d) furnizarea de contribuții la învățarea bazată pe dovezi în materie de reglementare;

(e) facilitarea și accelerarea accesului la piața Uniunii pentru sistemele de IA, în special atunci când sunt furnizate de IMM-uri, inclusiv de întreprinderi nou-înființate.

(10) Autoritățile naționale competente se asigură că, în măsura în care sistemele de IA inovatoare implică prelucrarea de date cu caracter personal sau aparțin în alt mod competenței de supraveghere a altor autorități naționale sau autorități competente care furnizează sau sprijină accesul la date, autoritățile naționale de protecție a datelor sau celelalte autorități naționale sau competente respective sunt asociate exploatării spațiului de testare în materie de reglementare în domeniul IA și sunt implicate în supravegherea aspectelor respective pe măsura sarcinilor și a competențelor lor respective.

(11) Spațiile de testare în materie de reglementare în domeniul IA nu afectează competențele de supraveghere sau atribuțiile corective ale autorităților competente care supraveghează spațiile de testare, inclusiv la nivel regional sau local. Orice riscuri semnificative pentru sănătate, siguranță și drepturile fundamentale identificate în timpul dezvoltării și testării unor astfel de sisteme de IA conduc la o atenuare adecvată. Autoritățile naționale competente au competența de a suspenda temporar sau permanent procesul de testare sau participarea la spațiul de testare dacă nu este posibilă o atenuare eficace și informează Oficiul pentru IA cu privire la o astfel de decizie. Autoritățile naționale competente își exercită competențele de supraveghere în limitele dreptului relevant, utilizându-și competențele discreționare atunci când pun în aplicare dispoziții juridice pentru un anumit proiect de spațiu de testare în materie de reglementare în domeniul IA, cu obiectivul de a sprijini inovarea în domeniul IA în Uniune.

(12) Furnizorii și potențialii furnizori care participă la spațiul de testare în materie de reglementare în domeniul IA rămân responsabili, în temeiul dreptului aplicabil al Uniunii și al dreptului național aplicabil în materie de răspundere, pentru orice prejudiciu adus terților ca urmare a experimentării care are loc în spațiul de testare. Cu toate acestea, cu condiția ca potențialii furnizori să respecte planul specific și termenele și condițiile pentru participarea lor și să urmeze cu bună-credință orientările oferite de autoritatea națională competentă, autoritățile nu impun amenzi administrative pentru încălcarea prezentului regulament. În cazurile în care în supravegherea sistemului de IA în spațiul de testare au mai fost implicate activ și alte autorități competente, responsabile de alte dispoziții ale dreptului Uniunii și ale dreptului intern, care au furnizat orientări pentru conformitate, nu se impun amenzi administrative în ceea ce privește actele legislative respective.

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

(14) Autoritățile naționale competente își coordonează activitățile și cooperează în cadrul comitetului.

(15) Autoritățile naționale competente informează Oficiul pentru IA și comitetul cu privire la instituirea unui spațiu de testare și le pot solicita sprijin și orientări. Oficiul pentru IA pune la dispoziția publicului o listă a spațiilor de testare planificate și existente și o actualizează pentru a încuraja o mai mare interacțiune în spațiile de testare în materie de reglementare în domeniul IA, precum și cooperarea transfrontalieră.

(16) Autoritățile naționale competente prezintă rapoarte anuale Oficiului pentru IA și comitetului, începând cu un an de la instituirea spațiului de testare în materie de reglementare în domeniul IA și, ulterior, în fiecare an, până la încetarea acestuia, precum și un raport final. Rapoartele respective furnizează informații cu privire la progresele și rezultatele punerii în aplicare a spațiilor de testare respective, inclusiv cu privire la bune practici, incidente, lecții învățate și recomandări privind instituirea acestora și, după caz, cu privire la aplicarea și posibila revizuire a prezentului regulament, inclusiv a actelor sale delegate și de punere în aplicare, precum și cu privire la aplicarea altor dispoziții de drept ale Uniunii sub supravegherea autorităților competente în spațiul de testare. Autoritățile naționale competente pun la dispoziția publicului, online, rapoartele anuale respective sau rezumate ale acestora. Comisia ține seama, după caz, de rapoartele anuale atunci când își exercită atribuțiile în temeiul prezentului regulament.

(17) Comisia dezvoltă o interfață unică și specifică în cadrul căreia sunt reunite toate informațiile relevante legate de spațiile de testare în materie de reglementare în domeniul IA pentru a permite părților interesate să interacționeze cu spațiile de testare în materie de reglementare în domeniul IA, să adreseze întrebări autorităților competente și să solicite orientări fără caracter obligatoriu cu privire la conformitatea produselor, a serviciilor și a modelelor de afaceri inovatoare care încorporează tehnologii de IA, în conformitate cu articolul 62 alineatul (1) litera (c). Comisia se coordonează în mod proactiv cu autoritățile naționale competente, după caz.

Articolul 58

Modalități detaliate privind spațiile de testare în materie de reglementare a IA și funcționarea acestora

(1) Pentru a evita fragmentarea în cadrul Uniunii, Comisia adoptă acte de punere în aplicare care precizează modalitățile detaliate de instituire, dezvoltare, punere în aplicare, exploatare și supraveghere a spațiilor de testare în materie de reglementare în domeniul IA. Actele de punere în aplicare includ principii comune cu privire la următoarele aspecte:

(a) criteriile de eligibilitate și de selecție pentru participarea la spațiul de testare în materie de reglementare în domeniul IA;

(b) procedurile de depunere a cererii, de participare, de monitorizare, de ieșire și de încetare în ceea ce privește spațiul de testare în materie de reglementare în domeniul IA, inclusiv planul privind spațiul de testare și raportul de ieșire;

(c) termenele și condițiile aplicabile participanților.

Actele de punere în aplicare respective se adoptă în conformitate cu procedura de examinare menționată la articolul 98 alineatul (2).

(2) Actele de punere în aplicare menționate la alineatul (1) garantează că:

(a) spațiile de testare în materie de reglementare în domeniul IA sunt deschise oricărui furnizor sau potențial furnizor al unui sistem de IA care solicită accesul și care îndeplinește criteriile de eligibilitate și de selecție, care sunt transparente și echitabile, și că autoritățile naționale competente informează solicitanții cu privire la decizia lor în termen de trei luni de la depunerea cererii;

(b) spațiile de testare în materie de reglementare în domeniul IA permit un acces larg și egal și țin pasul cu nivelul cererii în ceea ce privește participarea; furnizorii și potențialii furnizori pot, de asemenea, depune cereri în parteneriat cu implementatorii și alte părți terțe relevante;

(c) modalitățile și condițiile detaliate privind spațiile de testare în materie de reglementare în domeniul IA sprijină, în cea mai mare măsură posibilă, flexibilitatea pentru ca autoritățile naționale competente să instituie și să exploateze spațiile lor de testare în materie de reglementare în domeniul IA;

(d) accesul la spațiile de testare în materie de reglementare în domeniul IA este gratuit pentru IMM-uri, inclusiv întreprinderile nou-înființate, fără a aduce atingere costurilor excepționale pe care autoritățile naționale competente le pot recupera în mod echitabil și proporțional;

(e) facilitează respectarea de către furnizori și potențialii furnizori, prin intermediul rezultatelor învățării din spațiile de testare în materie de reglementare în domeniul IA, a obligațiilor de evaluare a conformității în temeiul prezentului regulament și aplicarea voluntară de către aceștia a codurilor de conduită menționate la articolul 95;

(f) spațiile de testare în materie de reglementare în domeniul IA facilitează implicarea altor actori relevanți din ecosistemul IA, cum ar fi organismele notificate și organizațiile de standardizare, IMM-urile, inclusiv întreprinderile nou-înființate, întreprinderile, inovatorii, instalațiile de testare și experimentare, laboratoarele de cercetare și experimentare și centrele europene de inovare digitală, centrele de excelență, cercetătorii individuali, pentru a permite și a facilita cooperarea cu sectorul public și cu sectorul privat;

(g) procedurile, procesele și cerințele administrative pentru depunerea cererilor, selecție, participare și ieșirea din spațiul de testare în materie de reglementare în domeniul IA sunt simple, ușor de înțeles și comunicate în mod clar pentru a facilita participarea IMM-urilor, inclusiv a întreprinderilor nou-înființate, cu capacități juridice și administrative limitate și sunt raționalizate în întreaga Uniune, pentru a evita fragmentarea și astfel încât participarea la un spațiu de testare în materie de reglementare în domeniul IA instituit de un stat membru sau de Autoritatea Europeană pentru Protecția Datelor să fie recunoscută reciproc și uniform și să producă aceleași efecte juridice în întreaga Uniune;

(h) participarea la spațiul de testare în materie de reglementare în domeniul IA este limitată la o perioadă adecvată complexității și amplorii proiectului, și că poate fi prelungită de autoritatea națională competentă;

(i) spațiile de testare în materie de reglementare în domeniul IA facilitează dezvoltarea de instrumente și de infrastructură pentru testarea, etalonarea, evaluarea și explicarea dimensiunilor sistemelor de IA relevante pentru învățarea în materie de reglementare, cum ar fi acuratețea, robustețea și securitatea cibernetică, precum și de măsuri vizând reducerea riscurilor pentru drepturile fundamentale și pentru societate în general.

(3) Potențialii furnizori din spațiile de testare în materie de reglementare în domeniul IA, în special IMM-urile și întreprinderile nou-înființate, sunt direcționați, după caz, către servicii de preimplementare, cum ar fi orientări privind punerea în aplicare a prezentului regulament, către alte servicii cu valoare adăugată, cum ar fi ajutorul acordat în privința documentelor de standardizare și a certificării, instalațiile de testare și experimentare, centrele europene de inovare digitală și centrele de excelență.

(4) Atunci când autoritățile naționale competente iau în considerare autorizarea testării în condiții reale supravegheate în cadrul unui spațiu de testare în materie de reglementare în domeniul IA care urmează a fi instituit în temeiul prezentului articol, acestea convin în mod specific cu participanții asupra clauzelor 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 59

Prelucrarea ulterioară a datelor cu caracter personal în vederea dezvoltării anumitor sisteme de IA în interes public în spațiul de testare în materie de reglementare în domeniul IA

(1) În spațiul de testare în materie de reglementare în domeniul IA, datele cu caracter personal colectate în mod legal în alte scopuri pot fi prelucrate numai în scopul dezvoltării, antrenării și testării anumitor sisteme de IA în spațiul de testare, dacă sunt îndeplinite toate condițiile următoare:

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

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

(ii) un nivel ridicat de protejare și de îmbunătățire a calității mediului, protejarea biodiversității, protecția împotriva poluării, măsuri privind tranziția verde, măsuri privind atenuarea schimbărilor climatice și adaptarea la acestea;

(iii) durabilitatea energetică;

(iv) siguranța și reziliența sistemelor de transport și a mobilității, a infrastructurii critice și a rețelelor;

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

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

(c) există mecanisme eficace de monitorizare pentru a constata dacă în timpul experimentării în spațiul de testare pot apărea riscuri ridicate la adresa drepturilor și libertăților persoanelor vizate, 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 potențialului furnizor și numai persoanele autorizate au acces la datele respective;

(e) furnizorii pot partaja ulterior datele colectate inițial numai în conformitate cu dreptul Uniunii în materie de protecție a datelor; datele cu caracter personal create în spațiul de testare nu pot fi partajate în afara spațiului de testare;

(f) nicio prelucrare a datelor cu caracter personal în contextul spațiului de testare nu conduce la măsuri sau la decizii care afectează persoanele vizate și nici nu afectează aplicarea drepturilor acestora prevăzute în dreptul Uniunii privind protecția datelor cu caracter personal;

(g) toate datele cu caracter personal prelucrate în contextul spațiului de testare sunt protejate prin măsuri tehnice și organizatorice 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) pe site-ul web al autorităților competente sunt publicate un scurt rezumat al proiectului în materie de IA elaborat în spațiul de testare, precum și obiectivele și rezultatele preconizate ale acestuia; această obligație nu vizează datele operaționale sensibile legate de activitățile autorităților de aplicare a legii, de control la frontiere, de imigrație sau de azil.

(2) În scopul prevenirii, investigării, depistării sau urmăririi penale a infracțiunilor sau al executării sancțiunilor penale, 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 în domeniul IA se bazează pe dispoziții specifice ale dreptului Uniunii sau ale dreptului intern și face obiectul acelorași condiții cumulative ca cele menționate la alineatul (1).

(3) Alineatul (1) nu aduce atingere dreptului Uniunii sau dreptului intern care exclude prelucrarea datelor cu caracter personal în alte scopuri decât cele menționate în mod explicit în dreptul respectiv, precum și dreptului Uniunii sau dreptului intern care stabilește temeiul pentru prelucrarea datelor cu caracter personal care este necesară în scopul dezvoltării, testării sau antrenării sistemelor de IA inovatoare sau orice alt temei juridic, în conformitate cu dreptul Uniunii privind protecția datelor cu caracter personal.

Articolul 60

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

(1) Testarea sistemelor de IA cu grad ridicat de risc în condiții reale în afara spațiilor de testare în materie de reglementare în domeniul 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 prezentul articol și cu planul de testare în condiții reale menționat în cadrul acestuia, fără a aduce atingere interdicțiilor prevăzute la articolul 5.

Comisia precizează, prin intermediul unor acte de punere în aplicare, elementele detaliate ale planului de testare în condiții reale. Respectivele acte de punere în aplicare se adoptă în conformitate cu procedura de examinare menționată la articolul 98 alineatul (2).

Prezentul alineat nu aduce atingere dreptului Uniunii sau dreptului intern privind testarea în condiții reale a sistemelor de IA cu grad ridicat de risc legate de produsele care fac obiectul actelor legislative enumerate în anexa I.

(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 sistemelor de IA pe cont propriu sau în parteneriat cu unul sau mai mulți implementatori sau implementatori potențiali.

(3) Testarea sistemelor de IA cu grad ridicat de risc în condiții reale în temeiul prezentului articol nu aduce atingere oricărei evaluări etice care este impusă de dreptul Uniunii sau de dreptul intern.

(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 în care urmează să se efectueze testarea în condiții reale;

(b) autoritatea de supraveghere a pieței din statul membru în care urmează să fie efectuată testarea în condiții reale a aprobat testarea în condiții reale și planul de testare în condiții reale; în cazul în care autoritatea de supraveghere a pieței nu a furnizat un răspuns în termen de 30 de zile, se consideră că testarea în condiții reale și planul de testare în condiții reale au fost aprobate; în cazul în care dreptul intern nu prevede o aprobare tacită, testarea în condiții reale face în continuare obiectul unei autorizații;

(c) furnizorul sau potențialul furnizor, cu excepția furnizorului sau a potențialului furnizor de sisteme de IA cu grad ridicat de risc menționate la punctele 1, 6 și 7 din anexa III în domeniul aplicării legii, al migrației, al azilului și al gestionării controlului la frontiere și de sisteme de IA cu grad ridicat de risc menționate la punctul 2 din anexa III, a înregistrat testarea în condiții reale în conformitate cu articolul 71 alineatul (4) cu un număr unic de identificare la nivelul întregii Uniuni și furnizând informațiile specificate în anexa IX; furnizorul sau potențialul furnizor de sisteme de IA cu grad ridicat de risc menționate la punctele 1, 6 și 7 din anexa III în domeniul aplicării legii, al migrației, al azilului și al gestionării controlului la frontiere a înregistrat testarea în condiții reale în secțiunea securizată care nu este accesibilă publicului a bazei de date a UE în conformitate cu articolul 49 alineatul (4) litera (d), cu un număr unic de identificare la nivelul întregii Uniuni și furnizând informațiile specificate în acesta; furnizorul sau potențialul furnizor de sisteme de IA cu grad ridicat de risc menționate la punctul 2 din anexa III a înregistrat testarea în condiții reale în conformitate cu articolul 49 alineatul (5);

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

(e) datele colectate și prelucrate în scopul testării în condiții reale se transferă către țări terțe numai cu condiția implementării unor garanții corespunzătoare și aplicabile în temeiul dreptului Uniunii;

(f) testarea în condiții reale nu durează mai mult decât este necesar pentru realizarea obiectivelor sale și, în orice caz, nu depășește o perioadă de 6 luni, care poate fi prelungită cu încă 6 luni, sub rezerva notificării prealabile de către furnizor sau potențialul furnizor a autorității de supraveghere a pieței, însoțită de o explicație privind necesitatea unei astfel de prelungiri;

(g) subiecții testării în condiții reale, care sunt persoane care aparțin grupurilor vulnerabile din cauza vârstei sau a dizabilității, sunt protejați în mod corespunzător;

(h) în cazul în care un furnizor sau un potențial furnizor organizează testarea în condiții reale în cooperare cu unul sau mai mulți implementatori sau implementatori potențiali, aceștia 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 pentru utilizarea sistemului de IA menționate la articolul 13; furnizorul sau potențialul furnizor și implementatorul sau potențialul implementator 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, precum și al dreptului intern;

(i) subiecții testării în condiții reale și-au dat consimțământul în cunoștință de cauză în conformitate cu articolul 61 sau, în cazul aplicării legii, în cazul în care solicitarea consimțământului în cunoștință de cauză ar împiedica testarea sistemului de IA, testarea în sine și rezultatul testării în condiții reale nu au niciun efect negativ asupra subiecților, iar datele cu caracter personal ale acestora se șterg după efectuarea testării;

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

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

(5) Orice subiecți ai testării în condiții reale sau reprezentanții lor desemnați legal, după caz, se pot retrage din testare în orice moment, fără vreun prejudiciu și fără a trebui să prezinte vreo justificare, prin revocarea consimțământului lor în cunoștință de cauză și pot solicita ștergerea imediată și permanentă a datelor lor cu caracter personal. Retragerea consimțământului în cunoștință de cauză nu afectează activitățile deja desfășurate.

(6) În conformitate cu articolul 75, statele membre conferă autorităților lor de supraveghere a pieței competența de a solicita informații furnizorilor și potențialilor furnizori, de a efectua inspecții neanunțate la distanță sau la fața locului și de a efectua verificări privind efectuarea testării în condiții reale și a sistemelor de IA cu grad ridicat de risc conexe. Autoritățile de supraveghere a pieței fac uz de aceste competențe pentru a asigura o dezvoltare în condiții de siguranță a testării în condiții reale.

(7) Orice incident grav identificat în cursul testării în condiții reale se raportează autorității naționale de supraveghere a pieței în conformitate cu articolul 73. 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.

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

(9) Furnizorul sau potențialul furnizor este responsabil, în temeiul dreptului aplicabil al Uniunii și al dreptului intern în materie de răspundere, pentru orice prejudiciu cauzat în cursul testării în condiții reale pe care o efectuează.

Articolul 61

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

(1) În scopul testării în condiții reale în conformitate cu articolul 60, consimțământul în cunoștință de cauză acordat în mod liber se obține de la subiecții testării înainte de participarea lor la o astfel de testare și după ce au fost informați în mod corespunzător cu informații concise, clare, relevante și inteligibile cu privire la:

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

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

(c) drepturile lor și garanțiile cu privire la participarea lor, în special dreptul lor 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 nevoiți să prezinte vreo justificare;

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

(e) numărul unic de identificare la nivelul întregii Uniuni al testării în condiții reale în conformitate cu articolul 60 alineatul (4) litera (c) 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 se datează și se documentează, iar o copie se înmânează subiecților testării sau reprezentanților lor legali.

Articolul 62

Măsuri pentru furnizori și implementatori, în special IMM-uri, inclusiv întreprinderi nou-înființate

(1) Statele membre întreprind următoarele acțiuni:

(a) oferă IMM-urilor, inclusiv întreprinderilor nou-înființate, care au un sediu social sau o sucursală în Uniune, acces prioritar la spațiile de testare în materie de reglementare în domeniul IA, în măsura în care îndeplinesc condițiile de eligibilitate și criteriile de selecție; accesul prioritar nu împiedică accesul altor IMM-uri, inclusiv întreprinderi nou-înființate, altele decât cele menționate la prezentul alineat, la spațiile de testare în materie de reglementare în domeniul IA, cu condiția ca acestea să îndeplinească de asemenea condițiile de eligibilitate și criteriile 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, ale implementatorilor și, după caz, ale autorităților publice locale;

(c) utilizează canalele specifice existente și, după caz, stabilesc altele noi pentru comunicarea cu IMM-urile, inclusiv cu întreprinderile nou-înființate, cu implementatorii, cu alți inovatori 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 în domeniul IA;

(d) facilitează participarea IMM-urilor și a altor părți interesate relevante la procesul de dezvoltare a standardizării.

(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 dimensiunile acestora, cu dimensiunea pieței și cu alți indicatori relevanți.

(3) Oficiul pentru IA întreprinde următoarele acțiuni:

(a) furnizează modele standardizate pentru domeniile vizate de prezentul regulament, astfel cum specifică comitetul în cererea sa;

(b) dezvoltă și menține o platformă unică de informare 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 bunelor practici în procedurile de achiziții publice în ceea ce privește sistemele de IA.

Articolul 63

Derogări pentru operatori specifici

(1) Microîntreprinderile în sensul Recomandării 2003/361/CE pot respecta anumite elemente ale sistemului de management al calității prevăzut la articolul 17 din prezentul regulament într-un mod simplificat, cu condiția să nu aibă întreprinderi partenere sau întreprinderi afiliate în sensul recomandării respective. În acest scop, Comisia elaborează orientări privind elementele sistemului de management al calității care pot fi respectate într-un mod simplificat, având în vedere nevoile microîntreprinderilor, fără a afecta nivelul de protecție sau necesitatea respectării cerințelor în ceea ce privește sistemele de IA cu grad ridicat de risc.

(2) Alineatul (1) de la prezentul articol nu se interpretează ca o exceptare a operatorilor respectivi de la îndeplinirea oricăror alte cerințe sau obligații prevăzute în prezentul regulament, inclusiv cele stabilite la articolele 9, 10, 11, 12, 13, 14, 15, 72 și 73.

Capitolul VII
Guvernanța

SECȚIUNEA 1
GUVERNANȚA LA NIVELUL UNIUNII

Articolul 64

Oficiul pentru IA

(1) Comisia dezvoltă cunoștințele de specialitate și capabilitățile Uniunii în domeniul IA prin intermediul Oficiului pentru IA.

(2) Statele membre facilitează sarcinile încredințate Oficiului pentru IA, astfel cum sunt reflectate în prezentul regulament.

Articolul 65

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. Oficiul pentru IA 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 prezintă relevanță pentru acestea.

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

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

(a) dețin competențele și prerogativele relevante în statul lor membru, astfel încât să contribuie în mod activ la îndeplinirea sarcinilor comitetului menționate la articolul 66;

(b) 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;

(c) 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.

(5) 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 detaliate pentru votare și organizarea activităților comitetului și a celor ale subgrupurilor acestuia.

(6) 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.

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.

Comitetul poate înființa alte subgrupuri permanente sau temporare, după caz, în scopul examinării unor chestiuni specifice. După caz, reprezentanții Forumului consultativ menționat la articolul 67 pot fi invitați la astfel de subgrupuri sau la reuniuni specifice ale subgrupurilor respective în calitate de observatori.

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

(8) Comitetul este prezidat de către unul dintre reprezentanții statelor membre.
Oficiul pentru IA asigură secretariatul pentru comitet, convoacă reuniunile la cererea președintelui și pregătește ordinea de zi în conformitate cu sarcinile care îi revin comitetului în temeiul prezentului regulament și al regulamentului său de procedură.

Articolul 66

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) să contribuie la coordonarea între autoritățile naționale competente responsabile cu aplicarea prezentului regulament și, în cooperare cu autoritățile de supraveghere a pieței în cauză și sub rezerva acordului acestora, să sprijine activitățile comune ale autorităților de supraveghere a pieței menționate la articolul 74 alineatul (11);

(b) să colecteze și să disemineze în rândul statelor membre cunoștințe de specialitate tehnice și în materie de reglementare și de bune practici;

(c) să ofere consiliere privind punerea în aplicare a prezentului regulament, în special în ceea ce privește aplicarea normelor privind modelele de IA de uz general;

(d) să contribuie la armonizarea practicilor administrative din statele membre, inclusiv în ceea ce privește derogarea de la procedurile de evaluare a conformității menționate la articolul 46, funcționarea spațiilor de testare în materie de reglementare în domeniul IA și testarea în condiții reale menționate la articolele 57, 59 și 60;

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

(i) elaborarea și aplicarea codurilor de conduită și a codurilor de bune practici în temeiul prezentului regulament, precum și al orientărilor Comisiei;

(ii) evaluarea și revizuirea prezentului regulament în temeiul articolului 112, inclusiv în ceea ce privește rapoartele privind incidentele grave menționate la articolul 73 și funcționarea bazei de date a UE menționate la articolul 71, pregătirea actelor delegate sau de punere în aplicare și în ceea ce privește posibilele alinieri ale prezentului regulament la legislația de armonizare a Uniunii enumerată în anexa I;

(iii) specificațiile tehnice sau standardele existente referitoare la cerințele prevăzute în capitolul III secțiunea 2;

(iv) utilizarea standardelor armonizate sau a specificațiilor comune menționate la articolele 40 și 41;

(v) tendințele în aspecte precum competitivitatea europeană la nivel mondial în domeniul IA, adoptarea IA în Uniune și dezvoltarea competențelor digitale;

(vi) tendințele în ceea ce privește tipologia în continuă evoluție a lanțurilor valorice ale IA, în special referitor la implicațiile rezultate în ceea ce privește responsabilitatea;

(vii) eventuala necesitate de modificare a anexei III în conformitate cu articolul 7 și privind eventuala necesitate de a revizui articolul 5 în temeiul articolului 112, ținând seama de dovezile relevante disponibile și de cele mai recente evoluții tehnologice;

(f) să sprijine Comisia în promovarea alfabetizării în domeniul IA, a acțiunilor de sensibilizare și de înțelegere în rândul publicului a beneficiilor, riscurilor, garanțiilor și drepturilor și obligațiilor legate de utilizarea sistemelor de IA;

(g) să faciliteze elaborarea unor criterii comune și a unei înțelegeri comune între operatorii de pe piață și autoritățile competente a conceptelor relevante prevăzute în prezentul regulament, inclusiv prin contribuirea la elaborarea de criterii de referință;

(h) să coopereze, după caz, cu alte instituții, organe, oficii și agenții relevante ale Uniunii, precum și cu grupuri de experți și rețelele relevante ale Uniunii, în special în domeniul siguranței produselor, al securității cibernetice, al concurenței, al serviciilor digitale și media, al serviciilor financiare, al protecției consumatorilor, al protecției datelor și a drepturilor fundamentale;

(i) să contribuie la cooperarea eficace cu autoritățile competente din țările terțe și cu organizațiile internaționale;

(j) să sprijine autoritățile naționale competente și Comisia în dezvoltarea cunoștințelor de specialitate organizaționale și tehnice necesare pentru punerea în aplicare a prezentului regulament, inclusiv prin contribuirea la evaluarea nevoilor de formare pentru personalul statelor membre implicat în punerea în aplicare a prezentului regulament;

(k) să sprijine Oficiul pentru IA în acordarea de asistență autorităților naționale competente pentru crearea și dezvoltarea de spații de testare în materie de reglementare în domeniul IA și să faciliteze cooperarea și schimbul de informații între spațiile de testare în materie de reglementare în domeniul IA;

(l) să contribuie la elaborarea documentelor de orientare și să ofere consiliere relevantă cu privire la aceasta;

(m) să consilieze Comisia în legătură cu chestiuni internaționale privind IA;

(n) să furnizeze Comisiei avize cu privire la alertele calificate referitoare la modelele de IA de uz general;

(o) să primească opinii din partea statelor membre cu privire la alertele calificate referitoare la modelele de IA de uz general și la experiențele și practicile naționale privind monitorizarea sistemelor de IA și aplicarea normelor referitoare la acestea, îndeosebi sistemele care integrează modelele de IA de uz general.

Articolul 67

Forumul consultativ

(1) Se instituie un forum consultativ pentru a furniza cunoștințe de specialitate tehnice comitetului și Comisiei și pentru a le consilia, precum și pentru a contribui la sarcinile care le revin în temeiul prezentului regulament.

(2) Componența Forumului consultativ reprezintă o selecție echilibrată a părților interesate, inclusiv a sectorului, a întreprinderilor nou-înființate, a IMM-urilor, a societății civile și a mediului academic. Componența Forumului consultativ este echilibrată între interesele comerciale și necomerciale și, în cadrul categoriei intereselor comerciale, în ceea ce privește IMM-urile și alte întreprinderi.

(3) Comisia numește membrii Forumului consultativ, în conformitate cu criteriile stabilite la alineatul (2), din rândul părților interesate cu cunoștințe de specialitate recunoscute în domeniul IA.

(4) Mandatul membrilor Forumului consultativ este de doi ani și poate fi prelungit cu cel mult patru ani.

(5) Agenția pentru Drepturi Fundamentale a Uniunii Europene, ENISA, Comitetul European de Standardizare (CEN), Comitetul European de Standardizare în Electrotehnică (CENELEC) și Institutul European de Standardizare în Telecomunicații (ETSI) sunt membri permanenți ai Forumului consultativ.

(6) Forumul consultativ își stabilește regulamentul de procedură. Acesta alege doi copreședinți dintre membrii săi, în conformitate cu criteriile stabilite la alineatul (2). Mandatul copreședinților este de doi ani, reînnoibil o singură dată.

(7) Forumul consultativ organizează reuniuni de cel puțin două ori pe an. Forumul consultativ poate invita experți și alte părți interesate la reuniunile sale.

(8) Forumul consultativ poate elabora avize, recomandări și contribuții scrise la cererea comitetului sau a Comisiei.

(9) Forumul consultativ poate institui subgrupuri permanente sau temporare, după caz, în scopul examinării unor chestiuni specifice legate de obiectivele prezentului regulament.

(10) Forumul consultativ întocmește un raport anual privind activitățile sale. Raportul respectiv este pus la dispoziția publicului.

Articolul 68

Grupul științific de experți independenți

(1) Comisia, prin intermediul unui act de punere în aplicare, adoptă dispoziții privind instituirea unui grup științific de experți independenți (denumit în continuare „grupul științific”) menit să sprijine activitățile de aplicare a legii în temeiul prezentului regulament. Actul de punere în aplicare respectiv se adoptă în conformitate cu procedura de examinare menționată la articolul 98 alineatul (2).

(2) Grupul științific este alcătuit din experți independenți selectați de Comisie pe baza cunoștințelor de specialitate științifice sau tehnice la zi în domeniul IA, necesare pentru îndeplinirea sarcinilor prevăzute la alineatul (3), și este în măsură să demonstreze îndeplinirea tuturor condițiilor următoare:

(a) să dispună de cunoștințe de specialitate și competențe specifice și cunoștințe de specialitate științifice și tehnice în domeniul IA;

(b) să fie independent față de orice furnizor de sisteme de IA sau de modele de IA de uz general;

(c) să aibă capacitatea de a desfășura activități cu diligență, acuratețe și obiectivitate.

Comisia, în consultare cu Comitetul pentru IA, stabilește numărul de experți din grup în funcție de necesități și asigură o reprezentare geografică și de gen echitabilă.

(3) Grupul științific consiliază și sprijină Oficiul pentru IA, în special în ceea ce privește următoarele sarcini:

(a) sprijinirea punerii în aplicare și a respectării prezentului regulament, în ceea ce privește modelele și sistemele de IA de uz general, îndeosebi prin:

(i) alertarea Oficiului pentru IA cu privire la posibile riscuri sistemice la nivelul Uniunii prezentate de modele de IA de uz general, în conformitate cu articolul 90;

(ii) contribuirea la dezvoltarea instrumentelor și metodologiilor de evaluare a capabilităților modelelor și sistemelor de IA de uz general, inclusiv prin valori de referință;

(iii) furnizarea de consiliere cu privire la clasificarea sistemelor de IA de uz general cu risc sistemic;

(iv) furnizarea de consiliere cu privire la clasificarea diverselor modele și sisteme de IA de uz general;

(v) contribuirea la dezvoltarea de instrumente și modele;

(b) sprijinirea activității autorităților de supraveghere a pieței, la cererea acestora;

(c) sprijinirea activităților transfrontaliere în materie de supraveghere a pieței menționate la articolul 74 alineatul (11), fără a aduce atingere competențelor autorităților de supraveghere a pieței;

(d) sprijinirea Oficiului pentru IA în îndeplinirea sarcinilor sale în contextul procedurii de salvgardare a Uniunii în temeiul articolului 81.

(4) Experții din cadrul grupului științific își îndeplinesc sarcinile cu imparțialitate și obiectivitate și asigură confidențialitatea informațiilor și a datelor obținute în cursul îndeplinirii sarcinilor și activităților lor. Aceștia nu solicită și nici nu acceptă instrucțiuni de la nicio persoană atunci când își exercită atribuțiile în temeiul alineatului (3). Fiecare expert întocmește o declarație de interese, care este pusă la dispoziția publicului. Oficiul pentru IA instituie sisteme și proceduri pentru a gestiona în mod activ și pentru a preveni potențialele conflicte de interese.

(5) Actul de punere în aplicare menționat la alineatul (1) include dispoziții privind condițiile, procedurile și modalitățile detaliate pentru emiterea de alerte de către grupul științific și membrii săi și pentru solicitarea de către aceștia de asistență din partea Oficiului pentru IA în îndeplinirea sarcinilor grupului științific.

Articolul 69

Accesul statelor membre la grupul de experți

(1) Statele membre pot apela la experți din cadrul grupului științific pentru sprijinirea activităților lor de aplicare a legii în temeiul prezentului regulament.

(2) Statele membre pot fi obligate să plătească taxe pentru consilierea și sprijinul furnizate de experți. Structura și nivelul taxelor, precum și amploarea și structura costurilor recuperabile sunt stabilite în actul de punere în aplicare menționat la articolul 68 alineatul (1), ținând seama de obiectivele punerii în aplicare adecvate a prezentului regulament, de raportul cost-eficacitate și de necesitatea de a asigura pentru toate statele membre accesul efectiv la experți.

(3) Comisia facilitează accesul în timp util al statelor membre la experți, după caz, și se asigură că combinarea activităților de sprijin desfășurate de structurile de sprijin pentru testarea IA ale Uniunii în temeiul articolului 84 și de experți în temeiul prezentului articol este organizată în mod eficient și oferă cea mai bună valoare adăugată posibilă.

SECȚIUNEA 2

AUTORITĂȚILE NAȚIONALE COMPETENTE

Articolul 70

Desemnarea autorităților naționale competente și a punctelor unice de contact

(1) Fiecare stat membru stabilește sau desemnează drept autorități naționale competente cel puțin o autoritate de notificare și cel puțin o autoritate de supraveghere a pieței în sensul prezentului regulament. Respectivele autorități naționale competente își exercită competențele în mod independent, imparțial și fără prejudecăți, astfel încât să garanteze obiectivitatea activităților și sarcinilor lor și să asigure punerea în aplicare a prezentului regulament. Membrii acestor autorități se abțin de la orice act incompatibil cu atribuțiile 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.

(2) Statele membre îi comunică Comisiei identitatea autorităților de notificare și a autorităților de supraveghere a pieței și sarcinile acestor autorități, precum și orice modificări ulterioare ale acestora. Până la ... [12 luni de la data intrării în vigoare a prezentului regulament], statele membre pun la dispoziția publicului informații cu privire la modul în care pot fi contactate autoritățile competente și punctele unice de contact, prin mijloace de comunicare electronică. Statele membre desemnează o autoritate de supraveghere a pieței care să acționeze ca punct unic de contact pentru prezentul regulament și îi notifică Comisiei identitatea punctului unic de contact. Comisia pune la dispoziția publicului o listă a punctelor unice de contact.

(3) Statele membre se asigură că autoritățile lor naționale competente dispun de resurse tehnice, financiare și umane adecvate și de infrastructură pentru a-și îndeplini cu eficacitate sarcinile care le revin în temeiul prezentului regulament. În special, autoritățile naționale competente dispun în permanență de un personal suficient ale cărui competențe și cunoștințe de specialitate includ o înțelegere aprofundată a tehnologiilor din domeniul IA, a datelor și a prelucrării de date, a protecției datelor cu caracter personal, a securității cibernetice, a drepturilor fundamentale, a riscurilor în materie de sănătate și siguranță, precum și cunoașterea standardelor și a cerințelor legale existente. Statele membre evaluează și, dacă este necesar, actualizează anual competențele și resursele necesare menționate la prezentul alineat.

(4) Autoritățile naționale competente iau măsuri corespunzătoare pentru a asigura un nivel de securitate cibernetică adecvat.

(5) Atunci când își îndeplinesc sarcinile, autoritățile naționale competente acționează în conformitate cu obligațiile de confidențialitate prevăzute la articolul 78.

(6) Până la ... [un an de la data intrării în vigoare a prezentului regulament] și, ulterior, la fiecare doi ani, statele membre îi prezintă Comisiei un raport privind situația resurselor financiare și umane ale autorităților naționale competente, împreună cu o evaluare a adecvării acestora. Comisia transmite aceste informații comitetului pentru a fi discutate și pentru a formula eventuale recomandări.

(7) Comisia facilitează schimbul de experiență între autoritățile naționale competente.

(8) Autoritățile naționale competente pot oferi orientări și consiliere cu privire la punerea în aplicare a prezentului regulament, îndeosebi IMM-urilor, inclusiv întreprinderilor nou-înființate, luând în considerare orientările și consilierea furnizate de comitet și de Comisie, după caz. 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 actelor legislative respective ale Uniunii sunt consultate, după caz.

(9) Atunci când instituțiile, organele, oficiile sau agențiile Uniunii intră în domeniul de aplicare al prezentului regulament, Autoritatea Europeană pentru Protecția Datelor acționează ca autoritate competentă pentru supravegherea lor.

Capitolul VIII

Baza de date a UE pentru sisteme de ia cu grad ridicat de risc

Articolul 71

Baza de date a UE pentru sisteme 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 alineatele (2) și (3) de la prezentul articol privind sistemele de IA cu grad ridicat de risc menționate la articolul 6 alineatul (2) care sunt înregistrate în conformitate cu articolele 49 și 60 și sistemele de IA care nu sunt considerate ca având un grad ridicat de risc în temeiul articolului 6 alineatul (3) și care sunt înregistrate în conformitate cu articolul 6 alineatul (4) și cu articolul 49. Atunci când stabilește specificațiile funcționale ale respectivei baze de date, Comisia consultă experții relevanți, iar atunci când actualizează specificațiile funcționale ale respectivei baze de date, Comisia consultă comitetul.

(2) Datele enumerate în secțiunile A și B din anexa VIII se introduc în baza de date a UE de către furnizor sau, după caz, de către reprezentantul autorizat**.**

(3) Datele enumerate în secțiunea C din anexa VIII se introduc în baza de date a UE de către implementatorul care este o autoritate publică, o agenție sau un organ ori care acționează în numele acestora, în conformitate cu articolul 49 alineatele (3) și (4).

(4) Cu excepția secțiunii menționate la articolul 49 alineatul (4) și la articolul 60 alineatul (4) litera (c), informațiile conținute în baza de date a UE înregistrate în conformitate cu articolul 49 sunt accesibile și puse la dispoziția publicului într-un mod ușor de utilizat. Informațiile ar trebui să fie ușor de navigat și prelucrabile automat. Informațiile înregistrate în conformitate cu articolul 60 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 puse și la dispoziția publicului.

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

(6) Comisia este operatorul bazei de date a UE. Aceasta pune la dispoziția furnizorilor, a potențialilor furnizori și a implementatorilor sprijin tehnic și administrativ adecvat. Baza de date a UE respectă cerințele de accesibilitate aplicabile.

Capitolul IX
Monitorizarea ulterioară introducerii pe piață, schimbul de informații și supravegherea pieței

SECȚIUNEA 1
MONITORIZAREA ULTERIOARĂ INTRODUCERII PE PIAȚĂ

Articolul 72

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

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

(2) Sistemul de monitorizare ulterioară introducerii pe piață colectează, documentează și analizează în mod activ și sistematic datele relevante care pot fi furnizate de implementatori sau pot fi colectate din alte surse cu privire la performanța sistemelor de IA cu grad ridicat de risc pe toată durata lor de viață și care permit furnizorului să evalueze conformitatea continuă a sistemelor de IA cu cerințele prevăzute în capitolul III secțiunea 2. După caz, monitorizarea ulterioară introducerii pe piață include o analiză a interacțiunii cu alte sisteme de IA. Această obligație nu acoperă datele operaționale sensibile ale implementatorilor 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 stabilire a unui model de plan de monitorizare ulterioară introducerii pe piață și a listei elementelor care trebuie incluse în plan până la ... [18 luni de la data intrării în vigoare a prezentului regulament]. Actul de punere în aplicare respectiv se adoptă în conformitate cu procedura de examinare menționată la articolul 98 alineatul (2).

(4) Pentru sistemele de IA cu grad ridicat de risc reglementate de actele legislative de armonizare ale Uniunii menționate în secțiunea A din anexa I, în cazul în care un sistem și un plan de monitorizare ulterioară introducerii pe piață sunt deja instituite în temeiul legislației respective, pentru a asigura coerența, a evita suprapunerile și a reduce la minimum sarcinile suplimentare, furnizorii au posibilitatea de a integra, după caz, elementele necesare descrise la alineatele (1), (2) și (3), utilizând modelul menționat la alineatul (3), în sistemele și planurile deja existente în temeiul legislației respective, cu condiția ca astfel să atingă un nivel de protecție echivalent.

Primul paragraf de la prezentul alineat 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 dreptului Uniunii din domeniul serviciilor financiare.

SECȚIUNEA 2

SCHIMBUL DE INFORMAȚII PRIVIND INCIDENTELE GRAVE

Articolul 73

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.

(2) Raportul menționat la alineatul (1) 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 sau, după caz, implementatorul a luat cunoștință de incidentul grav.

Termenul pentru raportarea menționată la primul paragraf ține seama de gravitatea incidentului grav.

(3) În pofida alineatului (2) de la prezentul articol, în cazul unei încălcări pe scară largă sau al unui incident grav, astfel cum sunt definite la articolul 3 punctul 49 litera (b), raportul menționat la alineatul (1) de la prezentul articol se furnizează imediat și în termen de cel mult două zile de la data la care furnizorul sau, după caz, implementatorul a luat cunoștință de incidentul respectiv.

(4) În pofida alineatului (2), în caz de deces al unei persoane, raportul se pune la dispoziție imediat după ce furnizorul sau implementatorul a stabilit sau de îndată ce suspectează o legătură de cauzalitate între sistemul de IA cu grad ridicat de risc și incidentul grav, dar nu mai târziu de 10 zile de la data la care furnizorul sau, după caz, implementatorul a luat cunoștință de incidentul grav.

(5) Dacă este necesar pentru a asigura raportarea în timp util, furnizorul sau, după caz, implementatorul poate prezenta un raport inițial care este incomplet, urmat de un raport complet.

(6) În urma raportării unui incident grav în temeiul alineatului (1), furnizorul efectuează, fără întârziere, investigațiile necesare cu privire la incidentul grav și la sistemul de IA în cauză. Acest lucru include o evaluare a riscurilor incidentului și măsuri corective.

În cursul investigațiilor menționate la primul paragraf, furnizorul cooperează cu autoritățile competente și, după caz, cu organismul notificat în cauză și nu efectuează nicio investigație care presupune modificarea sistemului de IA în cauză într-un mod care poate afecta orice evaluare ulterioară a cauzelor incidentului, înainte de a informa autoritățile competente în legătură cu o astfel de acțiune.

(7) La primirea unei notificări referitoare la un incident grav menționat la articolul 3 punctul 49 litera (c), autoritatea relevantă de supraveghere a pieței informează autoritățile sau organismele publice naționale menționate la articolul 77 alineatul (1). Comisia elaborează orientări specifice pentru a facilita respectarea obligațiilor prevăzute la alineatul (1) de la prezentul articol. Orientările respective se emit până la ... [12 luni de la data intrării în vigoare a prezentului regulament] și se evaluează periodic.

(8) Autoritatea de supraveghere a pieței ia măsurile corespunzătoare, astfel cum se prevede la articolul 19 din Regulamentul (UE) 2019/1020, în termen de șapte de zile de la data la care a primit notificarea menționată la alineatul (1) de la prezentul articol și urmează procedurile de notificare prevăzute în respectivul regulament.

(9) În cazul sistemelor de IA cu grad ridicat de risc menționate în anexa III care sunt introduse pe piață sau puse în funcțiune de furnizori care fac obiectul unor instrumente legislative ale Uniunii care prevăd obligații de raportare echivalente cu cele prevăzute în prezentul regulament, notificarea incidentelor grave se limitează la cele menționate la articolul 3 punctul 49 litera (c).

(10) În cazul sistemelor de IA cu grad ridicat de risc care sunt componente de siguranță ale unor dispozitive sau sunt ele însele dispozitive care fac obiectul Regulamentelor (UE) 2017/745 și (UE) 2017/746, notificarea incidentelor grave se limitează la cele menționate la articolul 3 punctul 49 litera (c) din prezentul regulament și se efectuează către autoritatea națională competentă aleasă în acest scop de statele membre în care s-a produs incidentul respectiv.

(11) Autoritățile naționale competente îi notifică imediat Comisiei orice incident grav, indiferent dacă au luat sau nu măsuri cu privire la acesta, în conformitate cu articolul 20 din Regulamentul (UE) 2019/1020.

SECȚIUNEA 3

APLICAREA LEGII

Articolul 74

Supravegherea pieței și controlul sistemelor de IA pe piața Uniunii

(1) Regulamentul (UE) 2019/1020 se aplică sistemelor de IA care intră sub incidența prezentului regulament. În scopul asigurării efective a respectării 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 alineatul (1) 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 lor de raportare în temeiul articolului 34 alineatul (4) din Regulamentul (UE) 2019/1020, autoritățile de supraveghere a pieței raportează anual Comisiei și autorităților naționale de concurență relevante toate informațiile identificate în cursul activităților de supraveghere a pieței care ar putea prezenta un potențial interes pentru aplicarea dreptului Uniunii privind normele în materie de concurență. De asemenea, acestea raportează anual Comisiei despre utilizarea practicilor interzise care a avut loc în anul respectiv și despre măsurile luate.

(3) În cazul sistemelor de IA cu grad ridicat de risc legate de produse reglementate de actele legislative de armonizare ale Uniunii enumerate în secțiunea A din anexa I, autoritatea de supraveghere a pieței în sensul prezentului regulament este autoritatea responsabilă cu activitățile de supraveghere a pieței desemnată în temeiul respectivelor acte legislative.

Prin derogare de la primul paragraf și în circumstanțe corespunzătoare, statele membre pot desemna o altă autoritate relevantă care să acționeze în calitate de autoritate de supraveghere a pieței, cu condiția ca acestea să asigure coordonarea cu autoritățile sectoriale relevante de supraveghere a pieței responsabile cu aplicarea legislației de armonizare a Uniunii enumerate în anexa I.

(4) Procedurile menționate la articolele 79-83 din prezentul regulament nu se aplică sistemelor de IA legate de produse reglementate de actele legislative de armonizare ale Uniunii enumerate în secțiunea A din anexa I, atunci când respectivele acte juridice prevăd deja proceduri care asigură un nivel de protecție echivalent și care au același obiectiv. În astfel de cazuri, se aplică în schimb procedurile sectoriale relevante.

(5) Fără a aduce atingere competențelor autorităților de supraveghere a pieței în temeiul articolului 14 din Regulamentul (UE) 2019/1020, în scopul aplicării efective a prezentului regulament, autoritățile de supraveghere a pieței pot exercita de la distanță competențele menționate la articolul 14 alineatul (4) literele (d) și (j) din respectivul regulament, după caz.

(6) Pentru sistemele de IA cu grad ridicat de risc introduse pe piață, puse în funcțiune sau utilizate de instituțiile financiare reglementate de dreptul Uniunii din domeniul serviciilor 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.

(7) Prin derogare de la alineatul (6), 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 instituit prin Regulamentul (UE) nr. 1024/2013, ar trebui să raporteze fără întârziere Băncii Centrale Europene orice informație identificată 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.

(8) Pentru sistemele de IA cu grad ridicat de risc enumerate la punctul 1 din anexa III la prezentul regulament, în măsura în care sistemele sunt utilizate în scopul aplicării legii, al gestionării frontierelor și al respectării justiției și democrației, și pentru sistemele de IA cu grad ridicat de risc enumerate la punctele 6, 7 și 8 din anexa III la prezentul regulament, statele membre desemnează drept autorități de supraveghere a pieței în sensul prezentului regulament fie autoritățile competente de supraveghere a protecției datelor în temeiul Regulamentului (UE) 2016/679 sau al Directivei (UE) 2016/680, fie orice alte autorități desemnate în temeiul aceloraşi condiții prevăzute la articolele 41-44 din Directiva (UE) 2016/680. 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.

(9) În cazul în care instituții, organe, oficii sau agenții ale Uniunii intră în domeniul de aplicare al prezentului regulament, Autoritatea Europeană pentru Protecția Datelor acționează în calitate de autoritate de supraveghere a pieței pentru acestea, cu excepția cazurilor în care Curtea de Justiție a Uniunii Europene acționează în exercițiul funcției sale judiciare.

(10) 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 actelor legislative de armonizare ale Uniunii enumerate în anexa I sau în alte acte legislative ale Uniunii care ar putea fi relevante pentru sistemele de IA cu grad ridicat de risc menționate în anexa III.

(11) Autoritățile de supraveghere a pieței și Comisia sunt în măsură să propună activități comune, inclusiv investigații comune, care să fie efectuate fie de autoritățile de supraveghere a pieței, fie de autoritățile de supraveghere a pieței în colaborare cu Comisia și care au scopul de a promova conformitatea, de a identifica cazurile de neconformitate, de a sensibiliza sau de a oferi orientări în legătură cu prezentul regulament în ceea ce privește anumite categorii de sisteme de IA cu grad ridicat de risc despre care se constată că prezintă un risc grav în două sau mai multe state membre, în conformitate cu articolul 9 din Regulamentul (UE) 2019/1020. Oficiul pentru IA oferă sprijin în materie de coordonare pentru investigațiile comune.

(12) 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, furnizorii 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 sistemelor de IA cu grad ridicat de risc, inclusiv, după caz 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.

(13) 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 ambele condiții următoare:

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

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

(14) Orice informații sau documentație obținute de autoritățile de supraveghere a pieței în temeiul prezentului articol sunt tratate în conformitate cu obligațiile de confidențialitate prevăzute la articolul 78.

Articolul 75

Asistența reciprocă, supravegherea pieței și controlul sistemelor de IA de uz general

(1) În cazul în care un sistem de IA se bazează pe un model de IA de uz general, iar modelul și sistemul sunt dezvoltate de același furnizor, Oficiul pentru IA are competența de a monitoriza și de a supraveghea conformitatea respectivului sistem de IA cu obligațiile impuse în temeiul prezentului regulament. Pentru a își îndeplini sarcinile de monitorizare și supraveghere, Oficiul pentru IA are toate competențele unei autorități de supraveghere a pieței prevăzute în prezenta secțiune și în Regulamentul (UE) 2019/1020.

(2) În cazul în care au motive suficiente să considere că sisteme de IA de uz general care pot fi utilizate direct de către implementatori pentru cel puțin un scop clasificat ca prezentând un grad ridicat de risc în temeiul prezentului regulament nu respectă cerințele prevăzute în prezentul regulament, autoritățile relevante de supraveghere a pieței cooperează cu Oficiul pentru IA pentru a efectua evaluări ale conformității și informează în consecință comitetul și alte autorități de supraveghere a pieței.

(3) Dacă o autoritate de supraveghere a pieței nu este în măsură să își încheie investigația privind sistemul de IA cu grad ridicat de risc din cauza incapacității sale de a accesa anumite informații legate de modelul de IA de uz general, în pofida faptului că a depus toate eforturile adecvate pentru a obține informațiile respective, aceasta poate transmite Oficiului pentru IA o cerere motivată prin care accesul la respectivele informații este impus. În acest caz, Oficiul pentru IA îi furnizează autorității solicitante fără întârziere și, în orice caz, în termen de 30 de zile toate informațiile pe care Oficiul pentru IA le consideră relevante pentru a stabili dacă un sistem de IA cu grad ridicat de risc este neconform. Autoritățile de supraveghere a pieței garantează confidențialitatea informațiilor pe care le obțin în conformitate cu articolul 78 din prezentul regulament. Procedura prevăzută în capitolul VI din Regulamentul (UE) 2019/1020 se aplică *mutatis mutandis*.

Articolul 76

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

(1) Autoritățile de supraveghere a pieței dețin competențele 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 sisteme de IA care sunt supravegheate într-un spațiu de testare în materie de reglementare în domeniul IA în temeiul articolului 58, autoritățile de supraveghere a pieței verifică conformitatea cu articolul 60 ca parte a rolului lor de supraveghere pentru spațiul de testare în materie de reglementare în domeniul 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 60 alineatul (4) literele (f) și (g).

(3) În cazul în care o autoritate de supraveghere a pieței a fost informată de către potențialul furnizor, de către furnizor sau de către orice parte terță despre un incident grav sau are alte motive pentru a considera că nu sunt îndeplinite condițiile prevăzute la articolele 60 și 61, aceasta poate lua oricare dintre următoarele decizii pe teritoriul său, după caz:

(a) suspendarea sau încetarea testării în condiții reale;

(b) solicitarea furnizorului sau a potențialului furnizor și a implementatorului sau a potențialului implementator 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) de la prezentul articol sau a emis o obiecție în sensul articolului 60 alineatul (4) litera (b), decizia sau obiecția indică motivele care stau la baza acesteia, precum și modul în care furnizorul sau potențialul furnizor poate contesta decizia sau obiecția.

(5) După caz, dacă o autoritate de supraveghere a pieței a luat o decizie menționată la alineatul (3), 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 77

Competențele autorităților care protejează drepturile fundamentale

(1) 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 într-un limbaj și un format accesibil, atunci când accesul la documentația respectivă este necesar pentru îndeplinirea cu eficacitate a mandatelor lor, în limitele jurisdicției lor. Autoritatea sau organismul public competent informează autoritatea de supraveghere a pieței din statul membru în cauză cu privire la orice astfel de cerere.

(2) Până la ... [trei luni de la data intrării în vigoare a prezentului regulament], fiecare stat membru identifică autoritățile sau organismele publice menționate la alineatul (1) și pune o listă a acestora la dispoziția publicului. Statele membre îi notifică lista Comisiei și celorlalte state membre și o mențin la zi.

(3) În cazul în care documentația menționată la alineatul (1) este insuficientă pentru a stabili dacă a avut loc sau nu o încălcare a obligațiilor în temeiul dreptului Uniunii care protejează drepturile fundamentale, autoritatea sau organismul public menționat la alineatul (1) 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.

(4) Toate informațiile și documentele obținute de autoritățile sau organismele publice naționale menționate la alineatul (1) de la prezentul articol în temeiul dispozițiilor prezentului articol sunt tratate în conformitate cu obligațiile de confidențialitate prevăzute la articolul 78.

Articolul 78

Confidențialitate

(1) Comisia, autoritățile de supraveghere a pieței și organismele notificate, precum și orice altă persoană fizică sau juridică implicată în aplicarea prezentului regulament respectă, în conformitate cu dreptul Uniunii sau cu dreptul intern, 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 (UE) 2016/943 a Parlamentului European și a Consiliului[57];

(b) punerea efectivă în aplicare a prezentului regulament, în special în scopul inspecțiilor, investigațiilor și auditurilor;

(c) interesele de securitate publică și națională;

(d) desfășurarea procedurilor penale sau administrative;

---

[57] Directiva (UE) 2016/943 a Parlamentului European și a Consiliului din 8 iunie 2016 privind protecția know-how-ului și a informațiilor de afaceri nedivulgate (secrete comerciale) împotriva dobândirii, utilizării și divulgării ilegale (JO L 157, 15.6.2016, p. 1).

(e) informațiile clasificate în temeiul dreptului Uniunii sau al dreptului intern.

(2) Autoritățile implicate în aplicarea prezentului regulament în temeiul alineatului (1) solicită numai datele care sunt strict necesare pentru evaluarea riscului prezentat de sistemele de IA și pentru exercitarea competențelor lor în conformitate cu prezentul regulament și cu Regulamentul (UE) 2019/1020. Acestea instituie măsuri de securitate cibernetică corespunzătoare și eficace pentru a proteja securitatea și confidențialitatea informațiilor și a datelor obținute și șterg datele colectate de îndată ce acestea nu mai sunt necesare în scopul pentru care au fost obținute, în conformitate cu dreptul Uniunii sau dreptul intern aplicabil.

(3) Fără a aduce atingere alineatelor (1) și (2), 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 implementatorului atunci când sistemele de IA cu grad ridicat de risc menționate la punctul 1, 6 sau 7 din anexa III sunt utilizate de autoritățile de aplicare a legii, de control la frontiere, de imigrație sau de azil și atunci când o astfel de divulgare ar pune în pericol interese de siguranță publică și de securitate națională. Acest schimb de informații nu acoperă datele operaționale sensibile legate de activitățile autorităților de aplicare a legii, de control la frontiere, de imigrație sau de azil.

În cazul în care autoritățile de aplicare a legii, de imigrație sau de azil sunt furnizori de sisteme de IA cu grad ridicat de risc menționate la punctul 1, 6 sau 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 74 alineatele (8) și (9), 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.

(4) Alineatele (1), (2) și (3) nu aduc atingere drepturilor și obligațiilor care revin Comisiei, statelor membre și autorităților relevante ale acestora, precum și celor care revin organismelor notificate cu privire la schimbul de informații și difuzarea avertizărilor, inclusiv în contextul cooperării transfrontaliere, și nu aduc atingere nici obligațiilor părților în cauză de a furniza informații în temeiul dreptului penal al statelor membre.

(5) Comisia și statele membre pot face schimb, atunci când este necesar și în conformitate cu dispozițiile relevante din acordurile internaționale și comerciale, de informații confidențiale cu autoritățile de reglementare din țări terțe cu care au încheiat acorduri de confidențialitate bilaterale sau multilaterale care garantează un nivel adecvat de confidențialitate.

Articolul 79

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

(1) Prin sisteme de IA care prezintă un risc se înțelege un „produs care prezintă un risc”, în sensul definiției de la articolul 3 punctul 19 din Regulamentul (UE) 2019/1020, în măsura în care prezintă riscuri pentru sănătatea sau siguranța ori 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) de la prezentul articol, 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. Se acordă o atenție deosebită sistemelor de IA care prezintă un risc pentru grupurile vulnerabile. Atunci când sunt identificate riscuri pentru drepturile fundamentale, autoritatea de supraveghere a pieței informează și autoritățile sau organismele publice naționale relevante menționate la articolul 77 alineatul (1) și cooperează pe deplin cu acestea. Operatorii relevanți cooperează, după caz, cu autoritatea de supraveghere a pieței și cu celelalte autorități sau organisme publice naționale menționate la articolul 77 alineatul (1).

În cazul în care, pe parcursul evaluării respective, autoritatea de supraveghere a pieței sau, după caz, autoritatea de supraveghere a pieței în cooperare cu autoritatea publică națională menționată la articolul 77 alineatul (1) 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 pe care autoritatea de supraveghere a pieței îl poate indica și, în orice caz, nu mai târziu de 15 zile lucrătoare sau astfel cum se prevede în actele legislative de armonizare relevante ale Uniunii.

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 de la prezentul alineat.

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

(4) Operatorul se asigură că sunt luate toate măsurile corective adecvate pentru toate sistemele de IA în cauză pe care acesta le-a pus la dispoziție pe piața Uniunii.

(5) În cazul în care operatorul unui sistem de IA nu ia măsurile 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 sau punerea acestuia în funcțiune, pentru a retrage produsul sau sistemul de IA de sine stătător de pe piața respectivă ori pentru a-l rechema. Autoritatea respectivă notifică fără întârzieri nejustificate Comisiei și celorlalte state membre măsurile respective.

(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 și lanțul de aprovizionare, natura neconformității invocate și riscul implicat, natura și durata măsurilor naționale luate, precum și argumentele prezentate de operatorul relevant. 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 IA menționate la articolul 5;

(b) nerespectarea de către sistemul de IA cu grad ridicat de risc a cerințelor prevăzute în capitolul III secțiunea 2;

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

(d) nerespectarea articolului 50.

(7) Autoritățile de supraveghere a pieței, 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 sistemului 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) de la prezentul articol, nicio autoritate de supraveghere a pieței a niciunui stat membru și nici Comisia nu ridică vreo obiecție cu privire la o măsură provizorie luată de o autoritate de supraveghere a pieței a unui alt 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 de trei luni menționat la prezentul alineat se reduce la 30 de zile în cazul nerespectării interdicției privind practicile în domeniul IA menționate la articolul 5 din prezentul regulament.

(9) Autoritățile de supraveghere a pieței se asigură că se iau măsuri restrictive adecvate în ceea ce privește produsul sau sistemul de IA în cauză, cum ar fi retragerea fără întârzieri nejustificate a produsului sau a sistemului de IA de pe piețele lor.

Articolul 80

Procedura aplicabilă sistemelor de IA clasificate de furnizor ca neprezentând un grad ridicat de risc în aplicarea anexei III

(1) În cazul în care o autoritate de supraveghere a pieței are motive suficiente să considere că un sistem de IA clasificat de furnizor ca neprezentând un grad ridicat de risc în conformitate cu articolul 6 alineatul (3) prezintă, de fapt, un grad ridicat de risc, autoritatea de supraveghere a pieței efectuează o evaluare a sistemului de IA în cauză în ceea ce privește clasificarea sa ca sistem de IA cu grad ridicat de risc, pe baza condițiilor prevăzute la articolul 6 alineatul (3) și în orientările Comisiei.

(2) În cazul în care, pe parcursul evaluării respective, autoritatea de supraveghere a pieței constată că sistemul de IA în cauză prezintă un grad ridicat de risc, aceasta solicită fără întârzieri nejustificate furnizorului relevant să ia toate măsurile necesare pentru a asigura conformitatea sistemului de IA cu cerințele și obligațiile prevăzute în prezentul regulament, precum și să ia măsuri corective adecvate într-un termen pe care autoritatea de supraveghere a pieței îl poate indica.

(3) În cazul în care autoritatea de supraveghere a pieței consideră că utilizarea sistemului de IA în cauză nu se limitează la teritoriul său național, aceasta informează fără întârzieri nejustificate Comisia și celelalte state membre cu privire la rezultatele evaluării și la măsurile pe care i le-a impus furnizorului.

(4) Furnizorul se asigură că se iau toate măsurile necesare pentru a asigura conformitatea sistemului de IA cu cerințele și obligațiile prevăzute în prezentul regulament. În cazul în care furnizorul unui sistem de IA în cauză nu asigură conformitatea sistemului de IA cu respectivele cerințe și obligații în termenul menționat la alineatul (2) de la prezentul articol, furnizorului i se aplică amenzi în conformitate cu articolul 99.

(5) Furnizorul se asigură că sunt întreprinse toate măsurile corective adecvate pentru toate sistemele de IA în cauză pe care acesta le-a pus la dispoziție pe piața Uniunii.

(6) Dacă furnizorul sistemului de IA în cauză nu ia măsurile corective adecvate în termenul menționat la alineatul (2) de la prezentul articol, se aplică articolul 79 alineatele (5)-(9).

(7) Dacă, în cursul evaluării respective în temeiul alineatului (1) de la prezentul articol, autoritatea de supraveghere a pieței stabilește că sistemul de IA a fost clasificat greșit de furnizor ca neprezentând un grad ridicat de risc pentru a eluda aplicarea cerințelor de la capitolul III secțiunea 2, furnizorului i se aplică amenzi în conformitate cu articolul 99.

(8) În exercitarea competenței lor de monitorizare a aplicării prezentului articol și în conformitate cu articolul 11 din Regulamentul (UE) 2019/1020, autoritățile de supraveghere a pieței pot efectua verificări adecvate, ținând seama în special de informațiile stocate în baza de date a UE menționată la articolul 71 din prezentul regulament.

Articolul 81

Procedura de salvgardare a Uniunii

(1) Dacă, în termen de trei luni de la primirea notificării menționate la articolul 79 alineatul (5) sau în termen de 30 de zile în cazul nerespectării interdicției privind practicile în domeniul IA menționate la articolul 5, se ridică obiecții de către autoritatea de supraveghere a pieței a unui stat membru împotriva unei măsuri luate de altă autoritate de supraveghere a pieței 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 a statului membru relevant și cu operatorul sau operatorii și evaluează măsura națională. Pe baza rezultatelor evaluării respective, Comisia decide dacă măsura națională este justificată sau nu în termen de șase luni ori, în cazul nerespectării interdicției privind practicile în domeniul IA menționate la articolul 5, în termen de 60 de zile de la notificarea menționată la articolul 79 alineatul (5) și notifică această decizie autorității de supraveghere a pieței a statului membru în cauză. Comisia informează, de asemenea, toate celelalte autorități de supraveghere a pieței cu privire la decizia sa.

(2) În cazul în care Comisia consideră că măsura luată de statul membru în cauză este justificată, toate statele membre se asigură că iau măsuri restrictive adecvate în ceea ce privește sistemul de IA în cauză, cum ar fi impunerea retragerii fără întârzieri nejustificate a sistemului de IA de pe piața lor, și informează Comisia în consecință. În cazul în care Comisia consideră că măsura națională este nejustificată, 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 standardelor 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 82

Sisteme de IA conforme care prezintă un risc

(1) Dacă, în urma efectuării unei evaluări în temeiul articolului 79, după consultarea autorității publice naționale relevante menționate la articolul 77 alineatul (1), autoritatea de supraveghere a pieței dintr-un stat membru constată că, deși un sistem de IA cu grad ridicat de risc este în conformitate cu prezentul regulament, acesta prezintă totuși un risc pentru sănătatea sau siguranța persoanelor, pentru drepturile fundamentale sau pentru alte aspecte legate de protecția interesului public, autoritatea de supraveghere a pieței respectivă impune 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 fără întârzieri nejustificate, într-un termen pe care aceasta îl poate indica.

(2) Furnizorul sau alt operator relevant se asigură că sunt luate măsuri corective cu privire la toate sistemele de IA în cauză pe care le-a pus la dispoziție pe piața Uniunii, în termenul prevăzut de autoritatea de supraveghere a pieței din statul membru menționat la alineatul (1).

(3) Statele membre informează imediat Comisia și celelalte state membre cu privire la o constatare în temeiul alineatului (1). 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 operatorii relevanți și evaluează măsurile naționale luate. Pe baza rezultatelor evaluării respective, Comisia decide dacă măsura este justificată și, după caz, propune alte măsuri adecvate.

(5) Comisia comunică imediat decizia sa statelor membre în cauză și operatorilor relevanți. Aceasta informează, de asemenea, celelalte state membre.

Articolul 83

Neconformitatea formală

(1) Autoritatea de supraveghere a pieței dintr-un stat membru solicită operatorului relevant să pună capăt neconformității în cauză, într-un termen pe care aceasta îl poate indica, atunci când constată una dintre situațiile următoare:

(a) marcajul CE a fost aplicat cu încălcarea articolului 48;

(b) marcajul CE nu a fost aplicat;

(c) declarația de conformitate UE menționată la articolul 47 nu a fost întocmită;

(d) declarația de conformitate UE menționată la articolul 47 nu a fost întocmită corect;

(e) nu a fost efectuată înregistrarea în baza de date a UE menționată la articolul 71;

(f) după caz, nu a fost numit un reprezentant autorizat;

(g) documentația tehnică nu este disponibilă.

(2) În cazul în care neconformitatea menționată la alineatul (1) persistă, autoritatea de supraveghere a pieței din statul membru în cauză ia măsuri corespunzătoare și proporționate pentru a restricționa sau a interzice punerea la dispoziție pe piață a sistemului de IA cu grad ridicat de risc sau pentru a se asigura că acesta este rechemat sau retras de pe piață fără întârziere.

Articolul 84

Structurile de sprijin pentru testarea IA ale Uniunii

(1) Comisia desemnează una sau mai multe structuri de sprijin pentru testarea IA ale Uniunii pentru a îndeplini sarcinile enumerate la articolul 21 alineatul (6) din Regulamentul (UE) 2019/1020 în domeniul IA.

(2) Fără a aduce atingere sarcinilor menționate la alineatul (1), structurile de sprijin pentru testarea IA ale Uniunii furnizează, de asemenea, consiliere tehnică sau științifică independentă la cererea comitetului, a Comisiei sau a autorităților de supraveghere a pieței.

SECȚIUNEA 4

CĂI DE ATAC

Articolul 85

Dreptul de a depune o plângere la o autoritate de supraveghere a pieței

Fără a aduce atingere altor căi de atac administrative sau judiciare, orice persoană fizică sau juridică care are motive să considere că a avut loc o încălcare a dispozițiilor prezentului regulament poate depune plângeri la autoritatea de supraveghere a pieței relevantă.

În conformitate cu Regulamentul (UE) 2019/1020, astfel de plângeri sunt luate în considerare în scopul desfășurării activităților de supraveghere a pieței și sunt tratate în conformitate cu procedurile specifice stabilite în acest scop de autoritățile de supraveghere a pieței.

Articolul 86

Dreptul la explicarea luării deciziilor individuale

(1) Orice persoană afectată care face obiectul unei decizii care este luată de implementator pe baza rezultatelor unui sistem de IA cu grad ridicat de risc enumerat în anexa III, cu excepția sistemelor enumerate la punctul 2 din aceasta, și care produce efecte juridice sau o afectează pe persoana respectivă în mod similar într-un grad semnificativ de o manieră pe care o consideră a avea un impact negativ asupra sănătății, siguranței sau drepturilor sale fundamentale are dreptul de a solicita implementatorului explicații clare și semnificative cu privire la rolul sistemului de IA în procedura decizională și la principalele elemente ale deciziei luate.

(2) Alineatul (1) nu se aplică utilizării sistemelor de IA pentru care excepțiile sau restricțiile de la obligația prevăzută la alineatul respectiv decurg din dreptul Uniunii sau din dreptul intern în conformitate cu dreptul Uniunii.

(3) Prezentul articol se aplică numai în măsura în care dreptul menționat la alineatul (1) nu este deja prevăzut în dreptul Uniunii.

Articolul 87

Raportarea încălcărilor și protecția persoanelor care efectuează raportarea

În ceea ce privește raportarea încălcărilor prezentului regulament și protecția persoanelor care raportează astfel de încălcări se aplică Directiva (UE) 2019/1937.

SECȚIUNEA 5

SUPRAVEGHEREA, INVESTIGAREA, APLICAREA LEGII ȘI MONITORIZAREA ÎN CEEA CE PRIVEȘTE FURNIZORII DE MODELE DE IA DE UZ GENERAL

Articolul 88

Executarea obligațiilor furnizorilor de modele de IA de uz general

(1) Comisia are competențe exclusive de a supraveghea și de a asigura respectarea capitolului V, ținând seama de garanțiile procedurale în temeiul articolului 94. Comisia încredințează Oficiului pentru IA punerea în aplicare a acestor sarcini, fără a aduce atingere competențelor de organizare ale Comisiei și repartizării competențelor între statele membre și Uniune pe baza tratatelor.

(2) Fără a aduce atingere articolului 75 alineatul (3), autoritățile de supraveghere a pieței îi pot solicita Comisiei să își exercite competențele prevăzute în prezenta secțiune, în cazul în care acest lucru este necesar și proporțional pentru a sprijini îndeplinirea sarcinilor care le revin în temeiul prezentului regulament.

Articolul 89

Măsuri de monitorizare

(1) În scopul îndeplinirii sarcinilor care îi sunt atribuite în temeiul prezentei secțiuni, Oficiul pentru IA poate lua măsurile necesare pentru a monitoriza punerea în aplicare și respectarea efectivă a prezentului regulament de către furnizorii de modele de IA de uz general, inclusiv respectarea de către aceștia a codurilor de bune practici aprobate.

(2) Furnizorii din aval au dreptul de a depune o plângere privind încălcarea prezentului regulament. O plângere trebuie să fie motivată corespunzător și să indice cel puțin:

(a) punctul de contact al furnizorului modelului de IA de uz general în cauză;

(b) o descriere a faptelor relevante, a dispozițiilor vizate ale prezentului regulament și a motivului pentru care furnizorul din aval consideră că furnizorul modelului de IA de uz general în cauză a încălcat prezentul regulament;

(c) orice alte informații pe care furnizorul din aval care a transmis cererea le consideră relevante, inclusiv, după caz, informații colectate din proprie inițiativă.

Articolul 90

Alerte privind riscurile sistemice transmise de grupul științific

(1) Grupul științific poate transmite o alertă calificată către Oficiul pentru IA în cazul în care are motive să suspecteze că:

(a) un model de IA de uz general prezintă un risc identificabil concret la nivelul Uniunii; sau

(b) un model de IA de uz general îndeplinește condițiile menționate la articolul 51.

(2) În urma unei astfel de alerte calificate, Comisia, prin intermediul Oficiului pentru IA și după ce a informat comitetul, poate exercita competențele prevăzute în prezenta secțiune în scopul analizării chestiunii. Oficiul pentru IA informează comitetul cu privire la orice măsură în conformitate cu articolele 91-94.

(3) O alertă calificată trebuie să fie motivată corespunzător și să indice cel puțin:

(a) punctul de contact al furnizorului modelului de IA de uz general cu risc sistemic în cauză;

(b) o descriere a faptelor relevante și a motivelor care stau la baza alertei transmise de grupul științific;

(c) orice alte informații pe care grupul științific le consideră relevante, inclusiv, după caz, informații colectate din proprie inițiativă.

Articolul 91

Competența de a solicita documente și informații

(1) Comisia poate solicita furnizorului modelului de IA de uz general în cauză să furnizeze documentația întocmită de furnizor în conformitate cu articolele 53 și 55 sau orice informații suplimentare care sunt necesare în scopul evaluării conformității furnizorului cu prezentul regulament.

(2) Înainte de trimiterea cererii de informații, Oficiul pentru IA poate iniția un dialog structurat cu furnizorul modelului de IA de uz general.

(3) La cererea justificată în mod corespunzător a grupului științific, Comisia poate emite o cerere de informații adresată unui furnizor al unui model de IA de uz general, în cazul în care accesul la informații este necesar și proporțional pentru îndeplinirea sarcinilor grupului științific în temeiul articolului 68 alineatul (2).

(4) Cererea de informații precizează temeiul juridic și scopul cererii, specifică informațiile solicitate, stabilește termenul în care acestea trebuie furnizate și indică amenzile prevăzute la articolul 101 pentru furnizarea de informații incorecte, incomplete sau înșelătoare.

(5) Furnizorul modelului de IA de uz general în cauză sau reprezentantul acestuia furnizează informațiile solicitate. În cazul persoanelor juridice, al societăților sau firmelor ori în cazul în care furnizorul nu are personalitate juridică, persoanele autorizate să le reprezinte în temeiul legii sau al statutului lor furnizează informațiile solicitate în numele furnizorului modelului de IA de uz general în cauză. Juriștii autorizați corespunzător să acționeze în acest sens pot furniza informațiile în numele clienților lor. Clienții rămân totuși pe deplin răspunzători în situația în care informațiile furnizate sunt incomplete, incorecte sau înșelătoare.

Articolul 92

Competența de a efectua evaluări

(1) Oficiul pentru IA, după consultarea comitetului, poate efectua evaluări ale modelului de IA de uz general în cauză:

(a) pentru a evalua respectarea de către furnizor a obligațiilor care îi revin în temeiul prezentului regulament, în cazul în care informațiile colectate în temeiul articolului 91 sunt insuficiente; sau

(b) pentru a investiga riscurile sistemice la nivelul Uniunii ale modelelor de IA de uz general cu risc sistemic, în special în urma unei alerte calificate a grupului științific în conformitate cu articolul 90 alineatul (1) litera (a).

(2) Comisia poate decide să numească experți independenți care să efectueze evaluări în numele său, inclusiv din cadrul grupului științific instituit în temeiul articolului 68. Experții independenți numiți pentru această sarcină îndeplinesc criteriile menționate la articolul 68 alineatul (2).

(3) În sensul alineatului (1), Comisia poate solicita accesul la modelul de IA de uz general în cauză prin intermediul API sau al altor mijloace și instrumente tehnice adecvate, inclusiv codul sursă.

(4) Cererea de acces menționează temeiul juridic, scopul și motivele cererii și stabilește termenul în care trebuie acordat accesul, precum și amenzile prevăzute la articolul 101 pentru neacordarea accesului.

(5) Furnizorul modelului de IA de uz general în cauză sau reprezentantul acestuia furnizează informațiile solicitate. În cazul persoanelor juridice, societăților sau firmelor ori în cazul în care furnizorul nu are personalitate juridică, persoanele autorizate să îl reprezinte în temeiul legii sau al statutului său furnizează accesul solicitat în numele furnizorului modelului de IA de uz general în cauză.

(6) Comisia adoptă acte de punere în aplicare care stabilesc modalitățile detaliate și condițiile evaluărilor, inclusiv modalitățile detaliate de implicare a experților independenți, precum și procedura de selecție a acestora. Actele de punere în aplicare respective se adoptă în conformitate cu procedura de examinare menționată la articolul 98 alineatul (2).

(7) Înainte de a solicita accesul la modelul de IA de uz general în cauză, Oficiul pentru IA poate iniția un dialog structurat cu furnizorul modelului de IA de uz general, pentru a colecta mai multe informații cu privire la testarea internă a modelului, la garanțiile interne pentru prevenirea riscurilor sistemice și la alte proceduri și măsuri interne pe care furnizorul le-a instituit pentru a atenua astfel de riscuri.

Articolul 93

Competența de a solicita măsuri

(1) În cazul în care este necesar și adecvat, Comisia le poate solicita furnizorilor:

(a) să ia măsuri adecvate pentru a respecta obligațiile prevăzute la articolele 53 și 54;

(b) să pună în aplicare măsuri de atenuare, în cazul în care evaluarea efectuată în conformitate cu articolul 92 a dat naștere unei preocupări serioase și întemeiate cu privire la un risc sistemic la nivelul Uniunii;

(c) să restricționeze punerea la dispoziție pe piață a modelului, să îl retragă sau să îl recheme.

(2) Înainte de a solicita o măsură, Oficiul pentru IA poate iniția un dialog structurat cu furnizorul modelului de IA de uz general.

(3) În cazul în care, în cursul dialogului structurat menționat la alineatul (2), furnizorul modelului de IA de uz general cu risc sistemic își asumă angajamente de a pune în aplicare măsuri de atenuare a unui risc sistemic la nivelul Uniunii, Comisia poate, prin intermediul unei decizii, să confere respectivelor angajamente caracter obligatoriu și să declare că nu există alte motive pentru a acționa.

Articolul 94

Drepturile procedurale ale operatorilor economici ai modelului de IA de uz general

Articolul 18 din Regulamentul (UE) 2019/1020 se aplică *mutatis mutandis* furnizorilor modelului de IA de uz general, fără a aduce atingere drepturilor procedurale mai specifice prevăzute în prezentul regulament.

Capitolul X
Coduri de conduită și orientări

Articolul 95

Coduri de conduită pentru aplicarea voluntară a cerințelor specifice

(1) Oficiul pentru IA și statele membre încurajează și facilitează elaborarea de coduri de conduită, inclusiv mecanisme de guvernanță conexe, menite să promoveze aplicarea voluntară în cazul altor sisteme de IA decât sistemele de IA cu grad ridicat de risc a unora dintre cerințele sau a tuturor cerințelor prevăzute în capitolul III secțiunea 2, ținând seama de soluțiile tehnice disponibile și de bunele practici ale sectorului care permit aplicarea unor astfel de cerințe.

(2) Oficiul pentru IA și statele membre facilitează elaborarea de coduri de conduită privind aplicarea voluntară, inclusiv de către implementatori, a unor cerințe specifice în privința tuturor sistemelor de IA, pe baza unor obiective clare și a unor indicatori-cheie de performanță pentru a măsura îndeplinirea obiectivelor respective, inclusiv a unor elemente precum următoarele, dar fără a se limita la acestea:

(a) elementele aplicabile prevăzute în orientările etice ale Uniunii pentru o IA de încredere;

(b) evaluarea și reducerea la minimum a impactului sistemelor de IA asupra durabilității mediului, inclusiv în ceea ce privește programarea eficientă din punct de vedere energetic și tehnici pentru proiectarea, antrenarea și utilizarea eficientă a IA;

(c) promovarea alfabetizării în domeniul IA, în special pe cea a persoanelor care se ocupă de dezvoltarea, operarea și utilizarea IA;

(d) facilitarea unei proiectări a sistemelor de IA care să țină seama de incluziune și diversitate, inclusiv prin crearea unor echipe de dezvoltare incluzive și diverse și promovarea participării părților interesate la acest proces;

(e) evaluarea și prevenirea impactului negativ al sistemelor de IA asupra persoanelor vulnerabile sau grupurilor de persoane vulnerabile, inclusiv în ceea ce privește accesibilitatea pentru persoanele cu dizabilități, precum și asupra egalității de gen.

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

(4) Oficiul pentru IA și statele membre țin seama de interesele și nevoile specifice ale IMM-urilor, inclusiv ale întreprinderilor nou-înființate, atunci când încurajează și facilitează elaborarea de coduri de conduită.

Articolul 96

Orientări din partea Comisiei privind punerea în aplicare a prezentului regulament

(1) Comisia elaborează orientări privind punerea în aplicare practică a prezentului regulament, în special cu privire la:

(a) aplicarea cerințelor și obligațiilor menționate la articolele 8-15 și la articolul 25;

(b) practicile interzise menționate la articolul 5;

(c) punerea în aplicare concretă a dispozițiilor referitoare la modificarea substanțială;

(d) punerea în aplicare concretă a obligațiilor de transparență prevăzute la articolul 50;

(e) informații detaliate privind relația dintre prezentul regulament și actele legislative de armonizare ale Uniunii enumerate în anexa I, precum și alte acte legislative relevante ale Uniunii, inclusiv în ceea ce privește coerența în aplicarea acestora;

(f) aplicarea definiției unui sistem de IA astfel cum este prevăzută la articolul 3 punctul 1.

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.

Orientările menționate la primul paragraf de la prezentul alineat țin seama în mod corespunzător de stadiul de avansare general recunoscut al tehnologiei în domeniul IA, precum și de standardele armonizate și specificațiile comune relevante menționate la articolele 40 și 41 sau de acele standarde armonizate sau specificații tehnice care sunt stabilite în temeiul legislației de armonizare a Uniunii.

(2) La cererea statelor membre sau a Oficiului pentru IA ori din proprie inițiativă, Comisia actualizează orientările adoptate anterior atunci când consideră necesar.

Capitolul XI
Delegarea de competențe și procedura comitetului

Articolul 97

Exercitarea delegării

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

(2) Competența de a adopta acte delegate menționată la articolul 6 alineatele (6) și (7), la articolul 7 alineatele (1) și (3), la articolul 11 alineatul (3), la articolul 43 alineatele (5) și (6), la articolul 47 alineatul (5), la articolul 51 alineatul (3), la articolul 52 alineatul (4) și la articolul 53 alineatele (5) și (6) se conferă Comisiei pe o perioadă de cinci ani de la ... [data intrării în vigoare a prezentului regulament]. 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 6 alineatele (6) și (7), la articolul 7 alineatele (1) și (3), la articolul 11 alineatul (3), la articolul 43 alineatele (5) și (6), la articolul 47 alineatul (5), la articolul 51 alineatul (3), la articolul 52 alineatul (4) și la articolul 53 alineatele (5) și (6) 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 care urmează 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) Înainte de adoptarea unui act delegat, Comisia consultă experții desemnați de fiecare stat membru în conformitate cu principiile prevăzute în Acordul interinstituțional din 13 aprilie 2016 privind o mai bună legiferare.

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

(6) Orice act delegat adoptat în temeiul articolului 6 alineatul (6) sau (7), al articolului 7 alineatul (1) sau (3), al articolului 11 alineatul (3), al articolului 43 alineatul (5) sau (6), al articolului 47 alineatul (5), al articolului 51 alineatul (3), al articolului 52 alineatul (4) sau al articolului 53 alineatul (5) sau (6) intră în vigoare numai în cazul în care nici Parlamentul European și nici Consiliul nu au formulat obiecții în termen de trei luni de la notificarea acestuia către Parlamentul European și Consiliu sau în cazul în care, înaintea expirării termenului respectiv, Parlamentul European și Consiliul au informat Comisia că nu vor formula obiecții. Respectivul termen se prelungește cu trei luni la inițiativa Parlamentului European sau a Consiliului.

Articolul 98

Procedura comitetului

(1) Comisia este asistată de un comitet. Respectivul comitet reprezintă un comitet în înțelesul 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.

Capitolul XII
Sancțiuni

Articolul 99

Sancțiuni

(1) În conformitate cu termenele și condițiile prevăzute în prezentul regulament, statele membre stabilesc normele privind sancțiunile și alte măsuri de aplicare a legii, care pot include, de asemenea, avertismente și măsuri nemonetare, aplicabile în cazul încălcării prezentului regulament de către operatori, și iau toate măsurile necesare pentru a se asigura că acestea sunt puse în aplicare în mod corespunzător și efectiv, ținând astfel seama de orientările emise de Comisie în temeiul articolului 96. Sancțiunile prevăzute trebuie să fie efective, proporționale și cu efect de descurajare. Acestea țin seama de interesele IMM-urilor, inclusiv ale întreprinderilor nou-înființate, precum și de viabilitatea lor economică.

(2) Statele membre îi notifică Comisiei, fără întârziere și cel târziu până la data începerii aplicării, normele privind sancțiunile și alte măsuri de aplicare a legii menționate la alineatul (1) și îi comunică acesteia fără întârziere orice modificare ulterioară a acestora.

(3) Nerespectarea oricăreia dintre interdicțiile privind practicile în domeniul IA menționate la articolul 5 face obiectul unor amenzi administrative de până la 35 000 000 EUR sau, în cazul în care autorul infracțiunii este o întreprindere, de până la 7 % din cifra sa de afaceri mondială totală anuală pentru exercițiul financiar precedent, luându-se în considerare valoarea cea mai mare dintre acestea.

(4) Neconformitatea cu oricare dintre următoarele dispoziții referitoare la operatori sau la organismele notificate, altele decât cele prevăzute la articolul 5, face obiectul unor amenzi administrative de până la 15 000 000 EUR sau, în cazul în care autorul infracțiunii este o întreprindere, de până la 3 % din cifra sa de afaceri mondială totală anuală pentru exercițiul financiar precedent, luându-se în considerare valoarea cea mai mare dintre acestea:

(a) obligațiile furnizorilor în temeiul articolului 16;

(b) obligațiile reprezentanților autorizați în temeiul articolului 22;

(c) obligațiile importatorilor în temeiul articolului 23;

(d) obligațiile distribuitorilor în temeiul articolului 24;

(e) obligațiile implementatorilor în temeiul articolului 26;

(f) cerințele și obligațiile organismelor notificate în temeiul articolului 31, al articolului 33 alineatele (1), (3) și (4) sau al articolului 34;

(g) obligațiile de transparență pentru furnizori și implementatori în temeiul articolului 50.

(5) Furnizarea de informații incorecte, incomplete sau înșelătoare organismelor notificate sau autorităților naționale competente ca răspuns la o cerere face obiectul unor amenzi administrative de până la 7 500 000 EUR sau, în cazul în care autorul infracțiunii este o întreprindere, de până la 1 % din cifra sa de afaceri mondială totală anuală pentru exercițiul financiar precedent, luându-se în considerare valoarea cea mai mare dintre acestea.

(6) În cazul IMM-urilor, inclusiv al întreprinderilor nou-înființate, fiecare amendă menționată la prezentul articol nu depășește procentajele sau cuantumul menționate la alineatele (3), (4) și (5), luându-se în considerare valoarea cea mai mică dintre acestea.

(7) Atunci când se decide dacă să se impună o amendă administrativă și 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, după caz, se acordă atenție următoarelor aspecte:

(a) natura, gravitatea și durata încălcării și a consecințelor acesteia, ținându-se seama de scopul sistemului de IA în cauză, precum și, după caz, de numărul de persoane afectate și de nivelul prejudiciilor suferite de acestea;

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

(c) dacă alte autorități au aplicat deja amenzi administrative aceluiași operator pentru încălcări ale altor acte din dreptul Uniunii sau de drept intern, în cazul în care astfel de încălcări rezultă din aceeași activitate sau omisiune care constituie o încălcare relevantă a prezentului regulament;

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

(e) orice alt factor agravant sau atenuant aplicabil circumstanțelor cazului, cum ar fi beneficiile financiare dobândite sau pierderile evitate în mod direct sau indirect ca urmare a încălcării;

(f) gradul de cooperare cu autoritățile naționale competente, pentru a remedia încălcarea și a atenua efectele negative posibile ale încălcării;

(g) gradul de responsabilitate al operatorului, ținându-se seama de măsurile tehnice și organizatorice puse în aplicare de acesta;

(h) modul în care încălcarea a fost adusă la cunoștința autorităților naționale competente, în special dacă și, în caz afirmativ, în ce măsură operatorul a notificat încălcarea;

(i) dacă încălcarea a fost comisă cu intenție sau din culpă;

(j) orice măsură luată de operator pentru a atenua dauna suferită de persoanele afectate.

(8) Fiecare stat membru stabilește norme cu privire la măsura în care pot fi impuse amenzi administrative autorităților și organismelor publice stabilite în statul membru respectiv.

(9) 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, după cum este aplicabil în statele membre respective. Aplicarea unor astfel de norme în statele membre respective are un efect echivalent.

(10) Exercitarea competențelor 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 eficace și dreptul la un proces echitabil.

(11) Statele membre raportează anual Comisiei cu privire la amenzile administrative pe care le-au aplicat în cursul anului respectiv, în conformitate cu prezentul articol, precum și cu privire la orice litigii sau proceduri judiciare conexe.

Articolul 100

Amenzi administrative aplicate instituțiilor, organelor, oficiilor și agențiilor Uniunii

(1) Autoritatea Europeană pentru Protecția Datelor poate impune amenzi administrative instituțiilor, organelor, oficiilor și agențiilor Uniunii care intră în domeniul de aplicare al prezentului regulament. Atunci când se decide dacă să se impună o amendă administrativă și 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, ținând seama de scopul sistemului de IA în cauză, precum și, după caz, de numărul de persoane afectate și de nivelul prejudiciului suferit de acestea;

(b) gradul de responsabilitate al instituției, organului, oficiului sau agenției Uniunii, ținându-se seama de măsurile tehnice și organizaționale implementate de acestea;

(c) orice măsură luată de instituția, organul, oficiul sau agenția Uniunii pentru a atenua prejudiciul suferit de persoanele afectate;

(d) gradul de cooperare cu Autoritatea Europeană pentru Protecția Datelor pentru a remedia încălcarea și a atenua posibilele efecte negative ale încălcării, inclusiv respectarea oricăreia dintre măsurile dispuse anterior de Autoritatea Europeană pentru Protecția Datelor împotriva instituției, organului, oficiului sau agenției Uniunii în cauză cu privire la același subiect;

(e) eventualele încălcări anterioare similare comise de instituția, organul, oficiul sau agenția Uniunii;

(f) modul în care încălcarea a fost adusă la cunoștința Autorității Europene pentru Protecția Datelor, în special dacă și în ce măsură instituția, organul, oficiul sau agenția Uniunii a notificat încălcarea;

(g) bugetul anual al instituției, organului, oficiului sau agenției Uniunii.

(2) Nerespectarea interdicției privind practicile în domeniul inteligenței artificiale menționate la articolul 5 face obiectul unor amenzi administrative de până la 1 500 000 EUR.

(3) Neconformitatea sistemului de IA cu oricare dintre cerințele sau obligațiile în temeiul prezentului regulament, altele decât cele prevăzute la articolul 5, face obiectul unor amenzi administrative de până la 750 000 EUR.

(4) Înaintea adoptării unor decizii în temeiul prezentului articol, Autoritatea Europeană pentru Protecția Datelor oferă instituției, organului, oficiului sau agenției Uniunii care face obiectul procedurilor desfășurate de Autoritatea Europeană pentru Protecția Datelor posibilitatea de a fi audiată 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 impunerea amenzilor prevăzute la prezentul articol contribuie la bugetul general al Uniunii. Amenzile nu afectează funcționarea eficace a instituției, organului, oficiului sau agenției Uniunii amendate.

(7) Autoritatea Europeană pentru Protecția Datelor notifică anual Comisiei amenzile administrative pe care le-a impus în temeiul prezentului articol și orice litigii sau orice proceduri judiciare pe care le-a inițiat.

Articolul 101

Amenzi pentru furnizorii de modele de IA de uz general

(1) Comisia poate impune furnizorilor de modele de IA de uz general amenzi care nu depășesc 3 % din cifra lor de afaceri mondială totală anuală pentru exercițiul financiar precedent sau 15 000 000 EUR, luându-se în considerare valoarea cea mai mare dintre acestea, atunci când Comisia constată că un furnizor, cu intenție sau din culpă:

(a) a încălcat dispozițiile relevante din prezentul regulament;

(b) nu s-a conformat unei solicitări de documente sau de informații în temeiul articolului 91 sau a furnizat informații incorecte, incomplete sau înșelătoare;

(c) nu s-a conformat unei măsuri solicitate în temeiul articolului 93;

(d) nu a pus la dispoziția Comisiei accesul la modelul de IA de uz general sau la modelul de IA de uz general cu risc sistemic în vederea efectuării unei evaluări în temeiul articolului 92.

La stabilirea cuantumului amenzii sau al penalităților cu titlu cominatoriu, se iau în considerare natura, gravitatea și durata încălcării, ținându-se seama în mod corespunzător de principiile proporționalității și adecvării. De asemenea, Comisia ia în considerare angajamentele asumate în conformitate cu articolul 93 alineatul (3) sau în temeiul codurilor de bune practici relevante, în conformitate cu articolul 56.

(2) Înainte de adoptarea deciziei în temeiul alineatului (1), Comisia comunică constatările sale preliminare furnizorului modelului de IA de uz general și îi oferă o posibilitate de a fi audiat.

(3) Amenzile impuse în conformitate cu prezentul articol trebuie să fie efective, proporționale și cu efect de descurajare.

(4) Informațiile privind amenzile impuse în temeiul prezentului articol se comunică de asemenea comitetului, după caz.

(5) Curtea de Justiție a Uniunii Europene are competența de fond de a examina deciziile Comisiei de stabilire a unei amenzi în temeiul prezentului articol. Curtea poate să anuleze, să reducă sau să majoreze amenda impusă.

(6) Comisia adoptă acte de punere în aplicare privind modalitățile detaliate și garanțiile procedurale ale procedurilor în vederea posibilei adoptări de decizii în temeiul alineatului (1) de la prezentul articol. Actele de punere în aplicare respective se adoptă în conformitate cu procedura de examinare menționată la articolul 98 alineatul (2).

Capitolul XIII
Dispoziții finale

Articolul 102

Modificarea 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 în ceea ce privește sistemele de inteligență artificială în sensul Regulamentului (UE) 2024/... al Parlamentului European și al Consiliului[*+], se ține seama de cerințele prevăzute în capitolul III secțiunea 2 din regulamentul respectiv.

---

[*] Regulamentul (UE) 2024/... al Parlamentului European și al Consiliului din ... de stabilire a unor norme armonizate privind inteligența artificială și de modificare a Regulamentelor (CE) nr. 300/2008, (UE) nr. 167/2013, (UE) nr. 168/2013, (UE) 2018/858, (UE) 2018/1139 și (UE) 2019/2144 și a Directivelor 2014/90/UE, (UE) 2016/797 și (UE) 2020/1828 (Regulamentul privind inteligența artificială) (JO L, ..., ELI: ...).”

[+] JO: a se introduce în text numărul prezentului regulament [2021/0106(COD)] și a se completa nota de subsol corespunzătoare.

Articolul 103

Modificarea 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 în ceea ce privește sistemele de inteligență artificială care sunt componente de siguranță în sensul Regulamentului (UE) 2024/... al Parlamentului European și al Consiliului[*+], se ține seama de cerințele prevăzute în capitolul III secțiunea 2 din regulamentul respectiv.

---

[*] Regulamentul (UE) 2024/... al Parlamentului European și al Consiliului din ... de stabilire a unor norme armonizate privind inteligența artificială și de modificare a Regulamentelor (CE) nr. 300/2008, (UE) nr. 167/2013, (UE) nr. 168/2013, (UE) 2018/858, (UE) 2018/1139 și (UE) 2019/2144 și a Directivelor 2014/90/UE, (UE) 2016/797 și (UE) 2020/1828 (Regulamentul privind inteligența artificială) (JO L, ..., ELI: ...).”

[+] JO: a se introduce în text numărul prezentului regulament [2021/0106(COD)] și a se completa nota de subsol corespunzătoare.

Articolul 104

Modificarea 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 în ceea ce privește sistemele de inteligență artificială care sunt componente de siguranță în sensul Regulamentului (UE) 2024/... al Parlamentului European și al Consiliului[*+], se ține seama de cerințele prevăzute în capitolul III secțiunea 2 din regulamentul respectiv.

---

[*] Regulamentul (UE) 2024/... al Parlamentului European și al Consiliului din ... de stabilire a unor norme armonizate privind inteligența artificială și de modificare a Regulamentelor (CE) nr. 300/2008, (UE) nr. 167/2013, (UE) nr. 168/2013, (UE) 2018/858, (UE) 2018/1139 și (UE) 2019/2144 și a Directivelor 2014/90/UE, (UE) 2016/797 și (UE) 2020/1828 (Regulamentul privind inteligența artificială) (JO L, ..., ELI: ...).”

[+] JO: a se introduce în text numărul prezentului regulament [2021/0106(COD)] și a se completa nota de subsol corespunzătoare.

Articolul 105

Modificarea Directivei 2014/90/UE

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

„(5) Pentru sistemele de inteligență artificială care sunt componente de siguranță în sensul Regulamentului (UE) 2024/... 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 capitolul III secțiunea 2 din regulamentul respectiv.

---

[*] Regulamentul (UE) 2024/... al Parlamentului European și al Consiliului din ... de stabilire a unor norme armonizate privind inteligența artificială și de modificare a Regulamentelor (CE) nr. 300/2008, (UE) nr. 167/2013, (UE) nr. 168/2013, (UE) 2018/858, (UE) 2018/1139 și (UE) 2019/2144 și a Directivelor 2014/90/UE, (UE) 2016/797 și (UE) 2020/1828 (Regulamentul privind inteligența artificială) (JO L, ..., ELI: ...).”

[+] JO: a se introduce în text numărul prezentului regulament [2021/0106(COD)] și a se completa nota de subsol corespunzătoare.

Articolul 106

Modificarea 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) în ceea ce privește sistemele de inteligență artificială care sunt componente de siguranță în sensul Regulamentului (UE) 2024/... al Parlamentului European și al Consiliului[*+], se ține seama de cerințele prevăzute în capitolul III secțiunea 2 din regulamentul respectiv.

---

[*] Regulamentul (UE) 2024/... al Parlamentului European și al Consiliului din ... de stabilire a unor norme armonizate privind inteligența artificială și de modificare a Regulamentelor (CE) nr. 300/2008, (UE) nr. 167/2013, (UE) nr. 168/2013, (UE) 2018/858, (UE) 2018/1139 și (UE) 2019/2144 și a Directivelor 2014/90/UE, (UE) 2016/797 și (UE) 2020/1828 (Regulamentul privind inteligența artificială) (JO L, ..., ELI: ...).”

[+] JO: a se introduce în text numărul prezentului regulament [2021/0106(COD)] și a se completa nota de subsol corespunzătoare.

Articolul 107

Modificarea 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) în ceea ce privește sistemele de inteligență artificială care sunt componente de siguranță în sensul Regulamentului (UE) 2024/... al Parlamentului European și al Consiliului[*+], se ține seama de cerințele prevăzute în capitolul III secțiunea 2 din regulamentul respectiv.

---

[*] Regulamentul (UE) 2024/... al Parlamentului European și al Consiliului din ... de stabilire a unor norme armonizate privind inteligența artificială și de modificare a Regulamentelor (CE) nr. 300/2008, (UE) nr. 167/2013, (UE) nr. 168/2013, (UE) 2018/858, (UE) 2018/1139 și (UE) 2019/2144 și a Directivelor 2014/90/UE, (UE) 2016/797 și (UE) 2020/1828 (Regulamentul privind inteligența artificială) (JO L, ..., ELI: ...).”

[+] JO: a se introduce în text numărul prezentului regulament [2021/0106(COD)] și a se completa nota de subsol corespunzătoare.

Articolul 108

Modificarea 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) în ceea ce privește sistemele de inteligență artificială care sunt componente de siguranță în sensul Regulamentului (UE) 2024/... al Parlamentului European și al Consiliului[*+], se ține seama de cerințele prevăzute în capitolul III secțiunea 2 din regulamentul respectiv.

---

[*] Regulamentul (UE) 2024/... al Parlamentului European și al Consiliului din ... de stabilire a unor norme armonizate privind inteligența artificială și de modificare a Regulamentelor (CE) nr. 300/2008, (UE) nr. 167/2013, (UE) nr. 168/2013, (UE) 2018/858, (UE) 2018/1139 și (UE) 2019/2144 și a Directivelor 2014/90/UE, (UE) 2016/797 și (UE) 2020/1828 (Regulamentul privind inteligența artificială) (JO L, ..., ELI: ...).”

2. La articolul 19, se adaugă următorul alineat:

„(4) La adoptarea actelor delegate în temeiul alineatelor (1) și (2) în ceea ce privește sistemele de inteligență artificială care sunt componente de siguranță în sensul Regulamentului (UE) 2024/...[++], se ține seama de cerințele prevăzute în capitolul III secțiunea 2 din regulamentul respectiv.”

[+] JO: a se introduce în text numărul prezentului regulament [2021/0106(COD)] și a se completa nota de subsol corespunzătoare.

[++] JO: a se introduce numărul prezentului regulament [2021/0106(COD)].

3. La articolul 43, se adaugă următorul alineat:

„(4) La adoptarea actelor de punere în aplicare în temeiul alineatului (1) în ceea ce privește sistemele de inteligență artificială care sunt componente de siguranță în sensul Regulamentului (UE) 2024/...[+], se ține seama de cerințele prevăzute în capitolul III secțiunea 2 din regulamentul respectiv.”

4. La articolul 47, se adaugă următorul alineat:

„(3) La adoptarea actelor delegate în temeiul alineatelor (1) și (2) în ceea ce privește sistemele de inteligență artificială care sunt componente de siguranță în sensul Regulamentului (UE) 2024/...[+] se ține seama de cerințele prevăzute în capitolul III secțiunea 2 din regulamentul respectiv.”

5. La articolul 57, se adaugă următorul paragraf:

„La adoptarea actelor de punere în aplicare în ceea ce privește sistemele de inteligență artificială care sunt componente de siguranță în sensul Regulamentului (UE) 2024/...[+] se ține seama de cerințele prevăzute în capitolul III secțiunea 2 din regulamentul respectiv.”

6. La articolul 58, se adaugă următorul alineat:

„(3) La adoptarea actelor delegate în temeiul alineatelor (1) și (2) în ceea ce privește sistemele de inteligență artificială care sunt componente de siguranță în sensul Regulamentului (UE) 2024/...[+], se ține seama de cerințele prevăzute în capitolul III secțiunea 2 din regulamentul respectiv.”

[+] JO: a se introduce numărul prezentului regulament [2021/0106(COD)].

Articolul 109

Modificarea 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) în ceea ce privește sistemele de inteligență artificială care sunt componente de siguranță în sensul Regulamentului (UE) 2024/... al Parlamentului European și al Consiliului[*+], se ține seama de cerințele prevăzute în capitolul III secțiunea 2 din regulamentul respectiv.

---

[*] Regulamentul (UE) 2024/... al Parlamentului European și al Consiliului din ... de stabilire a unor norme armonizate privind inteligența artificială și de modificare a Regulamentelor (CE) nr. 300/2008, (UE) nr. 167/2013, (UE) nr. 168/2013, (UE) 2018/858, (UE) 2018/1139 și (UE) 2019/2144 și a Directivelor 2014/90/UE, (UE) 2016/797 și (UE) 2020/1828 (Regulamentul privind inteligența artificială) (JO L, ..., ELI: ...).”

[+] JO: a se introduce în text numărul prezentului regulament [2021/0106(COD)] și a se completa nota de subsol corespunzătoare.

Articolul 110

Modificarea Directivei (UE) 2020/1828

În anexa I la Directiva (UE) 2020/1828 a Parlamentului European și a Consiliului[58] se adaugă următorul punct:

„(68) Regulamentul (UE) 2024/... al Parlamentului European și al Consiliului din ...[+] de stabilire a unor norme armonizate privind inteligența artificială și de modificare a Regulamentelor (CE) nr. 300/2008, (UE) nr. 167/2013, (UE) nr. 168/2013, (UE) 2018/858, (UE) 2018/1139 și (UE) 2019/2144 și a Directivelor 2014/90/UE, (UE) 2016/797 și (UE) 2020/1828 (Regulamentul privind inteligența artificială) (JO L ..., ELI: ...).”

Articolul 111

Sisteme de IA deja introduse pe piață sau puse în funcțiune și modele de IA de uz general deja introduse pe piață

(1) Fără a aduce atingere aplicării articolului 5, astfel cum se menționează la articolul 113 alineatul (3) litera (a), până la 31 decembrie 2030 se asigură conformitatea cu prezentul regulament a sistemelor de IA care sunt componente ale sistemelor informatice la scară largă instituite prin actele juridice enumerate în anexa X și care au fost introduse pe piață sau puse în funcțiune înainte de ... [36 de luni de la data intrării în vigoare a prezentului regulament].

---

58 Directiva (UE) 2020/1828 a Parlamentului European și a Consiliului din 25 noiembrie 2020 privind acțiunile în reprezentare pentru protecția intereselor colective ale consumatorilor și de abrogare a Directivei 2009/22/CE (JO L 409, 4.12.2020, p. 1).

[+] JO: a se introduce în text data și numărul prezentului regulament (2021/0106(COD)).

Cerințele prevăzute în prezentul regulament sunt luate în considerare la evaluarea fiecărui sistem informatic la scară largă instituit prin actele juridice enumerate în anexa X, care urmează să fie desfășurată astfel cum se prevede în actele juridice respective și în cazul în care actele juridice respective sunt înlocuite sau modificate.

(2) Fără a aduce atingere aplicării articolul 5, astfel cum se menționează la articolul 113 alineatul (3) litera (a), prezentul regulament se aplică operatorilor de sisteme de IA cu grad ridicat de risc, altele decât sistemele menționate la alineatul (1) de la prezentul articol, care au fost introduse pe piață sau puse în funcțiune înainte de ... [24 de luni de la data intrării în vigoare a prezentului regulament], numai dacă, de la data respectivă, sistemele respective fac obiectul unor modificări semnificative în ceea ce privește proiectarea lor. În orice caz, furnizorii și implementatorii sistemelor de IA cu grad ridicat de risc destinate a fi utilizate de autoritățile publice iau măsurile necesare pentru a se conforma cerințelor și obligațiilor din prezentul regulament până la ... [șase ani de la data intrării în vigoare a prezentului regulament].

(3) Furnizorii de modele de IA de uz general care au fost introduse pe piață înainte de ... [12 luni de la data intrării în vigoare a prezentului regulament] iau măsurile necesare pentru a se conforma obligațiilor prevăzute în prezentul regulament până la ... [36 de luni de la data intrării în vigoare a prezentului regulament].

Articolul 112

Evaluare și revizuire

(1) Comisia evaluează necesitatea modificării listei din anexa III și a listei practicilor interzise în domeniul IA stabilite la articolul 5 o dată pe an după intrarea în vigoare a prezentului regulament și până la sfârșitul perioadei de delegare a competențelor stabilite la articolul 97. Comisia transmite rezultatele acestei evaluări Parlamentului European și Consiliului.

(2) Până la ... [patru ani de la data aplicării prezentului regulament] și, ulterior, o dată la patru ani, Comisia evaluează următoarele aspecte și prezintă Parlamentului European și Consiliului un raport cu privire la acestea:

(a) necesitatea unor modificări de extindere a rubricilor de domeniu existente sau a adăugării unor noi rubrici de domeniu în anexa III;

(b) aducerea de modificări listei de sisteme de IA care necesită măsuri suplimentare de asigurare a transparenței astfel cum se menționează la articolul 50;

(c) aducerea de modificări care să sporească eficacitatea sistemului de supraveghere și de guvernanță.

(3) Până la ... [cinci ani de la data intrării în vigoare a prezentului regulament] și, ulterior, o dată la patru ani, Comisia prezintă Parlamentului European și Consiliului un raport privind evaluarea și revizuirea prezentului regulament. Raportul include o evaluare a structurii aplicării legii și a eventualei necesități ca o agenție a Uniunii să soluționeze orice deficiențe identificate. Pe baza constatărilor, raportul respectiv este însoțit, după caz, de o propunere de modificare a prezentului regulament. Rapoartele sunt făcute publice.

(4) Rapoartele menționate la alineatul (2) acordă o atenție deosebită următoarelor aspecte:

(a) situația resurselor financiare, tehnice și umane ale autorităților naționale competente în vederea îndeplinirii cu eficacitate a sarcinilor care le-au fost încredințate în temeiul prezentului regulament;

(b) situația sancțiunilor, în special a amenzilor administrative, astfel cum sunt menționate la articolul 99 alineatul (1), aplicate de statele membre în cazuri de încălcare a prezentului regulament;

(c) standardele armonizate adoptate și specificațiile comune elaborate pentru a sprijini prezentul regulament;

(d) numărul de întreprinderi care intră pe piață după începerea aplicării prezentului regulament și câte dintre acestea sunt IMM-uri.

(5) Până la ... [patru ani de la data intrării în vigoare a prezentului regulament], Comisia evaluează funcționarea Oficiului pentru IA, dacă Oficiul pentru IA a primit suficiente atribuții și competențe pentru a-și îndeplini sarcinile și dacă ar fi relevant și necesar, pentru punerea în aplicare și respectarea în mod corespunzător a prezentului regulament, ca Oficiul pentru IA și competențele sale de executare să fie întărite și resursele sale să fie sporite. Comisia transmite un raport privind evaluarea sa Parlamentului European și Consiliului.

(6) Până la ... [patru ani de la data intrării în vigoare a prezentului regulament] și, ulterior, o dată la patru ani, Comisia prezintă Parlamentului European și Consiliului un raport privind evaluarea progreselor înregistrate în elaborarea documentelor de standardizare privind dezvoltarea eficientă din punct de vedere energetic a modelelor de IA de uz general și evaluează necesitatea unor măsuri sau acțiuni suplimentare, inclusiv a unor măsuri sau acțiuni obligatorii. Raportul se transmite Parlamentului European și Consiliului și se face public.

(7) Până la ... [patru ani de la data intrării în vigoare a prezentului regulament] și, ulterior, o dată la trei ani, Comisia evaluează impactul și eficacitatea codurilor de conduită voluntare în ceea ce privește încurajarea aplicării cerințelor prevăzute în capitolul III secțiunea 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, altele decât sistemele de IA cu grad ridicat de risc, inclusiv în privința durabilității mediului.

(8) În sensul alineatelor (1)–(7), comitetul, statele membre și autoritățile naționale competente furnizează Comisiei informații la cererea acesteia și fără întârzieri nejustificate.

(9) La efectuarea evaluărilor și a revizuirilor menționate la alineatele (1)–(7), Comisia ține seama de pozițiile și constatările comitetului, ale Parlamentului European, ale Consiliului, precum și ale altor organisme sau surse relevante.

(10) Comisia transmite, dacă este necesar, propuneri corespunzătoare de modificare a prezentului regulament, în special ținând seama de evoluțiile din domeniul tehnologiei, de efectul sistemelor de IA asupra sănătății și siguranței, precum și asupra drepturilor fundamentale, și având în vedere progresele societății informaționale.

(11) Pentru a ghida evaluările și revizuirile menționate la alineatele (1)-(7) de la prezentul articol, Oficiul pentru IA elaborează o metodologie obiectivă și participativă pentru evaluarea nivelului de risc pe baza criteriilor stabilite la articolele relevante și includerea unor sisteme noi în:

(a) lista prevăzută în anexa III, inclusiv extinderea rubricilor de domeniu existente sau adăugarea unor noi rubrici de domeniu în anexa respectivă;

(b) lista de practici interzise prevăzute la articolul 5; și

(c) în lista de sisteme de IA care necesită măsuri suplimentare de asigurare a transparenței în temeiul articolului 50.

(12) Orice modificare a prezentului regulament în temeiul alineatului (10) sau orice act delegat ori de punere în aplicare relevant, care vizează actele legislative sectoriale de armonizare ale Uniunii enumerate în secțiunea B din anexa I, ia în considerare particularitățile de reglementare ale fiecărui sector și mecanismele și autoritățile existente de guvernanță, de evaluare a conformității și de aplicare a legii instituite în actele respective.

(13) Până la ... [șapte ani de la data intrării în vigoare a prezentului regulament], Comisia efectuează o evaluare aplicării prezentului regulament și prezintă un raport referitor la aceasta Parlamentului European, Consiliului și Comitetului Economic și Social European, vizând primii ani de aplicare a prezentului regulament. Pe baza constatărilor, raportul este însoțit, după caz, de o propunere de modificare a prezentului regulament cu privire la structura aplicării legii și la necesitatea ca o agenție a Uniunii să soluționeze deficiențele identificate.

Articolul 113

Intrare în vigoare și aplicare

Prezentul regulament intră în vigoare în a douăzecea zi de la data publicării în *Jurnalul Oficial al Uniunii Europene*.

Acesta se aplică de la ... [24 de luni de la data intrării în vigoare a prezentului regulament].

Cu toate acestea:

(a) capitolele I și II se aplică de la ... [șase luni de la data intrării în vigoare a prezentului regulament];

(b) Capitolul III secțiunea 4, capitolul V, capitolul VII, capitolul XII și articolul 78 se aplică de la ... [12 luni de la data intrării în vigoare a prezentului regulament], cu excepția articolului 101;

(c) Articolul 6 alineatul (1) și obligațiile corespunzătoare din prezentul regulament se aplică de la ... [36 de luni de la data intrării în vigoare a prezentului regulament].

Prezentul regulament este obligatoriu în toate elementele sale și se aplică direct în toate statele membre.

Adoptat la ...,

Pentru Parlamentul European	*Pentru Consiliu*
Președinta	*Președintele*

ANEXA I

Lista legislației de armonizare a Uniunii

Secțiunea A – Lista actelor legislative de armonizare ale 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

13. 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);

14. 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);

15. 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);

16. 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);

17. 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);

18. 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);

19. 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);

20. 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 II

Lista infracțiunilor menționate la articolul 5 alineatul (1) primul paragraf litera (h) punctul (iii)

Infracțiunile menționate la articolul 5 alineatul (1) primul paragraf litera (h) punctul (iii):

– terorism,

– trafic de ființe umane,

– exploatare sexuală a copiilor și pornografie infantilă,

– trafic ilicit de stupefiante sau de substanțe psihotrope,

– trafic ilicit de arme, muniții sau substanțe explozive,

– omor, vătămare corporală gravă,

– trafic ilicit de organe sau țesuturi umane,

– trafic ilicit de materiale nucleare sau radioactive,

– răpire, lipsire de libertate în mod ilegal sau luare de ostatici,

– infracțiuni de competența Curții Penale Internaționale,

– sechestrare ilicită de aeronave sau de nave,

– viol,

– infracțiuni împotriva mediului,

– jaf organizat sau armat,

– sabotaj,

– participare la o organizație criminală implicată în una sau mai multe dintre infracțiunile enumerate mai sus.

ANEXA III

Sisteme de IA cu grad ridicat de risc menționate la articolul 6 alineatul (2)

Sistemele de IA cu grad ridicat de risc conform articolului 6 alineatul (2) sunt sistemele de IA aparținând oricăruia dintre următoarele domenii:

1. Biometrie, în măsura în care utilizarea acesteia este permisă în temeiul dreptului Uniunii sau intern relevant:

   (a) sisteme de identificare biometrică la distanță.

   Acestea nu includ sistemele de IA destinate a fi utilizate pentru verificarea biometrică al cărei unic scop este de a confirma că o anumită persoană fizică este persoana care susține că este;

   (b) sisteme de IA destinate a fi utilizate pentru clasificarea biometrică, în funcție de atribute sau caracteristici sensibile ori protejate, pe baza deducerii acestor atribute sau caracteristici;

   (c) sisteme de IA destinate a fi utilizate pentru recunoașterea emoțiilor.

2. Infrastructură critică: sisteme de IA destinate a fi utilizate drept componente de siguranță în gestionarea și exploatarea infrastructurii digitale critice, a traficului rutier sau a aprovizionării cu apă, gaz, încălzire ori energie electrică.

3. Educație și formare profesională:

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

(c) sisteme de IA destinate a fi utilizate în scopul evaluării nivelului adecvat de educație pe care o persoană îl va primi sau îl va putea accesa, în contextul sau în cadrul instituțiilor de învățământ și formare profesională la toate nivelurile;

(d) sisteme de IA destinate a fi utilizate pentru monitorizarea și detectarea comportamentului interzis al elevilor și studenților în timpul testelor, în contextul sau în cadrul instituțiilor de educație și 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 direcționate în mod specific, pentru a analiza și a filtra candidaturile pentru locuri de muncă și pentru a evalua candidații;

(b) sisteme de IA destinate a fi utilizate pentru a lua decizii care afectează termenii relațiilor legate de muncă, promovarea și încetarea relațiilor contractuale legate de muncă, pentru a aloca sarcini pe baza comportamentului individual sau a trăsăturilor ori caracteristicilor personale sau pentru a monitoriza și evalua performanța și comportamentul persoanelor aflate în astfel de relații.

5. Accesul la servicii private esențiale 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 de asistență publică esențiale, inclusiv servicii de îngrijiri de sănătate, 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 utilizate în scopul detectării fraudelor financiare;

(c) 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;

(d) sisteme de IA destinate pentru a evalua și a clasifica apelurile de urgență efectuate de persoane fizice sau pentru a distribui ori pentru a stabili prioritatea în distribuirea serviciilor de primă intervenție de urgență, inclusiv de către poliție, pompieri și asistența medicală, precum și în cadrul sistemelor de triaj de urgență pentru pacienți.

6. Aplicarea legii, în măsura în care utilizarea lor este permisă în temeiul dreptului Uniunii sau intern relevant:

(a) sisteme de IA destinate a fi utilizate de către sau în numele autorităților de aplicare a legii sau de către instituțiile, organele, oficiile ori agențiile Uniunii în sprijinul autorităților de aplicare a legii sau în numele acestora pentru a evalua riscul ca o persoană fizică să devină victima unor infracțiuni;

(b) sisteme de IA destinate a fi utilizate de către sau în numele autorităților de aplicare a legii ca poligrafe sau instrumente similare sau de către instituțiile, organele, oficiile ori agențiile Uniunii în sprijinul autorităților de aplicare a legii;

(c) sisteme de IA destinate a fi utilizate de către sau în numele autorităților de aplicare a legii sau de instituțiile, organele, oficiile ori agențiile Uniunii în sprijinul autorităților de aplicare a legii pentru a evalua fiabilitatea probelor în cursul investigării sau al urmăririi penale a infracțiunilor;

(d) sisteme de IA destinate a fi utilizate de către autoritățile de aplicare a legii sau în numele acestora de către instituțiile, organele, oficiile sau agențiile Uniunii în sprijinul autorităților de aplicare a legii pentru evaluarea riscului ca o persoană fizică să comită infracțiuni sau să recidiveze, nu doar 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 ori comportamentul infracțional anterior al unor persoane fizice sau grupuri;

(e) sisteme de IA destinate a fi utilizate de către sau în numele autorităților de aplicare a legii sau de către instituțiile, organele, oficiile ori agențiile Uniunii în sprijinul autorităților de aplicare a legii 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 urmăririi penale a infracțiunilor.

7. Migrație, azil și gestionare a controlului la frontiere, în măsura în care utilizarea lor este permisă în temeiul dreptului Uniunii sau intern relevant:

(a) sisteme de IA destinate a fi utilizate de către sau în numele autorităților publice competente sau de către instituțiile, organele, oficiile ori agențiile Uniunii drept poligrafe sau instrumente similare;

(b) sisteme de IA destinate a fi utilizate de către sau în numele autorităților publice competente sau de către instituțiile, organele, oficiile ori agențiile Uniunii pentru evaluarea unui risc, inclusiv a unui risc de securitate, a unui risc de migrație ilegală sau a unui risc pentru sănătate din partea unei persoane fizice care intenționează să intre sau care a intrat pe teritoriul unui stat membru;

(c) sisteme de IA destinate a fi utilizate de către sau în numele autorităților publice competente sau de către instituțiile, organele, oficiile ori agențiile Uniunii pentru a asista autoritățile publice competente în examinarea cererilor de azil, de viză sau de permise de ședere și a plângerilor aferente în ceea ce privește eligibilitatea persoanelor fizice care solicită un statut, inclusiv în evaluările conexe ale fiabilității probelor;

(d) sisteme de IA destinate a fi utilizate de către sau în numele autorităților publice competente sau de către instituțiile, organele, oficiile sau agențiile Uniunii, în contextul migrației, azilului sau gestionării controlului la frontiere, în scopul detectării, recunoașterii sau identificării persoanelor fizice, cu excepția verificării documentelor de călătorie.

8. Administrarea justiției și procesele democratice:

(a) sisteme de IA destinate a fi utilizate de către sau în numele unei autorități judiciare pentru a asista o autoritate judiciară în cercetarea și interpretarea faptelor sau a legii, precum și în aplicarea legii la un set concret de fapte sau destinate a fi utilizate în mod similar în soluționarea alternativă a litigiilor;

(b) sisteme de IA destinate a fi utilizate pentru a influența rezultatul unei alegeri sau al unui referendum ori comportamentul de vot al persoanelor fizice în exercitarea votului lor la alegeri sau referendumuri. Acestea nu includ sistemele de IA la ale căror rezultate nu sunt expuse direct persoane fizice, cum ar fi instrumentele utilizate pentru organizarea, optimizarea sau structurarea campaniilor politice din punct de vedere administrativ sau logistic.

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, incluzând:

   (a) scopul său preconizat, numele/denumirea furnizorului și versiunea sistemului, care reflectă relația sa cu versiunile anterioare;

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

   (c) versiunile software-ului sau ale firmware-ului relevant și orice cerințe legate de actualizările versiunilor;

   (d) descrierea tuturor formelor sub care sistemul de IA este introdus pe piață sau este pus în funcțiune, cum ar fi pachete software integrate în hardware, sisteme care pot fi descărcate sau IPA;

   (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) o descriere de bază a interfeței cu utilizatorul furnizate implementatorului;

(h) instrucțiuni de utilizare pentru implementator și o descriere de bază a interfeței cu utilizatorul furnizate implementatorului, după caz;

2. O descriere detaliată a elementelor sistemului de IA și a procesului de dezvoltare a acestuia, incluzând:

(a) metodele și etapele parcurse pentru dezvoltarea sistemului de IA, inclusiv, dacă este cazul, recurgerea la sisteme sau instrumente preantrenate 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, incluzând justificarea și ipotezele asumate, inclusiv în ceea ce privește persoanele sau grupurile de persoane în legătură cu care se intenționează să fie utilizat sistemul; principalele opțiuni de clasificare; ce anume este proiectat să optimizeze sistemul și relevanța diverșilor parametri; descrierea rezultatelor preconizate ale sistemului și a calității preconizate a acestora; deciziile cu privire la orice posibil compromis făcut în ceea ce privește soluțiile tehnice adoptate în vederea respectării cerințelor prevăzute în capitolul III secțiunea 2;

(c) descrierea arhitecturii sistemului, care explică modul în care componentele de software se bazează una pe alta sau se susțin reciproc și se integrează în prelucrarea generală; 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 antrenament 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 implementatori, în conformitate cu articolul 13 alineatul (3) litera (d);

(f) după caz, 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 capitolul III secțiunea 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 acuratețea, robustețea și conformitatea cu alte cerințe relevante prevăzute în capitolul III secțiunea 2, precum și impactul potențial discriminatoriu; jurnalele de testare și toate rapoartele de testare datate și semnate de persoanele responsabile, inclusiv în ceea ce privește modificările prestabilite menționate la litera (f);

(h) măsurile de securitate cibernetică instituite;

3. Informații detaliate privind monitorizarea, funcționarea și controlul sistemului de IA, în special în ceea ce privește: capabilitățile 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 în materie de discriminare, având în vedere scopul preconizat al sistemului de IA; măsurile de supraveghere umană necesare în conformitate cu articolul 14, inclusiv măsurile tehnice instituite pentru a facilita interpretarea rezultatelor sistemelor de IA de către implementatori; specificații privind datele de intrare, după caz;

4. O descriere a gradului de adecvare a indicatorilor de performanță pentru sistemul de IA specific;

5. O descriere detaliată a sistemului de gestionare a riscurilor în conformitate cu articolul 9;

6. O descriere a modificărilor relevante aduse de furnizor sistemului de-a lungul ciclului său de viață;

7. 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 capitolul III secțiunea 2, inclusiv o listă a altor standarde și specificații tehnice relevante aplicate;

8. O copie a declarației de conformitate UE menționată la articolul 47;

9. O descriere detaliată a sistemului instituit pentru evaluarea performanței sistemului de IA în etapa ulterioară introducerii pe piață în conformitate cu articolul 72, inclusiv planul de monitorizare ulterioară introducerii pe piață menționat la articolul 72 alineatul (3).

ANEXA V

Declarația de conformitate UE

Declarația de conformitate UE menționată la articolul 47 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/denumirea și adresa furnizorului sau, după caz, ale reprezentantului autorizat al acestuia;

3. O declarație potrivit căreia declarația de conformitate UE menționată la articolul 47 este emisă pe răspunderea exclusivă a furnizorului;

4. O declarație potrivit căreia sistemul de IA este conform cu prezentul regulament și, după caz, cu orice alt act legislativ relevant al Uniunii care prevede emiterea declarației de conformitate UE menționată la articolul 47;

5. Dacă un sistem de IA implică prelucrarea de date cu caracter personal, o declarație că sistemul de IA respectiv este conform cu Regulamentele (UE) 2016/679 și (UE) 2018/1725 și Directiva (UE) 2016/680;

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

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

8. Locul și data emiterii declarației, numele și funcția persoanei care a semnat-o, precum și o indicație pentru cine sau în numele cui a semnat, 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, 3 și 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 capitolul III secțiunea 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 72, 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/denumirea și adresa furnizorului, iar, dacă cererea este depusă de către un reprezentant 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 cărora li se aplică acesta 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 căruia i se aplică sistemul de management al calității menționat la punctul 3.

4.2. Cererea include:

(a) numele/denumirea 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 limitându-se 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, după caz și sub rezerva unor garanții de securitate, prin 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 capitolul III secțiunea 2. Ori de câte ori organismul notificat nu este satisfăcut de testele efectuate de furnizor, organismul notificat efectuează el însuși direct teste adecvate, după caz.

4.5. În cazul în care este necesar pentru a evalua conformitatea sistemului de IA cu grad ridicat de risc cu cerințele prevăzute în capitolul III secțiunea 2, după ce toate celelalte modalități rezonabile de verificare a conformității au fost epuizate ori s-au dovedit a fi insuficiente și în urma unei cereri motivate, organismului notificat i se acordă, de asemenea, acces la modelele de antrenament sau modelele antrenate ale sistemului de IA, inclusiv la parametrii săi relevanți. Acest acces face obiectul dreptului existent al Uniunii privind protecția proprietății intelectuale și al secretelor comerciale.

4.6. Decizia organismului notificat 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 capitolul III secțiunea 2, organismul notificat eliberează un certificat de evaluare a documentației tehnice al Uniunii. Certificatul indică numele/denumirea 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 capitolul III secțiunea 2, organismul notificat refuză eliberarea unui certificat de evaluare a documentației tehnice al Uniunii și informează solicitantul în consecință, 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 de evaluare motivată a organismului notificat prin care se refuză eliberarea certificatului de evaluare a documentației tehnice al Uniunii conține considerații specifice privind calitatea datelor 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 evaluată de organismul notificat care a eliberat certificatul de evaluare a documentației tehnice al Uniunii. 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 în alt mod 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 de evaluare a documentației tehnice al Uniunii. 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 de evaluare a documentației tehnice al Uniunii.

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 respectă în mod corespunzător termenele 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 de evaluare a documentației tehnice al Uniunii.

ANEXA VIII

Informațiile care trebuie să fie prezentate la înregistrarea
sistemelor de IA cu grad ridicat de risc în conformitate cu articolul 49

Secțiunea A – Informațiile care trebuie să fie prezentate de furnizorii de sisteme de IA
cu grad ridicat de risc în conformitate cu articolul 49 alineatul (1)

Se furnizează și, ulterior, se actualizează următoarele informații referitoare la sistemele de IA cu grad ridicat de risc care se înregistrează în conformitate cu articolul 49 alineatul (1):

1. Numele/denumirea, adresa și datele de contact ale furnizorului;

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

3. Numele, adresa și datele de contact ale reprezentantului autorizat, după caz;

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

5. O descriere a scopului preconizat al sistemului de IA și a componentelor și funcțiilor sprijinite prin acest sistem de IA;

6. O descriere de bază și concisă a informațiilor utilizate de sistem (date, date de intrare) și a logicii sale de funcționare;

7. Statutul sistemului de IA (pe piață sau în funcțiune; nu mai este pe piață/în funcțiune, rechemat);

8. Tipul, numărul și data expirării certificatului eliberat de organismul notificat și denumirea sau numărul de identificare al organismului notificat respectiv, după caz;

9. O copie scanată a certificatului menționat la punctul 8, după caz;

10. Orice stat membru în care sistemul de IA a fost introdus pe piață, pus în funcțiune sau pus la dispoziție în Uniune;

11. O copie a declarației de conformitate UE prevăzută la articolul 47;

12. Instrucțiuni de utilizare electronice; aceste informații nu se furnizează pentru sistemele de IA cu grad ridicat de risc în domeniul aplicării legii și al migrației, al azilului și al gestionării controlului la frontiere menționate în anexa III punctele 1, 6 și 7;

13. Un URL pentru informații suplimentare (opțional).

Secțiunea B – Informațiile care trebuie să fie prezentate de furnizorii de sisteme de IA cu grad ridicat de risc în conformitate cu articolul 49 alineatul (2)

Se furnizează și, ulterior, se actualizează următoarele informații referitoare la sistemele de IA care se înregistrează în conformitate cu articolul 49 alineatul (2):

1. Numele/denumirea, adresa și datele de contact ale furnizorului;

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

3. Numele, adresa și datele de contact ale reprezentantului autorizat, după caz;

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

5. Descrierea scopului preconizat al sistemului de IA;

6. Condiția sau condițiile prevăzute la articolul 6 alineatul (3) pe baza cărora sistemul de IA este considerat ca neprezentând un grad ridicat de risc;

7. Un scurt rezumat al motivelor pentru care sistemul de IA este considerat ca neprezentând un grad ridicat de risc în aplicarea procedurii prevăzute la articolul 6 alineatul (3);

8. Statutul sistemului de IA (pe piață sau în funcțiune; nu mai este pe piață/în funcțiune, rechemat);

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

Secțiunea C – Informațiile care trebuie să fie prezentate de implementatorii de sistemele de IA cu grad ridicat de risc în conformitate cu articolul 49 alineatul (3)

Se furnizează și, ulterior, se actualizează următoarele informații referitoare la sistemele de IA cu grad ridicat de risc care se înregistrează în conformitate cu articolul 49:

1. Numele/denumirea, adresa și datele de contact ale implementatorului;

2. Numele, adresa și datele de contact ale oricărei persoane care transmite informații în numele implementatorului;

3. URL-ul introducerii sistemului de IA în baza de date a UE de către furnizorul său;

4. Un rezumat al constatărilor evaluării impactului asupra drepturilor fundamentale, efectuată în conformitate cu articolul 27;

5. Un rezumat al evaluării impactului asupra protecției datelor care a fost efectuată în conformitate cu articolul 35 din Regulamentul (UE) 2016/679 sau cu articolul 27 din Directiva (UE) 2016/680, astfel cum se specifică la articolul 26 alineatul (8) din prezentul regulament, după caz.

ANEXA IX

Informațiile care trebuie să fie prezentate la înregistrarea sistemelor de IA cu grad ridicat de risc enumerate în anexa III în legătură cu testarea în condiții reale, în conformitate cu articolul 60

Se furnizează și, ulterior, se actualizează următoarele informații referitoare la testarea în condiții reale care trebuie înregistrate în conformitate cu articolul 60:

1. Un număr unic de identificare la nivelul întregii Uniuni al testării în condiții reale;

2. Numele/denumirea și datele de contact ale furnizorului sau ale potențialului furnizor și ale implementatorilor 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 X

Actele legislative ale 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) Regulamentul (UE) 2021/1133 al Parlamentului European și al Consiliului din 7 iulie 2021 de modificare a Regulamentelor (UE) nr. 603/2013, (UE) 2016/794, (UE) 2018/1862, (UE) 2019/816 și (UE) 2019/818 în ceea ce privește stabilirea condițiilor de acces la celelalte sisteme de informații ale UE în scopuri legate de Sistemul de informații privind vizele (JO L 248, 13.7.2021, p. 1);

(b) Regulamentul (UE) 2021/1134 al Parlamentului European și al Consiliului din 7 iulie 2021 de modificare a Regulamentelor (CE) nr. 767/2008, (CE) nr. 810/2009, (UE) 2016/399, (UE) 2017/2226, (UE) 2018/1240, (UE) 2018/1860, (UE) 2018/1861, (UE) 2019/817 și (UE) 2019/1896 ale Parlamentului European și ale Consiliului și de abrogare a Deciziilor 2004/512/CE și 2008/633/JAI ale Consiliului, în scopul reformării Sistemului de informații privind vizele (JO L 248, 13.7.2021, p. 11).

3. Eurodac

Regulamentul (UE) 2024/... al Parlamentului European și al Consiliului privind instituirea sistemului „Eurodac” pentru compararea datelor biometrice în scopul aplicării eficace a Regulamentelor (UE) 2024/… și (UE) 2024/… ale Parlamentului European și ale Consiliului și a Directivei 2001/55/CE a Consiliului și al identificării resortisanților din țări terțe și a apatrizilor în situație de ședere ilegală și privind cererile de comparare cu datele Eurodac prezentate de autoritățile de aplicare a legii din statele membre și de Europol cu scopul de a asigura respectarea legii, de modificare a Regulamentelor (UE) 2018/1240 și (UE) 2019/818 ale Parlamentului European și ale Consiliului și de abrogare a Regulamentului (UE) nr. 603/2013 al Parlamentului European și al Consiliului[+].

4. Sistemul de intrare/ieșire

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).

[+] JO: a se introduce în text numărul regulamentului conținut în documentul PE-CONS 15/24 [2016/0132 (COD)] și a se introduce în nota de subsol numărul, data, titlul și referința de publicare în JO a regulamentului respectiv.

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

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 și de modificare a Regulamentelor (CE) nr. 767/2008, (UE) 2016/399, (UE) 2017/2226, (UE) 2018/1240, (UE) 2018/1726 și (UE) 2018/1861 ale Parlamentului European și ale Consiliului și a Deciziilor 2004/512/CE și 2008/633/JAI ale Consiliului (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 și de modificare a Regulamentelor (UE) 2018/1726, (UE) 2018/1862 și (UE) 2019/816 (JO L 135, 22.5.2019, p. 85).

ANEXA XI

Documentația tehnică menționată la articolul 53 alineatul (1) litera (a) – documentația tehnică pentru furnizorii de modele de IA de uz general

Secțiunea 1

Informații care trebuie furnizate de toți furnizorii de modele de IA de uz general

Documentația tehnică menționată la articolul 53 alineatul (1) litera (a) conține cel puțin următoarele informații, în funcție de dimensiunea și profilul de risc al modelului:

1. O descriere generală a modelului de IA de uz general, incluzând:

   (a) sarcinile pe care modelul este destinat să le îndeplinească, precum și tipul și natura sistemelor de IA în care acesta poate fi integrat;

   (b) politicile de utilizare acceptabile aplicabile;

   (c) data eliberării și metodele de distribuție;

   (d) arhitectura și numărul de parametri;

   (e) modalitatea (de exemplu, text, imagine) și formatul datelor de intrare și de ieșire;

   (f) licența.

2. O descriere detaliată a elementelor modelului menționate la punctul 1 și informații relevante privind procesul de dezvoltare, incluzând următoarele elemente:

(a) mijloacele tehnice (de exemplu, instrucțiuni de utilizare, infrastructură, instrumente) necesare pentru integrarea modelului de IA de uz general în sistemele de IA;

(b) specificațiile de proiectare ale modelului și ale procesului de antrenare, inclusiv metodologiile și tehnicile de antrenare, principalele opțiuni de proiectare, inclusiv justificarea și ipotezele formulate; ce anume este proiectat să optimizeze modelul și relevanța diverșilor parametri, după caz;

(c) informații privind datele utilizate pentru antrenare, testare și validare, după caz, inclusiv tipul și proveniența datelor și metodologiile de organizare (de exemplu, curățare, filtrare etc.), numărul de puncte de date, domeniul de aplicare și principalele caracteristici ale acestora; modul în care au fost obținute și selectate datele, precum și toate celelalte măsuri de detectare a caracterului inadecvat al surselor de date și metode de detectare a prejudecăților identificabile, după caz;

(d) resursele de calcul utilizate pentru antrenarea modelului (de exemplu, numărul de operații în virgulă mobilă), timpul de antrenare și alte detalii relevante legate de antrenare;

(e) consumul de energie cunoscut sau estimat al modelului.

În ceea ce privește litera (e), în cazul în care consumul de energie al modelului este necunoscut, consumul de energie se poate baza pe informații privind resursele de calcul utilizate.

Secțiunea 2

Informații suplimentare care trebuie furnizate

de furnizorii de modele de IA de uz general cu risc sistemic

1. O descriere detaliată a strategiilor de evaluare, inclusiv a rezultatelor evaluării, pe baza protocoalelor și instrumentelor de evaluare publice disponibile sau a altor metodologii de evaluare. Strategiile de evaluare includ criterii de evaluare, indicatori și metodologia de identificare a limitărilor.

2. După caz, o descriere detaliată a măsurilor puse în aplicare în scopul efectuării de testări contradictorii interne și/sau externe (de exemplu, testare de tipul „echipa roșie”) și de adaptări ale modelelor, inclusiv aliniere și calibrare.

3. După caz, o descrierea detaliată a arhitecturii sistemului, care explică modul în care componentele de software se bazează una pe alta sau se susțin reciproc și se integrează în prelucrarea generală.

ANEXA XII

Informațiile privind transparența menționate la articolul 53 alineatul (1) litera (b)
- documentația tehnică pentru furnizorii de modele de IA de uz general
către furnizorii din aval care integrează modelul în sistemul lor de IA

Informațiile menționate la articolul 53 alineatul (1) litera (b) conțin cel puțin următoarele:

1. O descriere generală a modelului de IA de uz general, incluzând:

   (a) sarcinile pe care modelul este destinat să le îndeplinească, precum și tipul și natura sistemelor de IA în care acesta poate fi integrat;

   (b) politicile de utilizare acceptabile aplicabile;

   (c) data eliberării și metodele de distribuție;

   (d) modul în care modelul interacționează sau poate fi utilizat pentru a interacționa cu hardware-ul sau cu software-ul care nu face parte din model în sine, după caz;

   (e) versiunile software-ului relevant legat de utilizarea modelului de IA de uz general, după caz;

   (f) arhitectura și numărul de parametri;

   (g) modalitatea (de exemplu, text, imagine) și formatul datelor de intrare și de ieșire;

   (h) licența modelului.

2. O descriere a elementelor modelului și a procesului de dezvoltare a acestuia, incluzând:

(a) mijloacele tehnice (de exemplu, instrucțiuni de utilizare, infrastructură, instrumente) necesare pentru integrarea modelului de IA de uz general în sistemele de IA;

(b) modalitatea (de exemplu, text, imagine) și formatul datelor de intrare și de ieșire și dimensiunea maximă a acestora (de exemplu, lungimea ferestrei de context etc.);

(c) informații privind datele utilizate pentru antrenare, testare și validare, după caz, inclusiv tipul și proveniența datelor și metodologiile de organizare.

ANEXA XIII

Criterii pentru desemnarea modelelor de IA de uz general
cu risc sistemic menționate la articolul 51

Pentru a stabili dacă un model de IA de uz general are capabilitățile prevăzute la articolul 51 alineatul (1) litera (a) sau un impact echivalent acestora, Comisia ia în considerare următoarele criterii:

(a) numărul de parametri ai modelului;

(b) calitatea sau dimensiunea setului de date, de exemplu, măsurate în tokenuri;

(c) volumul de calcul utilizat pentru antrenarea modelului, măsurat în operații în virgulă mobilă sau indicat printr-o combinație de alte variabile, cum ar fi costul estimat al antrenării, timpul estimat necesar pentru antrenare sau consumul estimat de energie pentru antrenare;

(d) modalitățile de intrare și de ieșire ale modelului, cum ar fi text către text (modele lingvistice de mari dimensiuni), text către imagine și multimodalitatea, și pragurile conform celui mai avansat stadiu al tehnologiei pentru determinarea capabilităților cu impact ridicat pentru fiecare modalitate, precum și tipul specific de date de intrare și de ieșire (de exemplu, secvențe biologice);

(e) valorile de referință și evaluările capabilităților modelului, inclusiv luând în considerare numărul de sarcini posibile fără antrenare suplimentară, adaptabilitatea la învățarea de sarcini noi și distincte, nivelul său de autonomie și scalabilitate, instrumentele la care are acces;

(f) dacă are un impact ridicat asupra pieței interne din cauza amplorii utilizării sale, care este prezumat atunci când a fost pus la dispoziția a cel puțin 10 000 de utilizatori comerciali înregistrați stabiliți în Uniune;

(g) numărul de utilizatori finali înregistrați.