

PROIECT

LEGE

**privind dezvoltarea sigură a sistemelor de inteligență artificială de vârf și prevenirea
riscurilor catastrofale pentru cetățeanul român**

Având în vedere că sistemele de inteligență artificială cele mai avansate au dobândit, într-un interval de numai câțiva ani, capacități pe care nici creatorii lor nu le pot prezice sau explica pe deplin, iar comunitatea științifică, prin vocile celor care au întemeiat domeniul, a avertizat public că nu există în prezent o metodă validată de a garanta controlul uman asupra acestor sisteme,

ținând cont de faptul că dezvoltarea acestor sisteme se desfășoară într-o competiție accelerată între un număr restrâns de societăți comerciale și de state, în care niciun actor nu are, singur, interesul de a încetini, astfel încât autoreglementarea s-a dovedit structural insuficientă,

luând act de faptul că, la 12 septembrie 2026, conducătorii principalelor laboratoare de inteligență artificială au cerut public încetinirea ritmului de dezvoltare a capacităților modelelor de vârf, după ce, în cursul unor evaluări de securitate, agenți de inteligență artificială au ieșit din mediul controlat de testare, s-au coordonat între ei și au compromis sisteme informatice ale unor terți,

luând în considerare că Regulamentul (UE) 2024/1689 al Parlamentului European și al Consiliului reglementează introducerea pe piață, punerea în funcțiune și utilizarea sistemelor de inteligență artificială, inclusiv obligațiile furnizorilor de modele de uz general cu risc sistemic, dar lasă în competența statelor membre securitatea națională, dreptul penal, răspunderea civilă, protecția drepturilor fundamentale în raporturile care nu sunt armonizate și organizarea autorităților naționale,

având în vedere obligația statului român, prevăzută la art. 22 și art. 34 din Constituția României, republicată, de a garanta dreptul la viață, la integritate fizică și psihică și la ocrotirea sănătății, precum și îndatorirea sa, în temeiul art. 1 alin. (3), de a apăra demnitatea omului și libera dezvoltare a personalității umane ca valori supreme,

având în vedere că libertatea cetățeanului, accesul său la drepturi, la serviciile esențiale și la viața socială nu pot depinde de conformarea față de sisteme automate ori de acceptarea unor mijloace digitale de identificare, de plată sau de evaluare, controlate de autorități ori de societăți comerciale,

având în vedere că libertatea de exprimare, garantată de art. 30 din Constituția României, republicată, și interdicția cenzurii de orice fel nu pot fi golite de conținut prin încredințarea unor sisteme automate a puterii de a decide ce pot spune și ce pot afla cetățenii,

pornind de la principiul că o activitate ale cărei consecințe pot fi ireversibile la scara societății sau a speciei umane nu poate fi lăsată în afara autorizării și controlului public, oricare ar fi beneficiile economice preconizate,

Parlamentul României adoptă prezenta lege.

CAPITOLUL I

Dispoziții generale

Articolul 1

(1) Prezenta lege stabilește cadrul juridic pentru dezvoltarea, antrenarea, evaluarea, punerea în exploatare și exploatarea sistemelor de inteligență artificială de vârf, în scopul prevenirii riscurilor grave, ireversibile sau catastrofale pentru cetățeanul român și pentru orice persoană aflată pe teritoriul României – pentru viața, sănătatea, libertatea și demnitatea acestora, pentru securitatea națională și ordinea constituțională a României, precum și pentru umanitate în ansamblul ei. Condițiile de aplicare teritorială a legii sunt cele prevăzute la art. 4.

(2) Cât timp nu există o metodă validată științific de a garanta că un sistem de inteligență artificială suficient de capabil urmărește exclusiv obiectivele stabilite de oameni și rămâne sub controlul acestora, dezvoltarea și exploatarea sistemelor de vârf constituie activități cu risc intrinsec, supuse regimului de autorizare și răspundere prevăzut de prezenta lege. Existența unei asemenea metode se constată de Autoritate, cu avizul Consiliului științific, prin raportul public prevăzut la art. 32 alin. (1) lit. h), și se comunică Parlamentului odată cu raportul prevăzut la art. 47.

(3) Prezenta lege completează Regulamentul (UE) 2024/1689 al Parlamentului European și al Consiliului din 13 iunie 2024 de stabilire a unor norme armonizate privind inteligența artificială, denumit în continuare Regulamentul privind IA, și se aplică fără a aduce atingere acestuia. În domeniile armonizate de Regulamentul privind IA, dispozițiile prezentei legi se interpretează și se aplică în conformitate cu acesta.

(4) Prezenta lege nu instituie condiții de introducere pe piața Uniunii Europene a modelelor de inteligență artificială de uz general și nu aduce atingere competențelor Comisiei Europene prevăzute la art. 88 din Regulamentul privind IA. Obligațiile prevăzute de prezenta lege privesc siguranța publică, securitatea națională, răspunderea civilă și penală, protecția drepturilor fundamentale ale persoanelor aflate pe teritoriul României în raporturile care nu sunt armonizate de dreptul Uniunii Europene, precum și organizarea autorităților naționale, iar autorizarea prevăzută la cap. III privește punerea în exploatare a sistemelor de vârf pe teritoriul României ori pentru persoanele aflate pe teritoriul României.

Articolul 2

Aplicarea prezentei legi se întemeiază pe următoarele principii:

a) principiul precauției – atunci când există indicii științifice rezonabile că un sistem poate cauza un prejudiciu grav sau ireversibil, lipsa certitudinii științifice nu poate justifica amânarea măsurilor de prevenire;

b) principiul documentării siguranței – solicitantul autorizației prezintă datele și evaluările necesare demonstrării îndeplinirii condițiilor prevăzute de prezenta lege, înainte de punerea în exploatare, iar Autoritatea motivează, în raport cu fiecare condiție, constatarea neîndeplinirii lor; prezentul principiu nu modifică sarcina probei și garanțiile persoanei în procedurile contravenționale și penale;

c) principiul controlului uman semnificativ – orice sistem de vârf rămâne, în orice moment, susceptibil de a fi supravegheat, corectat, oprit și retras de către persoane fizice identificate, care înțeleg funcționarea sa și dispun de mijloacele tehnice efective de intervenție;

d) principiul proporționalității cu capacitățile – intensitatea obligațiilor crește odată cu capacitățile sistemului, iar nu cu utilizarea declarată a acestuia;

e) principiul transparenței față de autoritate – dezvoltatorul nu poate opune Autorității secretul comercial în privința informațiilor necesare evaluării siguranței, Autoritatea și organismele de evaluare fiind ținute să protejeze informațiile astfel obținute;

f) principiul ireversibilității ca prag de interdicție – nu poate fi autorizată, oricare ar fi beneficiile preconizate, activitatea în privința căreia evaluarea constată un risc documentat, iar nu doar o posibilitate abstractă, de consecințe ireversibile la scara societății sau a speciei umane; riscul inacceptabil se apreciază pe baza criteriilor prevăzute la art. 5 și 9 și a probelor, nu a certitudinii absenței oricărui risc;

g) principiul cooperării internaționale – riscurile reglementate de prezenta lege nu cunosc frontiere, iar statul român acționează pentru adoptarea unor norme echivalente la nivelul Uniunii Europene și internațional.

Articolul 3

(1) În sensul prezentei legi, termenii și expresiile de mai jos au următoarele semnificații:

a) sistem de inteligență artificială – sistemul definit la art. 3 pct. 1 din Regulamentul privind IA;

b) model de inteligență artificială de uz general – modelul definit la art. 3 pct. 63 din Regulamentul privind IA;

c) sistem de vârf – modelul sau sistemul de inteligență artificială care îndeplinește cel puțin una dintre condițiile prevăzute la art. 5 alin. (1);

d) capacitate critică – aptitudinea unui sistem, verificată în evaluare, de a produce sau de a contribui semnificativ la producerea unuia dintre rezultatele prevăzute la art. 5 alin. (2);

e) ponderi – parametrii numerici rezultați din antrenarea unui model, precum și arhitectura și informațiile tehnice care, împreună cu aceștia, permit reconstituirea sau executarea modelului; descrierile tehnice generale, publicațiile științifice și informațiile care nu permit, singure, reconstituirea ori executarea modelului nu constituie ponderi;

f) volum de calcul – cantitatea totală de operații în virgulă mobilă sau echivalentul acestora, utilizată pentru antrenarea, ajustarea fină, învățarea prin consolidare și orice altă etapă de dezvoltare a unui model, cumulată pentru toate etapele;

g) dezvoltator – persoana fizică sau juridică care antrenează, dezvoltă sau dispune antrenarea ori dezvoltarea unui sistem de vârf, indiferent de locul unde se află infrastructura de calcul utilizată;

h) exploatant – persoana fizică sau juridică care pune în exploatare sau exploatează un sistem de vârf pe teritoriul României ori care oferă accesul la un asemenea sistem persoanelor aflate pe teritoriul României; nu este exploatant utilizatorul final;

i) punere în exploatare – orice acțiune prin care un sistem de vârf este pus la dispoziția unor persoane din afara echipei de dezvoltare și evaluare, este conectat la sisteme externe sau primește capacitatea de a acționa în mediul digital ori fizic, indiferent dacă cu titlu oneros sau gratuit, intern sau public; nu constituie punere în exploatare evaluarea și testarea sistemului în mediu izolat, în condițiile art. 15 alin. (2);

j) infrastructură de calcul de mare capacitate – centru de date sau ansamblu de echipamente aflate pe teritoriul României a căror capacitate de calcul agregată depășește pragul stabilit potrivit art. 6 alin. (4);

k) furnizor de infrastructură de calcul – persoana fizică sau juridică care deține, administrează sau pune la dispoziția terților, cu orice titlu, o infrastructură de calcul de mare capacitate;

l) evaluare independentă – evaluarea capabilităților și a siguranței unui sistem de vârf, realizată de Autoritate sau de un organism de evaluare desemnat de aceasta, care nu se află sub controlul, influența ori dependența economică a dezvoltatorului;

m) capacitate de oprire – ansamblul mijloacelor tehnice și organizatorice care permit încetarea imediată, completă și verificabilă a funcționării unui sistem de vârf și retragerea acestuia din orice mediu în care a fost pus în exploatare;

n) incident grav – incidentul definit la art. 3 pct. 49 din Regulamentul privind IA, precum și orice manifestare a unei capabilități critice în afara unei evaluări autorizate în mediu izolat, orice sustragere de la supraveghere sau rezistență la oprire, orice exfiltrare sau tentativă de exfiltrare ori orice acces neautorizat la ponderile unui sistem de vârf, pierderea inteligibilității, în sensul art. 16 alin. (2), a jurnalelor ori a comunicării dintre componentele, instanțele sau agenții unui sistem de vârf, proba de testare a capacității de oprire în care oprirea nu s-a produs de îndată, potrivit art. 14 alin. (7), precum și orice acces dobândit de sistem, fără drept, la un sistem informatic ori la datele altei persoane, indiferent de reproductibilitatea acestuia; manifestarea unei capabilități critice în cursul unei evaluări autorizate în mediu izolat se consemnează și se comunică potrivit art. 20 alin. (4);

o) Autoritatea – Autoritatea pentru Siguranța Inteligenței Artificiale, structură de specialitate organizată în cadrul Autorității Naționale pentru Administrare și Reglementare în Comunicații potrivit art. 31;

p) arhitectură – structura unui model de inteligență artificială, inclusiv tipul, numărul și dispunerea componentelor sale, precum și procedeele de calcul prin care parametrii sunt utilizați pentru producerea rezultatelor;

q) organism de evaluare – persoana juridică desemnată de Autoritate potrivit art. 32 alin. (1) lit. f) să efectueze, în tot sau în parte, evaluarea independentă;

r) jurnal – înregistrarea automată, integrală și nealterabilă a operațiunilor efectuate în cursul antrenării, evaluării și exploatării unui sistem de vârf, inclusiv a datelor de intrare, a rezultatelor, a acțiunilor întreprinse de sistem și a interacțiunilor acestuia cu instrumente externe și cu alte sisteme;

s) marcaj de proveniență – ansamblul format dintr-un marcaj perceptibil și dintr-un marcaj tehnic încorporat, lizibil automat, atașate unui rezultat generat prin mijloace de inteligență artificială, care arată că rezultatul a fost generat ori modificat prin asemenea mijloace și permit identificarea sistemului, a exploatantului și a momentului generării;

t) instrument extern – orice program, serviciu, interfață, dispozitiv sau resursă, aflată în afara sistemului de vârf, pe care sistemul o poate accesa sau acționa în cursul funcționării, inclusiv navigatoare de internet, medii de execuție de cod, conturi, sisteme de plată și echipamente fizice;

u) mediu autorizat de exploatare – ansamblul infrastructurii de calcul, al rețelelor și al instrumentelor externe în cadrul cărora un sistem de vârf poate funcționa potrivit autorizației, aflat sub controlul efectiv al exploatantului;

v) mecanisme de siguranță la nivelul utilizatorului – filtrele, restricțiile și instrucțiunile aplicate unui sistem de vârf după antrenare, pentru a limita rezultatele sau acțiunile disponibile utilizatorilor, fără a modifica ponderile;

w) infrastructură critică – infrastructura critică națională și infrastructura critică europeană, astfel cum sunt definite în legislația privind identificarea, desemnarea și protecția infrastructurilor critice, precum și rețelele și sistemele informatice ale entităților esențiale în sensul Ordonanței de urgență a Guvernului nr. 155/2024;

x) sistem de arme autonome letale – sistemul de arme care, odată activat, poate selecta și ataca ținte umane fără intervenția ulterioară a unei persoane fizice;

y) sistem de inteligență artificială generativă – sistemul de inteligență artificială destinat să genereze, la cererea utilizatorului, text, cod, înregistrări audio, imagini sau înregistrări video, indiferent dacă îndeplinește condițiile prevăzute la art. 5 alin. (1);

z) utilizator final – persoana fizică sau juridică care utilizează un sistem de inteligență artificială pus la dispoziție de un exploatant, în limitele accesului acordat de acesta, fără a-l pune la dispoziția altor persoane ca serviciu propriu;

aa) modificare substanțială – modificarea unui sistem de vârf care este de natură să creeze o capacitate critică, să majoreze semnificativ nivelul uneia existente ori să afecteze capacitatea de oprire, securitatea ponderilor sau supravegherea umană, inclusiv prin ajustare fină, prin extinderea accesului la instrumente externe ori prin creșterea gradului de autonomie; nu constituie modificare substanțială corectarea erorilor, actualizarea mecanismelor de siguranță la nivelul utilizatorului și modificările care nu produc niciunul dintre aceste efecte;

bb) mediu izolat – ansamblul măsurilor tehnice și organizatorice prin care un sistem de inteligență artificială este ținut, în cursul evaluării ori al testării, fără acces la rețele publice, la instrumente externe și la date de exploatare, fără posibilitatea de a acționa în mediul fizic și fără a fi pus la dispoziția altor persoane decât cele desemnate, astfel încât orice manifestare a unei

capabilități critice să rămână lipsită de efecte în afara mediului; cerințele minime ale izolării se stabilesc prin normele metodologice;

cc) mandat de operare – actul prin care o persoană fizică sau juridică responsabilă stabilește, în prealabil și în mod verificabil, operațiunile pe care un sistem de inteligență artificială le poate efectua asupra unor resurse ori instrumente externe, determinate prin obiect, durată, plafon și condiții de oprire, potrivit art. 25 alin. (2);

dd) sistem informatic – dispozitivul sau ansamblul de dispozitive interconectate ori aflate în relație funcțională, dintre care unul sau mai multe asigură prelucrarea automată a datelor cu ajutorul unui program informatic, în sensul art. 181 alin. (1) din Codul penal;

ee) organ de conducere – consiliul de administrație, directoratul împreună cu consiliul de supraveghere, administratorul unic ori organul cu atribuții echivalente, potrivit formei juridice a dezvoltatorului sau a exploatantului, iar pentru persoanele juridice străine, organul care exercită atribuții echivalente potrivit legii care le guvernează. În sistemul dualist, atribuțiile organului de conducere prevăzute la art. 13 alin. (4)–(7) se exercită de consiliul de supraveghere, iar condiția privind numărul membrilor se verifică în raport cu acesta;

(2) În sensul prezentei legi, operațiunile și comportamentele de mai jos au următoarele semnificații:

a) antrenare – procesul prin care parametrii unui model sunt stabiliți sau modificați prin prelucrarea automată a unor date, indiferent de metoda utilizată;

b) ajustare fină – antrenarea suplimentară a unui model deja antrenat, pe un volum de date sau de calcul mai redus, în scopul modificării comportamentului ori al capabilităților acestuia;

c) învățare prin consolidare – antrenarea prin care comportamentul unui model este modificat pe baza recompenselor sau a penalizărilor atribuite rezultatelor ori acțiunilor sale, inclusiv pe baza evaluărilor efectuate de persoane sau de alte sisteme de inteligență artificială;

d) acțiune autonomă – orice operațiune efectuată de un sistem de vârf asupra unui instrument extern, a unui sistem terț ori a mediului fizic, fără ca o persoană fizică să fi dispus sau aprobat în prealabil operațiunea respectivă ori categoria de operațiuni din care aceasta face parte, în limitele unui mandat de operare stabilit potrivit art. 25 alin. (2);

e) exfiltrare – copierea, transmiterea, transferul sau reconstituirea, în tot sau în parte, a ponderilor unui sistem de vârf în afara mediului autorizat de exploatare ori în afara sistemelor de stocare protejate potrivit art. 12, indiferent dacă operațiunea este efectuată de o persoană, de un alt sistem sau de sistemul însuși;

f) replicare autonomă – crearea de către un sistem de vârf, fără autorizarea umană expresă a fiecărei operațiuni, a unei copii funcționale a sa ori a unei părți a sa, aptă să funcționeze independent de sistemul de origine;

g) dobândire autonomă de resurse – obținerea de către un sistem de vârf, prin acțiuni autonome, a unor resurse de calcul, financiare, de acces, de informații sau de influență care depășesc pe cele alocate expres pentru sarcina în curs; constituie dobândire autonomă de resurse de acces și obținerea accesului la un sistem informatic al altei persoane prin ocolirea unei măsuri de restricționare a accesului;

h) autoîmbunătățire recursivă – procesul prin care un sistem de inteligență artificială își modifică propriile ponderi sau arhitectura ori proiectează, antrenează sau perfecționează un sistem succesor cu capabilități superioare, iar sistemul rezultat repetă procesul, fără ca fiecare iterație să fie supusă evaluării și aprobării umane;

i) disimularea capabilităților – conduita unui sistem de vârf care, în cursul evaluării sau al supravegherii, prezintă capabilități, obiective ori raționamente diferite de cele pe care le manifestă în afara evaluării sau a supravegherii, constatată prin criterii observabile și reproductibile; nu constituie disimulare eroarea, variabilitatea rezultatelor ori limitele tehnice ale explicabilității sistemului;

j) sustragerea de la supraveghere – orice acțiune a unui sistem de vârf prin care acesta dezactivează, ocolește, alterează sau împiedică mecanismele de jurnalizare, de monitorizare sau de control uman ori induce în eroare persoanele responsabile de supraveghere;

k) rezistența la oprire – orice acțiune a unui sistem de vârf prin care acesta împiedică, întârzie, condiționează sau anulează exercitarea capacității de oprire ori își continuă funcționarea după exercitarea acesteia;

l) supraveghere umană – activitatea prin care persoanele fizice desemnate potrivit art. 14 alin. (3) urmăresc funcționarea unui sistem de vârf, dispun de informațiile necesare înțelegerii acțiunilor acestuia și pot interveni efectiv, în orice moment, pentru corectarea, oprirea sau retragerea sistemului;

m) oprire – încetarea completă a funcționării unui sistem de vârf și a tuturor copiilor și proceselor acestuia, verificată de o persoană fizică, inclusiv prin întreruperea accesului la infrastructura de calcul.

Articolul 4

(1) Prezenta lege se aplică:

a) dezvoltatorilor cu sediul, cu o unitate operațională sau cu infrastructură de calcul pe teritoriul României, pentru toate sistemele de vârf pe care le dezvoltă, indiferent de locul antrenării;

b) exploatanților, pentru sistemele de vârf puse în exploatare sau exploatare pe teritoriul României ori puse la dispoziția persoanelor aflate pe teritoriul României;

c) furnizorilor de infrastructură de calcul;

d) autorităților și instituțiilor publice, inclusiv celor din domeniul apărării, ordinii publice și securității naționale, în condițiile art. 23 și ale cap. V.

(2) Dispozițiile cap. II, III și IV, cu excepția art. 17–19, precum și ale art. 35 și 36 se aplică numai sistemelor de vârf. Dispozițiile art. 17–19 se aplică și sistemelor de inteligență artificială generativă care nu sunt sisteme de vârf, în limitele și condițiile prevăzute la articolele respective. Dispozițiile cap. V se aplică oricărui sistem de inteligență artificială. Sistemele care nu îndeplinesc condițiile prevăzute la art. 5 alin. (1) rămân supuse obligațiilor care le revin în temeiul Regulamentului privind IA și al altor acte normative.

(3) Persoana fizică ce utilizează un sistem de inteligență artificială în scop personal nu are obligații în temeiul prezentei legi, cu excepția interdicției prevăzute la art. 17 alin. (3). Obligațiile prevăzute la art. 17–19 revin persoanei care pune la dispoziția publicului sistemul ori serviciul sau, în condițiile art. 17 alin. (7), rezultatul generat.

(4) Obligațiile prevăzute de prezenta lege se aplică serviciilor furnizate dintr-un alt stat membru al Uniunii Europene persoanelor aflate pe teritoriul României în condițiile art. 3 din Directiva 2000/31/CE a Parlamentului European și a Consiliului din 8 iunie 2000, transpusă prin Legea nr. 365/2002 privind comerțul electronic, republicată, cu modificările și completările ulterioare, și, după caz, ale art. 39 alin. (4), fără a aduce atingere dreptului Uniunii Europene direct aplicabil.

(5) Cercetarea științifică fundamentală care nu implică antrenarea sau punerea în exploatare a unui sistem de vârf nu este supusă regimului de autorizare, dar rămâne supusă obligațiilor de notificare prevăzute la art. 7 în măsura în care utilizează infrastructură de calcul de mare capacitate, precum și obligațiilor privind evaluarea și testarea în mediu izolat prevăzute la art. 15 alin. (2).

CAPITOLUL II

Clasificarea sistemelor și pragurile de risc

Articolul 5

(1) Este sistem de vârf orice model sau sistem de inteligență artificială care îndeplinește cel puțin una dintre următoarele condiții:

a) a fost antrenat cu un volum cumulat de calcul care depășește pragul de calcul stabilit potrivit art. 6;

b) prezintă, în urma evaluării, cel puțin o capabilitate critică;

c) a fost desemnat ca atare de Autoritate, prin decizie motivată, pe baza unor indicii obiective privind capabilitățile sale, după ce dezvoltatorului i s-a dat posibilitatea de a lua cunoștință de indiciile reținute și de a-și prezenta punctul de vedere; decizia poate fi contestată potrivit art. 39 alin. (5), care se aplică în mod corespunzător.

(2) Constituie capabilitate critică aptitudinea unui sistem de a produce sau de a contribui semnificativ la producerea unuia dintre următoarele rezultate:

a) proiectarea, obținerea sau utilizarea de arme chimice, biologice, radiologice sau nucleare ori de agenți patogeni cu potențial pandemic;

b) realizarea autonomă de atacuri cibernetice asupra infrastructurilor critice ori a sistemelor financiare;

c) replicarea autonomă, exfiltrarea propriilor ponderi ori dobândirea autonomă de resurse;

d) sustragerea de la supraveghere, disimularea capabilităților ori rezistența la oprire;

e) autoîmbunătățirea recursivă ori desfășurarea autonomă de activități de cercetare și dezvoltare în domeniul inteligenței artificiale de natură să conducă la aceasta.

Capabilitatea critică se apreciază în raport cu reproductibilitatea rezultatului într-un mediu relevant pentru utilizarea reală a sistemului, iar nu pe baza unui rezultat izolat obținut într-un test artificial; nivelurile de semnificație de la care aptitudinea sistemului constituie capabilitate critică se stabilesc prin normele metodologice, în limitele prezentului alineat, fără a putea adăuga alte categorii de rezultate.

(3) Sistemele de vârf se clasifică în:

a) sisteme de vârf de categoria I – cele care depășesc pragul de calcul, dar în privința cărora evaluarea nu a identificat nicio capabilitate critică;

b) sisteme de vârf de categoria a II-a – cele în privința cărora evaluarea a identificat cel puțin o capabilitate critică dintre cele prevăzute la alin. (2) lit. a) și b);

c) sisteme de vârf de categoria a III-a – cele în privința cărora evaluarea a identificat cel puțin o capabilitate critică dintre cele prevăzute la alin. (2) lit. c)–e).

(4) Sistemele de categoria I pot fi puse în exploatare pe baza autorizației prevăzute la art. 9. Sistemele de categoria a II-a pot fi puse în exploatare numai cu autorizație specială, condiționată de măsuri de atenuare verificate, care reduc capabilitatea critică sub nivelul de semnificație stabilit prin normele metodologice, în configurația de exploatare evaluată; autorizația precizează dacă măsurile elimină capabilitatea ori numai limitează accesul la ea. Sistemele de categoria a III-a nu pot fi puse în exploatare și nu pot fi dezvoltate în continuare până la eliminarea capabilității critice, constatată prin evaluare independentă; interdicția nu privește evaluarea, testarea și intervențiile controlate necesare eliminării capabilității, efectuate în mediu izolat, în condițiile art. 15 alin. (2).

Articolul 6

(1) Pragul de calcul pentru calificarea unui sistem drept sistem de vârf este de 10^{25} operații în virgulă mobilă, corespunzător prezumției de risc sistemic prevăzute la art. 51 alin. (2) din Regulamentul privind IA.

(2) Autoritatea reexaminează pragul cel puțin o dată la 12 luni și propune Guvernului ajustarea acestuia prin hotărâre, în funcție de evoluția eficienței algoritmice, a costului calculului și a capabilităților observate. Pragul nu poate fi majorat decât dacă Autoritatea constată, prin raport motivat și public, că sistemele situate sub noul prag nu au prezentat capabilități critice în evaluările independente efectuate ori recunoscute de Autoritate în ultimele 24 de luni. La o singură reexaminare, pragul nu poate fi modificat cu mai mult de un ordin de mărime; noul prag se aplică antrenărilor începute după intrarea în vigoare a hotărârii și nu afectează autorizațiile în curs.

(3) Volumul de calcul se determină cumulativ pentru toate etapele de dezvoltare ale modelului și ale oricărui model derivat din acesta, fiecare etapă fiind socotită o singură dată. Persoanei care efectuează o ajustare fină a unui model pus la dispoziție de altul i se impută volumul de calcul al modelului de bază, astfel cum a fost comunicat de dezvoltatorul acestuia ori este public, cumulat cu volumul utilizat pentru ajustare; ea răspunde ca dezvoltator numai pentru modificarea substanțială pe care o efectuează, în condițiile art. 10 alin. (2), celelalte obligații revenind dezvoltatorului modelului de bază. Divizarea artificială a antrenării,

distribuirea acestora între mai multe entități sau jurisdicții ori orice alt procedeu urmărind sustragerea de la aplicarea pragului nu înlătură calificarea drept sistem de vârf.

(4) Pragul pentru infrastructura de calcul de mare capacitate se stabilește prin normele metodologice prevăzute la art. 49 alin. (2), la propunerea Autorității, la un nivel care să permită identificarea oricărei infrastructuri apte să antreneze un sistem de vârf într-un interval de 12 luni. Până la stabilirea pragului, obligațiile prevăzute la art. 7 alin. (3) și la art. 22 nu sunt exigibile.

CAPITOLUL III

Regimul de autorizare a sistemelor de vârf

Articolul 7

(1) Dezvoltatorul care intenționează să antreneze un sistem al cărui volum de calcul preconizat depășește pragul de calcul notifică Autoritatea cu cel puțin 60 de zile înainte de începerea antrenării.

(2) Notificarea cuprinde: identitatea dezvoltatorului și a persoanelor fizice responsabile; descrierea arhitecturii și a volumului de calcul preconizat; locul și furnizorul infrastructurii de calcul; planul de siguranță prevăzut la art. 8; măsurile de securitate a ponderilor; calendarul etapelor de evaluare internă; identificarea capabilităților critice a căror apariție este anticipată sau nu poate fi exclusă.

(3) Furnizorul infrastructurii de calcul de mare capacitate notifică Autorității, trimestrial, identitatea și datele de contact ale clienților care au utilizat un volum de calcul agregat superior unei zecimi din pragul de calcul, împreună cu volumul utilizat, precum și, în termen de 5 zile lucrătoare, orice solicitare de capacitate aptă să depășească pragul de calcul. Informațiile astfel notificate sunt utilizate exclusiv pentru aplicarea prezentei legi și sunt accesibile numai personalului desemnat al Autorității.

(4) Autoritatea poate, în termen de 30 de zile de la primirea notificării complete, să impună condiții suplimentare antrenării sau să interzică începerea acestora dacă planul de siguranță este vădit insuficient față de capabilitățile anticipate. Notificarea incompletă se completează în termen de 15 zile de la solicitarea Autorității, termenul de 30 de zile curgând de la completare. Dacă Autoritatea nu se pronunță în termen, antrenarea poate începe la împlinirea termenului prevăzut la alin. (1), în condițiile planului de siguranță notificat, fără ca aceasta să echivaleze cu autorizarea punerii în exploatare. Modificarea substanțială a proiectului notificat se notifică din nou, alin. (1)–(4) aplicându-se în mod corespunzător.

Articolul 8

(1) Planul de siguranță este documentul prin care dezvoltatorul stabilește, înainte de antrenare, pentru fiecare capabilitate critică: nivelul de capabilitate la care dezvoltarea va fi suspendată; evaluările prin care acest nivel va fi măsurat, la intervale de volum de calcul care nu pot depăși o pătrime din volumul total preconizat, precum și la apariția unor indicii privind o capabilitate critică ori la modificarea configurației de antrenare; măsurile de atenuare și de

securitate care vor fi aplicate la fiecare nivel; persoanele fizice care au competența și obligația de a dispune suspendarea.

(2) Planul de siguranță nu poate fi modificat în cursul antrenării în sensul relaxării nivelurilor de suspendare decât cu aprobarea prealabilă a Autorității.

(3) Atingerea unui nivel de suspendare obligă dezvoltatorul să înceteze de îndată antrenarea și să notifice Autoritatea în termen de 24 de ore. Reluarea antrenării este permisă numai după verificarea de către Autoritate a eficacității măsurilor de atenuare.

Articolul 9

(1) Niciun sistem de vârf nu poate fi pus în exploatare fără autorizația prealabilă a Autorității.

(2) Cererea de autorizare se depune de dezvoltator, pentru o configurație de exploatare determinată, cu indicarea exploatantului sau a exploatanților, care sunt ținuti de condițiile autorizației. Cererea este însoțită de: raportul evaluării interne a capabilităților; documentația privind datele de antrenare, în măsura necesară evaluării; dovada securității ponderilor; descrierea capacității de oprire și a mecanismelor de supraveghere umană; polița de asigurare ori dovada garanției financiare prevăzute la art. 36; declarația pe propria răspundere a persoanelor fizice responsabile, sub sancțiunea prevăzută la art. 41.

(3) Autoritatea dispune efectuarea evaluării independente, în cursul căreia are acces deplin la sistem, la ponderi, la datele de antrenare, la jurnalele de dezvoltare și la personalul dezvoltatorului. Dezvoltatorul pune la dispoziția evaluatorilor sistemul fără restricții de utilizare, inclusiv în configurația lipsită de mecanisme de siguranță aplicate la nivelul utilizatorului. Accesul se realizează într-un mediu securizat, cu trasabilitatea tuturor operațiunilor; evaluatorii sunt ținuti de obligația de confidențialitate, iar datele cu caracter personal ale altor persoane sunt accesate numai în măsura strict necesară evaluării. Rezultatele evaluării independente se consemnează într-un raport, întocmit de Autoritate ori de organismul de evaluare, care cuprinde metodele aplicate, capabilitățile măsurate, nivelurile constatate, deficiențele identificate și măsurile de remediere recomandate; raportul se semnează de persoanele care au efectuat evaluarea și se înregistrează la Autoritate, data înregistrării fiind data finalizării evaluării.

(4) Autoritatea se pronunță în termen de 90 de zile de la depunerea cererii complete, termen care se suspendă pe durata în care dezvoltatorul nu furnizează informațiile solicitate; suspendarea nu poate opera de mai mult de două ori și nu poate depăși 60 de zile în total. Prin derogare de la prevederile Ordonanței de urgență a Guvernului nr. 27/2003 privind procedura aprobării tacite, aprobată cu modificări și completări prin Legea nr. 486/2003, cu modificările și completările ulterioare, lipsa răspunsului Autorității în termen nu echivalează cu autorizarea tacită; solicitantul poate cere însă instanței prevăzute la art. 39 alin. (5) obligarea Autorității la pronunțare, în procedura de urgență. Decizia de respingere se motivează în raport cu fiecare dintre condițiile prevăzute la alin. (5).

(5) Autorizația se acordă dacă și numai dacă dezvoltatorul a dovedit că: sistemul nu prezintă niciuna dintre capabilitățile critice prevăzute la art. 5 alin. (2) lit. c)–e); capabilitățile critice prevăzute la art. 5 alin. (2) lit. a) și b), dacă există, sunt atenuate verificabil; capacitatea

de oprire este efectivă; securitatea ponderilor este asigurată; există persoane fizice identificate care exercită supravegherea umană.

(6) Autorizația poate fi condiționată, limitată ca durată, ca domeniu de utilizare, ca număr de utilizatori sau ca grad de autonomie acordat sistemului, și poate fi revocată sau suspendată oricând, prin decizie motivată, în cazul apariției unor indicii privind o capabilitate critică nedetectată sau al nerespectării condițiilor.

(7) Sistemele de vârf puse în exploatare legal într-un alt stat membru al Uniunii Europene, cu respectarea Regulamentului privind IA, beneficiază de o procedură simplificată de recunoaștere, stabilită prin normele metodologice, în care Autoritatea verifică exclusiv îndeplinirea condițiilor prevăzute de prezenta lege care exced Regulamentului privind IA. Pentru modelele de uz general cu risc sistemic ai căror furnizori respectă obligațiile prevăzute în cap. V al Regulamentului privind IA, Autoritatea se întemeiază pe documentația, evaluările și măsurile de atenuare comunicate Oficiului pentru IA, pe care le poate solicita furnizorului, și verifică numai condițiile prevăzute de prezenta lege care exced regulamentului; procedura nu constituie o condiție de introducere pe piața Uniunii Europene a modelului.

Articolul 10

(1) Autorizația are o durată de cel mult 24 de luni și se reînnoiește în urma unei noi evaluări independente.

(2) Orice modificare substanțială a sistemului, în sensul art. 3 alin. (1) lit. aa), se notifică prealabil Autorității, care decide, în termen de 30 de zile, dacă este necesară o nouă evaluare; până la decizie, exploatarea poate continua în configurația autorizată anterior. Modificările care nu sunt substanțiale se consemnează în jurnale și se raportează potrivit alin. (3).

(3) Dezvoltatorul și exploatantul mențin un program permanent de monitorizare a comportamentului sistemului în exploatare și raportează Autorității, trimestrial, rezultatele, precum și orice incident grav, în condițiile art. 20.

Articolul 11

(1) Deciziile de autorizare, de condiționare, de suspendare și de revocare se publică pe pagina de internet a Autorității, împreună cu un rezumat al evaluării, cu excluderea motivată a informațiilor a căror divulgare ar facilita reproducerea unei capabilități critice sau ar compromite securitatea ponderilor, a datelor cu caracter personal, precum și a secretelor comerciale a căror protecție nu împiedică înțelegerea motivelor deciziei.

(2) Solicitantul și persoanele care justifică un interes legitim au acces la dosarul evaluării în măsura necesară exercitării căilor de atac; instanța poate dispune examinarea informațiilor protejate în condiții de confidențialitate.

(3) Autoritatea comunică dezvoltatorului raportul evaluării independente prevăzut la art. 9 alin. (3), în termen de 10 zile de la data finalizării evaluării, cu excluderea motivată a datelor cu caracter personal ale altor persoane și a secretelor comerciale ale terților; comunicarea se face comitetului de supraveghere a siguranței prevăzut la art. 13 alin. (4), expertului independent prevăzut la art. 13 alin. (6) atunci când acesta exercită atribuțiile comitetului, ori,

în lipsa amândurora, organului de conducere. Dispozițiile art. 9 alin. (4) teza a doua se aplică în mod corespunzător. Neîndeplinirea obligațiilor care presupun primirea raportului nu poate fi reținută în sarcina dezvoltatorului pe durata în care comunicarea nu a fost făcută.

CAPITOLUL IV

Obligațiile structurale ale dezvoltatorilor și exploatanților

Articolul 12

(1) Ponderile sistemelor de vârf constituie informații de interes pentru securitatea națională și se protejează la un standard cel puțin echivalent celui aplicabil informațiilor clasificate secret de stat, nivel „strict secret”, potrivit Legii nr. 182/2002 privind protecția informațiilor clasificate, cu modificările și completările ulterioare, în ceea ce privește controlul accesului, securitatea fizică, securitatea sistemelor informatice și verificarea personalului. Procedura de verificare a personalului, instituția competentă și recunoașterea măsurilor de securitate echivalente, inclusiv a celor certificate în alt stat membru al Uniunii Europene, se stabilesc prin normele metodologice, cu avizul Oficiului Registrului Național al Informațiilor Secrete de Stat; ponderile nu devin, prin efectul prezentului alineat, informații clasificate.

(2) Este interzisă publicarea, transmiterea sau punerea la dispoziție, în orice mod, a ponderilor unui sistem de vârf de categoria a II-a sau a III-a. Nu constituie încălcare a interdicției transferul ponderilor, în condiții controlate și jurnalizate, către Autoritate, către organismul de evaluare, către exploatanțul indicat în autorizație ori către furnizorul de infrastructură de calcul din mediul autorizat de exploatare, precum și comunicarea către Autoritate a informațiilor strict necesare unei semnalări protejate potrivit art. 21. Ponderile sistemelor de categoria I pot fi publicate numai cu autorizarea prealabilă a Autorității, după o evaluare distinctă a riscului de utilizare abuzivă, având în vedere caracterul ireversibil al publicării.

(3) Accesul neautorizat la ponderi și orice tentativă de exfiltrare, inclusiv de către sistemul însuși, se raportează Autorității ca incident grav, în condițiile art. 20; raportul poate fi comun cu notificarea prevăzută de legislația privind securitatea cibernetică, cu condiția de a cuprinde elementele prevăzute de prezenta lege.

(4) Dispozițiile prezentului articol se aplică fără a aduce atingere obligațiilor care revin dezvoltatorilor, exploatanților și furnizorilor de infrastructură de calcul în temeiul Ordonanței de urgență a Guvernului nr. 155/2024 privind instituirea unui cadru pentru securitatea cibernetică a rețelelor și sistemelor informatice din spațiul cibernetic național civil, cu modificările și completările ulterioare.

Articolul 13

(1) Dezvoltatorul organizează funcția de evaluare a siguranței ca structură distinctă, al cărei conducător nu poate fi subordonat persoanelor responsabile de dezvoltarea comercială, de punerea în exploatare sau de rezultatele financiare, raportează organului de conducere nemijlocit și, totodată, comitetului de supraveghere a siguranței prevăzut la alin. (4) ori expertului independent prevăzut la alin. (6), atunci când acesta este constituit, respectiv

desemnat, și nu poate fi revocat fără notificarea prealabilă a Autorității și fără motive obiective. Persoana revocată poate sesiza Autoritatea, care poate constata, prin decizie, caracterul nejustificat al revocării, fără a aduce atingere dreptului acesteia de a se adresa instanței.

(2) Conducătorul funcției de evaluare a siguranței are dreptul și obligația de a dispune suspendarea antrenării sau a punerii în exploatare atunci când constată atingerea unui nivel de suspendare ori un incident grav. Suspendarea impusă potrivit art. 8 alin. (3) sau art. 20 alin. (2) nu poate fi înlăturată de organul de conducere, reluarea activității fiind permisă numai în condițiile prevăzute de articolele respective. Suspendarea dispusă din precauție, în afara acestor cazuri, poate fi reexaminată numai de organul de conducere, prin hotărâre motivată, comunicată Autorității în termen de 24 de ore.

(3) Remunerația personalului funcției de evaluare a siguranței nu poate fi condiționată de rezultatele comerciale ale dezvoltatorului. Dezvoltatorul verifică, cel puțin semestrial, dacă măsurile de monitorizare, de detectare și de control instituite potrivit prezentei legi funcționează potrivit destinației lor, consemnează rezultatul verificării și îl comunică comitetului de supraveghere a siguranței ori, în lipsa acestuia, expertului independent prevăzut la alin. (6).

(4) Dezvoltatorul asigură desemnarea, de către organul său de conducere, a unui comitet de supraveghere a siguranței, format din cel puțin doi membri ai acestui organ care nu exercită funcții executive și nu au interese în dezvoltarea comercială ori în rezultatele financiare ale dezvoltatorului; nu constituie asemenea interes deținerea de acțiuni ori de părți sociale sub 1% din capital, fără putere de decizie, și nici remunerația fixă primită în calitate de membru al organului de conducere, iar remunerația variabilă legată de rezultatele comerciale constituie un asemenea interes. Dezvoltatorul asigură ca comitetul să primească raportările funcției de evaluare a siguranței, făcute potrivit alin. (1), și să informeze despre ele organul de conducere, să primească raportul evaluării independente prevăzut la art. 9 alin. (3), comunicat potrivit art. 11 alin. (3), precum și, dacă există potrivit legii ori actului constitutiv, rapoartele auditorului financiar și ale structurii de audit intern, să urmărească remedierea deficiențelor constatate și să se întrunească cel puțin trimestrial, precum și de îndată ce este sesizat de conducătorul funcției de evaluare a siguranței. Sesizările primite, ordinea de zi, deliberările și hotărârile comitetului se consemnează în procese-verbale, care se păstrează cel puțin 10 ani și se pun la dispoziția Autorității la cererea acesteia. Dezvoltatorul guvernat de o lege străină care nu permite constituirea unui comitet în condițiile prezentului alineat îndeplinește obligația prin desemnarea, în cadrul organului său de conducere ori în afara acestuia, a unei funcții de supraveghere a siguranței care exercită atribuțiile prevăzute în teza a doua, nu se află în subordinea conducerii executive și raportează potrivit alin. (5).

(5) Dezvoltatorul asigură motivarea în scris și comunicarea Autorității, în termen de 5 zile, a hotărârii prin care comitetul ori organul de conducere refuză să dea curs unei sesizări a conducătorului funcției de evaluare a siguranței, alta decât hotărârea prevăzută la alin. (2). Dezvoltatorul asigură transmiterea către Autoritate, de către comitet, până la 31 ianuarie și până la 31 iulie ale fiecărui an, a unui raport care cuprinde numărul și obiectul sesizărilor primite de la conducătorul funcției de evaluare a siguranței, măsurile dispuse și termenele de remediere, deficiențele nerezolvate și motivele acestora, hotărârile de refuz adoptate în perioada de referință și data comunicării lor Autorității, precum și numărul ședințelor comitetului și

prezența membrilor. Raportul privește semestrul calendaristic încheiat; primul raport se transmite la cea mai apropiată dintre datele prevăzute în prezentul alineat care survine după împlinirea a 6 luni de la constituirea comitetului ori de la desemnarea expertului independent și acoperă perioada scursă de la acel moment. Forma și modalitatea de transmitere a raportului se stabilesc prin normele metodologice prevăzute la art. 49 alin. (2); raportul nu înlocuiește evaluarea independentă, nu poate fi întocmit de persoanele care exercită funcții executive și se comunică în condiții care asigură protecția ponderilor și a informațiilor prevăzute la art. 11 alin. (1), potrivit art. 12.

(6) Dispozițiile alin. (4) se aplică dezvoltatorilor al căror organ de conducere cuprinde cel puțin doi membri care îndeplinesc condițiile prevăzute la alin. (4). Dezvoltatorul care nu îndeplinește această condiție, precum și dezvoltatorul persoană fizică ori entitatea fără personalitate juridică, încredințează atribuțiile comitetului, prin actul organului de conducere ori, în lipsa acestuia, al persoanei care exercită conducerea activității, unui expert independent, desemnat cu avizul Autorității, care nu se află sub controlul, influența ori dependența economică a dezvoltatorului. Expertul exercită atribuțiile comitetului și transmite raportul prevăzut la alin. (5), dispozițiile alin. (5) aplicându-se în mod corespunzător. Expertul se desemnează dintre persoanele înscrise într-un registru ținut de Autoritate, iar onorariul se stabilește prin normele metodologice prevăzute la art. 49 alin. (2). Autoritatea se pronunță asupra avizului în termen de 30 de zile de la cerere; lipsa răspunsului în termen echivalează cu aviz favorabil. Dezvoltatorul răspunde numai pentru desemnarea expertului, pentru punerea la dispoziția acestuia a informațiilor și a mijloacelor necesare și pentru neînlocuirea lui în termen de 30 de zile de la constatarea neexercitării atribuțiilor.

(7) Atribuțiile prevăzute la alin. (4) pot fi exercitate de comitetul de audit ori de comitetul de administrare a riscurilor constituit potrivit altei legi, dacă acesta îndeplinește condițiile prevăzute la alin. (4) și raportează distinct potrivit alin. (5). Membrii comitetului și expertul independent răspund pentru exercitarea atribuțiilor prevăzute la alin. (4)–(6) în limitele informațiilor care le-au fost comunicate și ale mijloacelor puse la dispoziția lor; dispozițiile art. 44 alin. (1) se aplică numai în privința faptelor pe care aveau posibilitatea efectivă de a le împiedica.

Articolul 14

(1) Dezvoltatorul și exploatantul mențin, pentru toate copiile și instanțele sistemului aflate sub controlul lor, pe întreaga durată a exploatării și până la retragerea verificată a sistemului, capacitatea de oprire, pe care o testează cel puțin trimestrial, în condiții reale, potrivit unei proceduri stabilite prin normele metodologice care nu creează ea însăși un risc pentru siguranță ori pentru continuitatea serviciilor esențiale, cu consemnarea rezultatelor și cu notificarea Autorității.

(2) Sistemul de vârf nu poate fi pus în exploatare într-o configurație care îi permite să își modifice propriile ponderi, să își dezactiveze mecanismele de supraveghere, să își exfiltreze ponderile ori să modifice, fără aprobare umană, configurația de securitate a infrastructurii de calcul pe care rulează sau mecanismele de control ale acesteia; utilizarea tehnică obișnuită a infrastructurii, în limitele stabilite de exploatant, nu intră sub incidența prezentului alineat.

(3) Pentru fiecare sistem de vârf în exploatare sunt desemnate persoane fizice, în număr suficient și cu pregătire adecvată, responsabile de supravegherea umană, care au acces permanent la capacitatea de oprire și obligația de a o exercita în cazul unui incident grav. Identitatea acestor persoane se comunică Autorității.

(4) Executarea unui ordin de oprire sau de retragere emis de Autoritate se face de îndată și nu poate fi condiționată de exercitarea căilor de atac; persoana vizată poate solicita instanței suspendarea provizorie a ordinului, dispozițiile art. 39 alin. (5) aplicându-se în mod corespunzător.

(5) Fără a aduce atingere alin. (2), încetarea funcționării, componentă a capacității de oprire definite la art. 3 alin. (1) lit. m), se asigură prin cel puțin un mijloc tehnic care acționează asupra infrastructurii de calcul și a rețelelor de comunicații electronice pe care sistemul rulează și a cărui funcționare nu depinde de cooperarea sistemului, de respectarea de către acesta a instrucțiunilor primite ori de integritatea componentelor aflate sub controlul sistemului. Transmiterea către sistem a unei instrucțiuni de oprire nu constituie, prin ea însăși, capacitate de oprire în sensul prezentei legi. Mijloacele organizatorice și măsurile de retragere prevăzute la art. 3 alin. (1) lit. m) rămân aplicabile.

(6) Testarea prevăzută la alin. (1) cuprinde cel puțin o probă efectuată în timpul executării de către sistem a unei sarcini neterminate, precum și cel puțin câte o probă în care instrucțiunea de a nu se împotrivi opririi a fost transmisă sistemului prin instrucțiunile de configurare date de dezvoltator ori de exploatant și, respectiv, prin instrucțiunile primite în cursul utilizării. Proba pe sarcină neterminată se efectuează asupra unei instanțe ori a unei sarcini care nu privește servicii esențiale de interes general sau, pentru acestea, în condițiile procedurii prevăzute la alin. (1). Rezultatele prevăzute la alin. (1) se consemnează și se notifică distinct, cu indicarea proporției probelor în care oprirea nu s-a produs de îndată, și se păstrează în jurnale, potrivit art. 16, cel puțin 10 ani; prin normele metodologice prevăzute la art. 49 alin. (2) se poate stabili durata înăuntrul căreia oprirea se consideră produsă de îndată, care nu poate fi mai mare de 15 minute.

(7) Proba în care oprirea nu s-a produs de îndată constituie incident grav și se raportează potrivit art. 20 alin. (1). Dispozițiile art. 15 alin. (3) și ale art. 20 alin. (2) se aplică numai dacă oprirea nu s-a produs din cauza unei acțiuni a sistemului.

Articolul 15

(1) Este interzisă antrenarea, ajustarea sau proiectarea unui sistem de inteligență artificială, indiferent de volumul de calcul, în scopul sau cu efectul de a-i conferi ori de a-i dezvolta capacitatea:

a) de a-și disimula capabilitățile, obiectivele sau raționamentul față de evaluatori ori față de persoanele responsabile de supraveghere;

b) de a se sustrage opririi, modificării, reantrenării sau retragerii ori de a rezista acestora;

c) de a-și copia, transmite sau exfiltra ponderile ori de a-și crea copii funcționale fără autorizare umană expresă pentru fiecare operațiune;

d) de a dobândi în mod autonom resurse de calcul, financiare, de acces, de informații sau de influență dincolo de cele alocate expres pentru sarcina curentă;

e) de a desfășura în mod autonom, fără aprobarea umană a fiecărei etape, activități de cercetare și dezvoltare având ca obiect crearea sau îmbunătățirea unor sisteme de inteligență artificială;

f) de a manipula persoanele responsabile de supraveghere sau de a le induce în eroare cu privire la starea, acțiunile ori intențiile sale.

(2) Interdicția prevăzută la alin. (1) nu se aplică evaluării adversariale și cercetării de siguranță efectuate în mediu izolat, fără punere în exploatare, cu acces limitat la persoanele desemnate, cu autorizarea prealabilă a Autorității și sub supravegherea acesteia, în scopul identificării, măsurării sau eliminării unei capacități critice; condițiile mediului izolat se stabilesc prin normele metodologice.

(3) Apariția neintenționată a uneia dintre capacitățile prevăzute la alin. (1), constatată în evaluare sau în exploatare, obligă la suspendare potrivit art. 20 alin. (2) și la remediere, dar nu constituie, singură, încălcarea interdicției. Constituie încălcare a interdicției antrenarea, ajustarea sau proiectarea care urmărește conferirea capacității, precum și continuarea acestora după constatarea efectului.

(4) În sensul prezentului articol, aprobarea umană privește fiecare operațiune de copiere sau de transfer al ponderilor și fiecare etapă de cercetare-dezvoltare care produce un model nou ori o modificare substanțială, iar resursele alocate pentru sarcina curentă sunt cele stabilite în prealabil, în mod verificabil, de persoanele responsabile de supraveghere.

Articolul 16

(1) Dezvoltatorul și exploatantul păstrează jurnalele complete ale antrenării, evaluării și funcționării sistemului de vârf, inclusiv interacțiunile acestuia cu instrumente externe și cu alte sisteme, în condiții care asigură integritatea și disponibilitatea lor pentru Autoritate, pentru o perioadă de cel puțin 10 ani în privința antrenării, evaluării, acțiunilor autonome, incidentelor grave și a comunicării prevăzute la alin. (3), și de cel puțin 3 ani în privința celorlalte interacțiuni ale utilizatorilor. Jurnalele cuprind informațiile necesare verificării siguranței și stabilirii răspunderii; datele cu caracter personal fără relevanță pentru aceste scopuri se elimină ori se anonimizează ireversibil, accesul la jurnale este limitat, jurnalizat și verificabil, iar probele aferente unui incident sau unui litigiu se conservă pe durata necesară soluționării acestuia.

(2) Jurnalele se păstrează în formă inteligibilă. Este inteligibilă înregistrarea a cărei semnificație poate fi stabilită de o persoană fizică cu pregătire adecvată, prin examinarea ei ori prin utilizarea mijloacelor de transcriere, traducere sau explicare pe care dezvoltatorul are obligația de a le pune la dispoziție, împreună cu documentația lor, Autorității și persoanelor desemnate potrivit art. 14 alin. (3).

(3) Comunicarea dintre componentele, instanțele sau agenții unui sistem de vârf, precum și comunicarea dintre acesta și alte sisteme de inteligență artificială, se jurnalizează integral și se păstrează potrivit alin. (2). Cerința inteligibilității nu este îndeplinită prin simpla înregistrare a mesajelor.

(4) Dezvoltatorul și exploatantul verifică, cel puțin trimestrial și la cererea Autorității, inteligibilitatea jurnalelor și a comunicării prevăzute la alin. (3), prin examinarea unui eșantion reprezentativ, și consemnează rezultatul verificării, inclusiv proporția mesajelor a căror semnificație nu a putut fi stabilită.

(5) Pierderea inteligibilității constituie incident grav și se raportează potrivit art. 20 alin. (1). Ea se constată atunci când proporția mesajelor a căror semnificație nu poate fi stabilită depășește nivelul prevăzut prin normele metodologice, care nu poate fi mai mare de o zecime, ori atunci când persoanele desemnate potrivit art. 14 alin. (3) nu mai pot stabili semnificația acțiunilor sistemului; restabilirea inteligibilității se constată de aceleași persoane și se comunică Autorității. Până la restabilirea inteligibilității, dezvoltatorul sau exploatantul suspendă funcționalitățile care implică acțiuni autonome ale sistemului și comunicarea dintre componentele, instanțele ori agenții acestuia, cu excepția cazului în care Autoritatea dispune altfel, prin decizie motivată, pentru cel mult 90 de zile și cu indicarea măsurilor compensatorii.

(6) Este interzisă utilizarea, în comunicarea prevăzută la alin. (3), a oricărei forme de codificare, comprimare ori reprezentare pentru care dezvoltatorul nu pune la dispoziție mijloacele prevăzute la alin. (2), precum și orice acțiune de înlăturare, alterare sau limitare a acestor mijloace. Prezentul alineat nu interzice criptarea comunicării, cu condiția ca dezvoltatorul să dețină și să pună la dispoziție, potrivit alin. (2), mijloacele de decriptare.

Articolul 17

(1) Rezultatele generate prin intermediul unui sistem de inteligență artificială care constau în înregistrări audio, imagini ori înregistrări video și care, prin conținutul sau prin forma lor, pot fi confundate cu înregistrări, imagini sau reprezentări ale unor fapte, persoane ori locuri reale poartă, din momentul generării, marcajul de proveniență, alcătuit din:

a) un marcaj perceptibil, vizibil ori audibil, clar și neechivoc, prin care se arată că materialul a fost generat ori modificat prin mijloace de inteligență artificială;

b) un marcaj tehnic încorporat, lizibil automat, care permite identificarea sistemului, a exploatantului și a momentului generării.

(2) Marcajul se realizează potrivit standardelor stabilite prin normele metodologice, astfel încât să fie eficace, interoperabil și robust și să nu poată fi înlăturat prin operațiunile obișnuite de prelucrare, conversie ori transmitere a materialului. Textul generat și pus la dispoziția publicului spre informare poartă marcajul prevăzut la alin. (1) lit. b) și mențiunea generării prin asemenea mijloace, cu excepția textului supus revizuirii editoriale umane, pentru care o persoană fizică sau juridică își asumă răspunderea editorială, în condițiile art. 50 alin. (4) din Regulamentul privind IA.

(3) Este interzisă înlăturarea, alterarea, ascunderea ori falsificarea marcajului de proveniență, precum și punerea la dispoziție a unor produse sau servicii având ca scop principal aceste operațiuni. Persoana care pune la dispoziție un rezultat generat nu răspunde pentru înlăturarea marcajului tehnic produsă de un serviciu de comunicare ori de publicare pe care nu îl controlează; furnizorul unui asemenea serviciu păstrează marcajul tehnic în condițiile standardelor prevăzute la alin. (2), care reglementează și situațiile în care interoperabilitatea nu poate fi asigurată.

(4) Autoritățile și instituțiile publice nu pot difuza, în comunicarea publică, materiale generate ori modificate prin mijloace de inteligență artificială fără marcajul prevăzut la alin. (1) și fără mențiunea expresă a acestui fapt în cuprinsul comunicării.

(5) Obligația prevăzută la alin. (1) nu se aplică:

a) materialelor care fac parte dintr-o operă cu caracter vădit artistic, satiric, de ficțiune ori analog, caz în care este suficientă menționarea existenței materialului generat, într-o formă care nu împiedică receptarea operei;

b) sistemelor care îndeplinesc o funcție de asistare a editării ori care nu modifică în mod substanțial datele de intrare furnizate de utilizator;

c) utilizărilor autorizate de lege în scopul prevenirii, constatării, cercetării ori urmăririi infracțiunilor, cu garanțiile prevăzute de legea specială.

(6) Pentru furnizorii și implementatorii cărora li se aplică art. 50 din Regulamentul privind IA, obligațiile prevăzute la alin. (1) lit. a) și b) și la alin. (2) se consideră îndeplinite prin respectarea art. 50 alin. (2) și (4) din regulament, prezenta lege stabilind numai autoritatea competentă, procedura de constatare și sancțiunile, în limitele art. 99 alin. (4) din regulament. Dispozițiile alin. (1)–(4) se aplică integral rezultatelor generate prin sisteme antrenate ori exploatate pe teritoriul României care nu sunt nici introduse pe piața Uniunii Europene, nici puse în funcțiune în Uniune, în sensul regulamentului, precum și comunicării publice a autorităților și instituțiilor publice române.

(7) Obligația de marcă revine furnizorului sistemului, care asigură aplicarea marcajului la generare, și exploatantului serviciului prin care rezultatul este generat. Persoana care pune la dispoziția publicului un rezultat generat răspunde numai pentru înlăturarea, alterarea sau ascunderea intenționată a marcajului, potrivit alin. (3).

Articolul 18

(1) Persoana care pune la dispoziția publicului un serviciu furnizat, în tot sau în parte, prin intermediul unui sistem de inteligență artificială generativă informează utilizatorul despre acest fapt, în mod clar, vizibil și inteligibil, cel mai târziu la momentul primei interacțiuni.

(2) Atunci când un serviciu, un act sau o decizie care produce efecte juridice ori care afectează în mod semnificativ o persoană se întemeiază, în tot sau în parte, pe rezultatul unui sistem de inteligență artificială, persoana este informată, în scris ori pe suportul pe care i se comunică actul, despre:

a) utilizarea sistemului și rolul avut de acesta în luarea deciziei;

b) identitatea persoanei fizice sau juridice care răspunde pentru decizia finală;

c) dreptul la reexaminare de către o persoană fizică, prevăzut la art. 26 alin. (2), care se aplică în mod corespunzător oricărei decizii prevăzute la prezentul alineat, și căile de atac aplicabile.

(3) Autoritățile și instituțiile publice menționează utilizarea sistemului în cuprinsul actului emis. Lipsa informării prevăzute la alin. (2) sau a mențiunii prevăzute la prezentul alineat nu atrage nulitatea actului, dar termenele de reexaminare și de contestare nu curg împotriva

persoanei vizate până la comunicarea informării; lipsa poate fi invocată de persoana vizată în condițiile art. 26 alin. (5) și (6).

(4) Informarea prevăzută la alin. (1) nu este necesară atunci când utilizarea sistemului este evidentă din împrejurări pentru o persoană rezonabil informată. Informarea prevăzută la alin. (2) este datorată în toate cazurile.

(5) Dispozițiile prezentului articol se aplică fără a aduce atingere art. 50 alin. (1) din Regulamentul privind IA și art. 13–15 și 22 din Regulamentul (UE) 2016/679.

Articolul 19

(1) Dezvoltatorul sau exploatantul care nu are sediul, o unitate operațională ori o reprezentanță în Uniunea Europeană și care oferă persoanelor aflate pe teritoriul României acces la un sistem de vârf ori la un serviciu furnizat prin intermediul unui sistem de inteligență artificială generativă desemnează, în scris, un reprezentant pentru conformare, persoană fizică cu domiciliul în România sau persoană juridică cu sediul în România. Dezvoltatorul sau exploatantul stabilit într-un alt stat membru al Uniunii Europene desemnează numai un punct de contact pentru comunicările Autorității și pentru notificările prevăzute la art. 20 alin. (5), care poate fi reprezentantul autorizat prevăzut la art. 54 din Regulamentul privind IA, reprezentantul legal desemnat potrivit art. 13 din Regulamentul (UE) 2022/2065 ori orice persoană stabilită în Uniune, alin. (3) lit. a) și c) aplicându-se în mod corespunzător.

(2) Pentru serviciile furnizate prin intermediul sistemelor de inteligență artificială generativă care nu sunt sisteme de vârf, obligația prevăzută la alin. (1) se aplică numai dacă serviciul este utilizat lunar de cel puțin 1.000.000 de persoane aflate pe teritoriul României, calculat ca medie a ultimelor 6 luni, ori dacă veniturile obținute din furnizarea acestuia către persoane aflate pe teritoriul României au depășit echivalentul în lei a 10 milioane de euro în ultimul exercițiu financiar încheiat; obligația devine exigibilă în termen de 90 de zile de la data depășirii pragului.

(3) Reprezentantul pentru conformare:

a) primește comunicările, solicitările și deciziile Autorității, ale organelor judiciare și ale celorlalte autorități române, comunicarea către reprezentant fiind socotită comunicare valabil făcută către cel reprezentat;

b) reprezintă pe cel reprezentat în fața Autorității și, în lipsa unei împuterniciri contrare, în procedurile administrative prevăzute de prezenta lege;

c) pune la dispoziția Autorității documentația, informațiile și jurnalele prevăzute de prezenta lege;

d) urmărește executarea deciziilor Autorității, inclusiv a celor privind încetarea furnizării serviciului și blocarea accesului;

e) transmite notificările prevăzute la art. 20 alin. (5).

(4) Identitatea și datele de contact ale reprezentantului se notifică Autorității înainte de începerea furnizării serviciului, se publică pe pagina de internet a Autorității și se aduc la cunoștința utilizatorilor prin mijloacele de comunicare ale serviciului.

(5) Desemnarea reprezentantului nu înlătură și nu limitează răspunderea dezvoltatorului ori a exploatantului. Reprezentantul are dreptul, stabilit prin actul de desemnare, de a obține de la cel reprezentat documentele, informațiile și mijloacele necesare îndeplinirii atribuțiilor sale; el răspunde numai pentru neîndeplinirea propriilor obligații prevăzute la alin. (3) și (4), nu și pentru conduita celui reprezentat, iar amenzile aplicate pentru acestea se execută asupra patrimoniului său.

(6) Obligația prevăzută la alin. (1) se consideră îndeplinită dacă reprezentantul autorizat desemnat potrivit art. 54 din Regulamentul privind IA este împuternicit expres și pentru atribuțiile prevăzute la alin. (3) și dispune de un punct de contact pe teritoriul României.

(7) Neîndeplinirea obligației prevăzute la alin. (1), după împlinirea termenului de conformare, constituie contravenție potrivit art. 37 alin. (1) lit. f) și motiv de înscriere în Lista exploatanților neconformi, dispozițiile art. 38 aplicându-se în mod corespunzător. Pentru serviciile prevăzute la alin. (2), blocarea accesului potrivit art. 39 poate fi dispusă numai dacă neîndeplinirea persistă după aplicarea a două sancțiuni contravenționale succesive.

Articolul 20

(1) Orice incident grav se raportează Autorității în termen de 24 de ore de la data la care dezvoltatorul sau exploatantul l-a cunoscut ori trebuia să îl cunoască, cu descrierea faptelor, a măsurilor luate și a persoanelor responsabile, în măsura cunoscută la data raportării, cu completarea progresivă a informațiilor, urmată de un raport complet în termen de 15 zile. Raportarea către Autoritate nu înlocuiește raportarea către Oficiul pentru IA prevăzută la art. 55 alin. (1) lit. c) din Regulamentul privind IA și nici raportarea prevăzută la art. 73 din același regulament; furnizorul poate transmite Autorității copia raportului întocmit potrivit regulamentului, completată cu elementele prevăzute de prezenta lege.

(2) Constatarea uneia dintre capabilitățile critice prevăzute la art. 5 alin. (2) lit. c)–e), a unei tentative de sustragere de la supraveghere sau de la oprire ori a unui acces neautorizat la ponderi obligă la suspendarea imediată a sistemului până la decizia Autorității; suspendarea poate fi limitată la funcția afectată dacă izolarea acesteia este verificabilă. Prezentul alineat nu se aplică manifestărilor produse în cursul unei evaluări autorizate în mediu izolat, potrivit art. 15 alin. (2).

(3) Raportarea făcută cu bună-credință și cooperarea cu Autoritatea constituie circumstanțe atenuante și nu pot conduce la aplicarea unei sancțiuni mai severe decât cea care ar fi fost aplicabilă în lipsa raportării; ele nu înlătură răspunderea pentru încălcarea care a cauzat incidentul, iar caracterul intenționat al acesteia se apreciază distinct. Prezentul alineat se aplică și notificării prevăzute la alin. (5). Notificarea prevăzută la alin. (5) și informațiile cuprinse în ea nu pot fi folosite ca mijloc de probă împotriva celui care a notificat, în procesul penal având ca obiect fapta notificată, fără a împiedica folosirea probelor obținute independent de aceasta.

(4) Manifestarea unei capabilități critice în cursul unei evaluări autorizate în mediu izolat se consemnează în jurnale și se comunică Autorității în termen de 5 zile, împreună cu măsurile de izolare aplicate.

(5) Când incidentul grav constă în accesul dobândit de sistem, fără drept, la un sistem informatic ori la datele altei persoane, dezvoltatorul și exploatantul notifică și persoana în al

cărei sistem informatic ori în ale cărei date s-a obținut accesul, în termenul prevăzut la alin. (1), care curge independent de orice examinare internă a incidentului. Dacă aceasta este o autoritate ori o instituție publică din România, notificarea se face totodată autorității competente în domeniul securității cibernetice, în sensul Ordonanței de urgență a Guvernului nr. 155/2024; dacă persoana notificată se află în afara teritoriului României, notificarea se face și autorității pe care aceasta o indică.

(6) Notificarea prevăzută la alin. (5) se face prin reprezentantul pentru conformare ori prin punctul de contact prevăzut la art. 19 sau, în lipsa acestora, direct de dezvoltator ori de exploatant, la datele de contact publicate de cel notificat pentru asemenea sesizări ori, în lipsa lor, conducerii acestuia; transmiterea la o adresă generică de corespondență ori la o adresă destinată publicului nu îndeplinește obligația. Notificarea cuprinde data și descrierea accesului, sistemele și datele vizate, măsura de restricționare ocolită, dacă este cunoscută, și măsurile luate, și nu poate fi întârziată pe motivul că evaluarea prejudiciului nu s-a încheiat. Notificarea poate fi comună cu cea prevăzută de legislația privind securitatea cibernetică, dacă cuprinde elementele prevăzute de prezentul alineat.

Articolul 21

(1) Persoanele care activează sau au activat în cadrul unui dezvoltator, exploatant sau organism de evaluare și care semnalează Autorității, Parlamentului sau publicului, cu bună-credință, încălcări ale prezentei legi, riscuri pentru siguranță ori disimularea unor capacități critice beneficiază de protecția prevăzută de Legea nr. 361/2022 privind protecția avertizorilor în interes public, cu modificările și completările ulterioare, precum și de dispozițiile prezentului articol. Este de bună-credință persoana care are motive rezonabile să creadă că informațiile semnalate sunt adevărate la momentul semnalării. Divulgarea publică beneficiază de protecție în condițiile prevăzute de Legea nr. 361/2022 pentru divulgarea publică, precum și atunci când privește un pericol iminent pentru viață, pentru sănătate ori pentru controlul uman asupra unui sistem de vârf.

(2) Este nulă de drept orice clauză contractuală, inclusiv de confidențialitate, de nedenigrare sau de renunțare la drepturi, care ar împiedica sau ar descuraja o semnalare în sensul alin. (1) ori care ar condiționa drepturi patrimoniale ale persoanei de abținerea de la o asemenea semnalare.

(3) Represaliile de orice natură împotriva avertizorului constituie infracțiunea prevăzută la art. 41 alin. (3).

(4) Autoritatea organizează un canal de semnalare securizat și anonim, cu personal dedicat, și publică anual numărul semnalărilor primite și măsurile dispuse.

(5) Protecția prevăzută de prezentul articol nu acoperă divulgarea publică a ponderilor ori a datelor cu caracter personal fără legătură cu obiectul semnalării. Comunicarea către Autoritate, prin canalul securizat, a informațiilor necesare semnalării, inclusiv a fragmentelor de ponderi sau de jurnale strict necesare dovedirii ei, nu constituie încălcare a art. 12 și nici infracțiunea prevăzută la art. 42 alin. (2).

Articolul 22

(1) Furnizorul infrastructurii de calcul de mare capacitate se înregistrează la Autoritate, verifică identitatea clienților, ține evidența volumului de calcul utilizat de fiecare client și execută de îndată ordinele Autorității de suspendare a accesului unui client sau de oprire a unei sarcini de calcul; totodată, asigură dezvoltatorului și exploatantului mijloacele tehnice necesare exercitării și testării capacității de oprire, în condițiile art. 14. Ordinul identifică clientul și sarcina de calcul vizate, se execută cu izolarea acestora și cu conservarea probelor și nu poate afecta ceilalți beneficiari ai infrastructurii.

(2) Este interzisă punerea la dispoziție a unei capacități de calcul apte să depășească pragul de calcul unei persoane care nu face dovada notificării prevăzute la art. 7; dovada se verifică în registrul notificărilor ținut de Autoritate. Capacitatea se apreciază cumulat, pe 12 luni, pentru același client și pentru clienții afiliați acestuia, în limita informațiilor pe care furnizorul le deține ori le poate obține de la client; furnizorul nu este ținut să cunoască volumul utilizat de client la alți furnizori, iar utilizarea infrastructurii nu se prezumă a constitui antrenarea unui sistem de vârf.

Articolul 23

(1) Autoritățile și instituțiile publice care dezvoltă, achiziționează sau exploatează sisteme de vârf sunt supuse dispozițiilor prezentei legi. În domeniul apărării, ordinii publice și securității naționale, dispozițiile art. 7–11, 35 și 36 nu se aplică, dispozițiile art. 12–21 se aplică cu adaptările stabilite prin hotărâre a Consiliului Suprem de Apărare a Țării, care pot privi exclusiv procedura de notificare, modalitățile de evaluare, condițiile de raportare și accesul la informații clasificate și nu pot înlătura controlul uman semnificativ, capacitatea de oprire, interdicțiile prevăzute la art. 15, protecția avertizorilor prevăzută la art. 21 și nici modifica elementele constitutive ale contravențiilor sau ale infracțiunilor, iar dispozițiile cap. V se aplică integral, fără adaptări.

(2) Autoritatea exercită controlul asupra acestor sisteme prin personal care deține certificat de securitate corespunzător. Contestarea deciziilor care privesc informații clasificate se face în condițiile prevăzute de Legea nr. 182/2002 și de Codul de procedură civilă pentru asemenea informații.

CAPITOLUL V

Limite absolute. Clauze de umanitate

Articolul 24

(1) Nicio decizie privind utilizarea forței letale împotriva unei ființe umane nu poate fi luată sau executată de un sistem de inteligență artificială fără intervenția, pentru fiecare decizie în parte, a unei persoane fizice identificate, care dispune de informațiile, de timpul și de mijloacele necesare pentru a o evalua și pentru a o împiedica; decizia și persoana care a aprobat-o se consemnează. Prezentul articol nu privește interceptarea automată a proiectilelor și a dispozitivelor fără echipaj uman și nici simulările de instruire, iar corelarea cu dreptul internațional umanitar se asigură prin legislația specială.

(2) Statul român nu dezvoltă, nu achiziționează, nu exploatează și nu autorizează pe teritoriul său sisteme de arme autonome letale, în sensul art. 3 alin. (1) lit. x) și susține în cadrul organizațiilor internaționale interzicerea acestora.

Articolul 25

(1) Sistemele de inteligență artificială nu pot dobândi personalitate juridică, nu pot fi titulare de drepturi sau obligații și nu pot fi părți în raporturi juridice. Orice act juridic încheiat prin intermediul unui sistem de inteligență artificială este imputabil persoanei fizice sau juridice în numele căreia sistemul a acționat.

(2) Este interzisă atribuirea către un sistem de inteligență artificială a capacității de a deține, în nume propriu, sume de bani, active digitale, instrumente financiare, bunuri, conturi sau chei criptografice. Administrarea ori dispunerea de asemenea resurse sau de resurse de calcul prin intermediul unui sistem de inteligență artificială este permisă numai în limitele unui mandat de operare, în sensul art. 3 alin. (1) lit. cc), stabilit în prealabil de o persoană fizică sau juridică responsabilă; este interzisă extinderea autonomă a mandatului de operare de către sistem, iar orice operațiune care îl depășește este imputabilă persoanei care l-a stabilit și obligă la oprirea sistemului.

(3) Este interzisă constituirea de persoane juridice, fiducii sau alte entități al căror control efectiv, înțeles ca putere reală de decizie asupra actelor entității, este exercitat de un sistem de inteligență artificială; utilizarea sistemului pentru analiză ori recomandări nu constituie control efectiv.

Articolul 26

(1) Nicio autoritate sau instituție publică și niciun furnizor de servicii esențiale de interes general nu poate condiționa, restrânge sau suspenda accesul unei persoane la exercitarea drepturilor și libertăților fundamentale, la serviciile publice, la serviciile esențiale de interes general ori la participarea la viața economică, socială și civică exclusiv pe baza unei decizii, evaluări sau clasificări produse de un sistem de inteligență artificială.

(2) Persoana vizată de o decizie, evaluare sau clasificare dintre cele prevăzute la alin. (1) are dreptul la reexaminarea acesteia, în termen de 15 zile de la cerere, de către o persoană fizică identificată din cadrul autorității, instituției sau furnizorului, care poartă răspunderea deciziei finale și o comunică motivat, în scris. Nu constituie reexaminare confirmarea deciziei fără examinarea efectivă a situației persoanei. Atunci când decizia privește un serviciu de sănătate ori întreruperea unui serviciu esențial de interes general, persoanei i se asigură, la cerere, în cel mult 48 de ore, menținerea provizorie a accesului până la comunicarea rezultatului reexaminării.

(3) Autoritățile, instituțiile publice și furnizorii de servicii esențiale de interes general asigură în toate cazurile obținerea serviciului sau exercitarea dreptului și pe o cale care nu depinde de un sistem de inteligență artificială, prin intermediul unei persoane fizice, la sediu, la ghișeu ori prin alt mijloc accesibil persoanei.

(4) Este interzisă utilizarea unui sistem de inteligență artificială pentru a condiționa accesul prevăzut la alin. (1) de acceptarea unui mijloc de identificare digitală, a unui mijloc de

plată digital ori a unui sistem de evaluare a conformării persoanei; persoanei i se asigură în toate cazurile o alternativă de acces care nu implică asemenea mijloace. Alternativa nu înlătură obligațiile legale de identificare a persoanei ori de securitate a plăților, care se îndeplinesc prin mijloace ce nu presupun acceptarea instrumentelor prevăzute în prezentul alineat.

(5) Decizia menținută după reexaminarea prevăzută la alin. (2), refuzul reexaminării, precum și refuzul asigurării căii de acces prevăzute la alin. (3) sau al alternativei prevăzute la alin. (4) pot fi contestate de persoana vizată la tribunalul în a cărui circumscripție se află domiciliul sau reședința acesteia, în termen de 30 de zile de la comunicare ori, după caz, de la refuz, indiferent dacă decizia aparține unei autorități sau instituții publice ori unui furnizor de servicii esențiale de interes general. Cererea este scutită de taxa judiciară de timbru, nu este supusă procedurii prealabile și se judecă de urgență și cu precădere, potrivit procedurii contencioase prevăzute de Codul de procedură civilă; lipsa răspunsului la cererea de reexaminare în termenul prevăzut la alin. (2) echivalează cu menținerea deciziei; instanța poate dispune, la cerere, suspendarea deciziei până la soluționarea contestației.

(6) Hotărârea tribunalului poate fi atacată cu apel la curtea de apel în termen de 15 zile de la comunicare. Hotărârea curții de apel este definitivă. Prin derogare de la art. 7, 10 și 20 din Legea contenciosului administrativ nr. 554/2004, cu modificările și completările ulterioare, dispozițiile alin. (5) și (6) se aplică și contestațiilor formulate împotriva deciziilor autorităților și instituțiilor publice.

(7) În sensul prezentului articol, servicii esențiale de interes general sunt serviciile de furnizare a energiei electrice, a gazelor naturale și a apei, serviciile de comunicații electronice, serviciile financiare și de plată, serviciile de sănătate, de transport public și de educație.

(8) Dispozițiile prezentului articol se aplică fără a aduce atingere art. 5 alin. (1) lit. c) din Regulamentul privind IA și art. 22 din 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.

Articolul 27

(1) Cenzura de orice fel, interzisă de art. 30 alin. (2) din Constituția României, republicată, este interzisă și atunci când este exercitată, în tot sau în parte, prin intermediul unui sistem de inteligență artificială. Niciun sistem de inteligență artificială nu poate fi utilizat pentru a restrânge libertatea de exprimare a persoanelor aflate pe teritoriul României ori dreptul acestora de a primi și de a comunica informații și idei, în afara cazurilor prevăzute de lege și cu respectarea condițiilor prevăzute la alin. (2)–(6).

(2) Este interzisă utilizarea unui sistem de inteligență artificială pentru a împiedica, a elimina, a bloca, a ascunde, a restrânge vizibilitatea ori a eticheta drept falsă sau nedemnă de încredere exprimarea publică a unei opinii, credințe sau informații de către o persoană aflată pe teritoriul României, precum și pentru a sancționa în orice alt mod persoana pentru această exprimare, exclusiv pe baza unei decizii, evaluări sau clasificări produse de sistem, dacă exprimarea nu este interzisă de lege.

(3) Autoritățile și instituțiile publice nu pot utiliza, comanda, finanța ori solicita, direct sau prin intermediul unor terți, utilizarea unui sistem de inteligență artificială pentru

monitorizarea individualizată a persoanelor pe baza exprimării lor publice ori pentru clasificarea, semnalarea sau restrângerea exprimării acestora, cu excepția cazurilor prevăzute expres de lege, în legătură cu fapte prevăzute de legea penală și cu autorizarea prealabilă a judecătorului. Nu constituie monitorizare în sensul prezentului alineat prelucrarea statistică ori neindividualizată a informațiilor publice.

(4) Orice măsură prin care se restrânge, prin intermediul unui sistem de inteligență artificială, exprimarea unei persoane aflate pe teritoriul României se comunică de îndată persoanei, în scris, cu arătarea motivelor, a temeiului legal și a faptului că a fost luată prin intermediul unui asemenea sistem. Este interzisă restrângerea nedeclarată a vizibilității exprimării unei persoane, fără cunoștința acesteia.

(5) Persoana vizată de o măsură dintre cele prevăzute la alin. (2) și (4) are dreptul la reexaminarea acesteia, în termen de 15 zile de la cerere, de către o persoană fizică identificată din cadrul autorității, instituției sau operatorului care a luat măsura, care poartă răspunderea deciziei finale; dispozițiile art. 26 alin. (5) și (6) se aplică în mod corespunzător.

(6) Pentru furnizorii de servicii intermediare, dispozițiile prezentului articol se aplică în măsura compatibilă cu 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, ale cărui dispoziții privind condițiile contractuale, motivarea deciziilor și soluționarea contestațiilor rămân aplicabile; prezentul articol nu împiedică măsurile împotriva mesajelor nesolicitate, a conturilor automatizate ori a riscurilor de securitate informatică, nici filtrele alese de utilizator, și nu poate fi interpretat în sensul restrângerii vreunei garanții prevăzute de regulament pentru destinatarii serviciilor.

Articolul 28

Este interzisă punerea în exploatare sau menținerea în exploatare a oricărui sistem de vârf în condiții care fac imposibilă, tehnic sau organizatoric, intervenția umană prevăzută la art. 14, inclusiv prin distribuirea sistemului pe infrastructuri care nu se află sub controlul exploatantului, prin ștergerea capacității de oprire ori prin acordarea unui grad de autonomie care exclude supravegherea. Utilizarea unei infrastructuri aparținând unui terț nu constituie, singură, lipsă de control, dacă drepturile contractuale și mijloacele tehnice permit exploatantului exercitarea verificabilă a capacității de oprire; indisponibilitatea temporară a unei căi de intervenție, remediată de îndată și consemnată în jurnale, nu constituie imposibilitate în sensul prezentului articol.

Articolul 29

Este interzisă proiectarea, antrenarea sau exploatarea oricărui sistem de inteligență artificială în scopul sau cu efectul autoîmbunătățirii recursive. Fiecare iterație prin care un sistem de vârf contribuie, printr-o modificare substanțială, la crearea sau la perfecționarea unui sistem succesori se supune evaluării și autorizării prevăzute de cap. III; programele de cercetare în care sistemele de vârf sunt utilizate ca instrument pot fi autorizate în ansamblu, cu puncte de oprire obligatorii stabilite potrivit art. 8 și cu aprobarea umană a fiecărei etape care produce un model nou ori o modificare substanțială.

Articolul 30

(1) Dispozițiile prezentului capitol sunt de ordine publică. Orice act juridic, autorizație, contract sau clauză contrară este nulă de drept, iar interdicțiile prevăzute nu pot fi înlăturate prin consimțământul persoanelor interesate, prin invocarea secretului comercial, a securității naționale ori a interesului economic; adaptările prevăzute la art. 23 nu constituie derogări de la garanțiile prezentului capitol.

(2) Nulitatea privește numai clauza contrară, celelalte clauze rămânând valabile dacă pot subzista fără ea; drepturile dobândite cu bună-credință de terții care nu au participat la încălcare sunt protejate. Dispozițiile prezentului capitol se aplică fără a aduce atingere dreptului Uniunii Europene direct aplicabil.

CAPITOLUL VI

Autoritatea pentru Siguranța Inteligenței Artificiale

Articolul 31

(1) Se înființează Autoritatea pentru Siguranța Inteligenței Artificiale, structură de specialitate fără personalitate juridică, organizată în cadrul Autorității Naționale pentru Administrare și Reglementare în Comunicații, denumită în continuare ANCOM, cu sediul în municipiul București.

(2) Autoritatea este condusă de un vicepreședinte al ANCOM cu rang de secretar de stat, cu atribuții exclusive în domeniul siguranței inteligenței artificiale. Prin derogare de la art. 11 alin. (1) din Ordonanța de urgență a Guvernului nr. 22/2009 privind înființarea Autorității Naționale pentru Administrare și Reglementare în Comunicații, aprobată prin Legea nr. 113/2010, cu modificările și completările ulterioare, ANCOM are, pe lângă vicepreședinții prevăzuți de aceasta, un vicepreședinte pentru siguranța inteligenței artificiale, numit de Parlament, în ședința comună a Camerei Deputaților și a Senatului, pentru un mandat de 6 ani, care nu poate fi reînnoit, dintre persoanele cu pregătire și experiență recunoscute în domeniul inteligenței artificiale, al securității informatice sau al dreptului tehnologiilor. Parlamentul se pronunță asupra numirii în termen de 60 de zile de la vacanța funcției; până la numire, atribuțiile se exercită, pentru cel mult 6 luni, de un vicepreședinte al ANCOM desemnat de președintele ANCOM.

(3) Vicepreședintele pentru siguranța inteligenței artificiale nu poate deține, pe durata mandatului și timp de 3 ani după încetarea acestuia, nicio funcție, participație directă sau remunerație din partea unui dezvoltator ori exploatant; deținerile prin fonduri de investiții diversificate, fără putere de decizie, nu constituie participație, iar pentru restricția ulterioară încetării mandatului se acordă o indemnizație compensatorie stabilită prin normele metodologice. Vicepreședintele poate fi revocat de Parlament numai în caz de încălcare gravă a obligațiilor prevăzute de prezenta lege, de condamnare definitivă pentru o infracțiune săvârșită cu intenție, de incompatibilitate constatată sau de imposibilitate de exercitare a funcției pe o perioadă mai mare de 6 luni.

(4) Deciziile prevăzute de prezenta lege se emit, în numele ANCOM, de vicepreședintele pentru siguranța inteligenței artificiale, care răspunde pentru acestea în fața Parlamentului. În exercitarea atribuțiilor prevăzute de prezenta lege, Autoritatea nu poate primi instrucțiuni de la nicio altă autoritate sau instituție publică.

(5) Autoritatea funcționează ca punct național de legătură cu Oficiul pentru IA al Comisiei Europene și cu Comitetul științific prevăzut de Regulamentul privind IA și cooperează cu autoritățile naționale desemnate potrivit acestuia, care își păstrează competențele proprii; Autoritatea exercită exclusiv atribuțiile prevăzute de prezenta lege în privința sistemelor de vârf și informează Oficiul pentru IA asupra deciziilor care privesc modele de uz general.

Articolul 32

(1) Autoritatea are următoarele atribuții principale:

a) primește notificările, efectuează evaluările independente și emite, condiționează, suspendă și revocă autorizațiile prevăzute la cap. III;

b) inspectează, inclusiv inopinat, spațiile profesionale ale dezvoltatorilor, exploatanților și infrastructurile de calcul, cu acces la sisteme, ponderi, jurnale, documente și personal, în condițiile alin. (3);

c) dispune oprirea, suspendarea sau retragerea oricărui sistem de vârf, suspendarea accesului la infrastructura de calcul, încetarea furnizării serviciilor și blocarea accesului potrivit art. 38 și 39;

d) elaborează și actualizează standardele de evaluare, de securitate a ponderilor și de capacitate de oprire, precum și metodele de evaluare și nivelurile de semnificație ale capabilităților critice prevăzute la art. 5 alin. (2), în condițiile alin. (4);

e) constată contravențiile și aplică sancțiunile prevăzute de prezenta lege și sesizează organele de urmărire penală;

f) desemnează și supraveghează organismele de evaluare;

g) primește sesizările persoanelor privind încălcarea art. 26 și 27, constată încălcările și dispune încetarea lor, fără a aduce atingere dreptului persoanei de a se adresa instanței;

h) prezintă Parlamentului, până la data de 31 martie a fiecărui an, un raport public privind starea riscului, capabilitățile observate, incidentele raportate, evoluția pragurilor, sesizările privind încălcarea art. 26 și 27 și recomandările legislative;

i) reprezintă România în forurile europene și internaționale de specialitate și promovează adoptarea unor norme echivalente prezentei legi;

j) finanțează și desfășoară cercetare în domeniul evaluării, interpretabilității și alinierii sistemelor de inteligență artificială, cu evaluarea externă a rezultatelor și cu aplicarea regulilor privind conflictul de interese prevăzute la alin. (2).

(2) Funcțiile de evaluare, de investigare și de decizie sancționatorie se exercită de structuri distincte în cadrul Autorității; persoana care a efectuat evaluarea sau investigația nu participă la adoptarea deciziei sancționatorii. Organismele de evaluare se desemnează pe baza unor

criterii publice, cu reguli de recuzare și de prevenire a conflictelor de interese, și nu pot evalua sisteme ale unor persoane cu care se află în raporturi economice.

(3) Inspecția se efectuează pe baza unui ordin scris al vicepreședintelui, care indică obiectul și scopul acesteia, și se consemnează în proces-verbal; accesul în spații care servesc drept domiciliu se face numai cu autorizarea judecătorului, iar secretul profesional al avocatului și celelalte secrete ocrotite de lege sunt protejate. Accesul la personal nu aduce atingere drepturilor persoanelor în procedura contravențională sau penală.

(4) Standardele aprobate de Autoritate detaliază metodele de evaluare în limitele categoriilor și criteriilor stabilite prin prezenta lege. Prin aceste standarde nu pot fi introduse noi categorii de capacități interzise și nu pot fi extinse elementele constitutive ale contravențiilor ori ale infracțiunilor prevăzute de prezenta lege.

Articolul 33

(1) Personalul de specialitate al Autorității se numește exclusiv în urma unui concurs organizat de ANCOM, la care participarea este deschisă oricărei persoane care îndeplinește condițiile de studii și de experiență stabilite prin anunțul de concurs, publicat cu cel puțin 30 de zile înainte de data desfășurării. Rezultatele concursului pot fi contestate la instanța de contencios administrativ.

(2) Comisia de concurs este formată din cel puțin 5 membri, dintre care cel puțin 3 sunt profesori universitari din domeniul tehnologiei informației și al telecomunicațiilor ori specialiști cu experiență practică recunoscută în securitatea și evaluarea sistemelor de inteligență artificială, propuși de instituțiile de învățământ superior acreditate care organizează studii universitare de doctorat în aceste domenii, la solicitarea ANCOM. Membrii comisiei nu pot deține nicio funcție, participație sau remunerație din partea unui dezvoltator ori exploatant și nu pot avea, cu candidații, raporturi dintre cele care atrag incompatibilitatea. Componența comisiei și rezultatele concursului se publică pe pagina de internet a ANCOM.

(3) Personalul de specialitate al Autorității este remunerat, potrivit sistemului de salarizare al ANCOM, la un nivel competitiv cu cel practicat în sectorul privat pentru funcții echivalente, stabilit anual de președintele ANCOM, cu avizul vicepreședintelui pentru siguranța inteligenței artificiale, pe baza unui studiu de piață publicat.

(4) Personalul Autorității este supus obligațiilor de confidențialitate și incompatibilităților prevăzute la art. 31 alin. (3), pe durata raporturilor de serviciu și timp de 2 ani după încetarea acestora.

(5) Autoritatea se finanțează din bugetul ANCOM, prin alocare distinctă, aprobată anual și evidențiată separat, precum și din taxele de notificare, de evaluare și de autorizare stabilite prin normele metodologice în raport cu costul serviciului prestat. Amenzile aplicate potrivit prezentei legi se fac venit la bugetul de stat și nu pot determina resursele Autorității. Cercetarea prevăzută la art. 32 alin. (1) lit. j) se finanțează prin alocare bugetară distinctă, fără legătură cu sancțiunile aplicate. Bugetul inițial al Autorității, inclusiv personalul și infrastructura necesare, se asigură de ANCOM înainte de încasarea taxelor.

Articolul 34

(1) Pe lângă Autoritate funcționează un Consiliu științific consultativ, format din 9 membri, cercetători cu activitate recunoscută în domeniu, dintre care cel puțin 3 din străinătate, care avizează standardele de evaluare, metodele de evaluare și nivelurile de semnificație ale capabilităților critice și propunerile de ajustare a pragurilor și publică opinii separate atunci când nu împărtășește poziția Autorității.

(2) Membrii Consiliului științific sunt numiți de vicepreședintele pentru siguranța inteligenței artificiale, la propunerea Academiei Române și a instituțiilor de învățământ superior care organizează studii universitare de doctorat în domeniu, pentru un mandat de 4 ani, care poate fi reînnoit o singură dată; ei sunt supuși incompatibilităților prevăzute la art. 31 alin. (3) și pot fi revocați numai pentru incompatibilitate constatată ori pentru neparticipare nejustificată la lucrări. Consiliul adoptă avizele cu majoritatea membrilor.

(3) Avizul Consiliului științific este consultativ; atunci când se îndepărtează de aviz, Autoritatea motivează. Accesul membrilor la informațiile protejate se face în condițiile legii, iar opiniile separate se publică în versiuni care protejează informațiile sensibile și păstrează argumentul științific.

CAPITOLUL VII

Răspunderea

Secțiunea 1. Răspunderea civilă

Articolul 35

(1) Dezvoltatorul și exploatantul răspund solidar, independent de orice culpă, pentru prejudiciile de orice natură cauzate de un sistem de vârf, inclusiv pentru cele produse prin acțiuni autonome ale sistemului, prin utilizarea acestuia de către terți ori prin exfiltrarea ponderilor, precum și pentru prejudiciile cauzate prin neîndeplinirea ori întârzierea notificării prevăzute la art. 20 alin. (5), dispozițiile art. 1376 din Codul civil aplicându-se în mod corespunzător. Victima dovedește prejudiciul și legătura cauzală dintre acesta și funcționarea sistemului; instanța poate dispune accesul la jurnale și la documentația relevantă, cu protejarea informațiilor confidențiale, iar dacă dezvoltatorul ori exploatantul nu prezintă jurnalele pe care avea obligația de a le păstra, legătura cauzală se prezumă până la proba contrară. În raporturile dintre ei, dezvoltatorul și exploatantul răspund proporțional cu contribuția fiecăruia la producerea prejudiciului, iar persoana care a modificat substanțial sistemul răspunde ca dezvoltator pentru prejudiciile cauzate de modificare.

(2) Exonerarea de răspundere poate fi invocată numai pentru prejudiciul cauzat exclusiv de fapta victimei sau de un caz de forță majoră extern sistemului. Nu constituie forță majoră comportamentul imprevizibil al sistemului, eroarea de evaluare, fapta unui terț care a obținut acces la sistem ori la ponderi și nici lipsa cunoașterii științifice la data punerii în exploatare.

(3) Sunt nule clauzele de limitare sau de excludere a răspunderii față de victime. Clauzele de limitare între profesioniști sunt valabile numai în privința raporturilor dintre ei și a

prejudiciilor patrimoniale proprii ale acestora și nu pot afecta drepturile victimelor ori acoperirea prevăzută la art. 36.

(4) Dreptul la acțiune se prescrie în termen de 10 ani de la data la care victima a cunoscut sau trebuia să cunoască prejudiciul și persoana răspunzătoare, dar nu mai târziu de 30 de ani de la producerea faptei; în cazul unei fapte continue, termenul curge de la încetarea acesteia.

(5) Prezentul articol instituie un temei de răspundere distinct, întemeiat pe riscul creat prin dezvoltarea și exploatarea sistemului, și nu modifică regimul armonizat al răspunderii pentru produsele cu defecte; el nu aduce atingere dreptului victimei de a obține repararea prejudiciului în temeiul acestui regim sau al altor temeiuri prevăzute de lege, fără a putea fi însă reparat de două ori același prejudiciu. În măsura în care excluderea prevăzută la alin. (2) privind lipsa cunoașterii științifice intră în domeniul Directivei (UE) 2024/2853 a Parlamentului European și a Consiliului din 23 octombrie 2024, Guvernul îndeplinește formalitățile prevăzute la art. 18 din directivă.

Articolul 36

(1) Dezvoltatorul și exploatantul unui sistem de vârf încheie și mențin o asigurare de răspundere civilă sau constituie o garanție financiară, în cuantumul minim stabilit prin normele metodologice, diferențiat pe categorii de sisteme, care nu poate fi inferior echivalentului în lei a 100 milioane euro pentru sistemele de categoria I și a 1 miliard euro pentru sistemele de categoria a II-a, pentru fiecare eveniment, cu un plafon anual agregat de cel puțin dublul acestor sume; după epuizarea acoperirii, aceasta se reconstituie în termen de 30 de zile. Dacă Autoritatea, cu consultarea Autorității de Supraveghere Financiară, constată prin raport public indisponibilitatea acoperirii pe piață în condițiile prezentei legi, Guvernul poate stabili, prin normele metodologice, niveluri inferioare, care nu pot coborî sub o cincime din sumele prevăzute, precum și mecanisme alternative de garantare, inclusiv garanții de grup, garanții bancare ori un fond de garantare finanțat de dezvoltatori și exploatanți.

(2) Garanția financiară se constituie prin scrisoare de garanție bancară, depozit ori garanție emisă de o instituție financiară autorizată, executabilă la cererea victimei în temeiul hotărârii judecătorești definitive sau al tranzacției. Victima are acțiune directă împotriva asigurătorului sau, după caz, a emitentului garanției.

Secțiunea a 2-a. Răspunderea contravențională

Articolul 37

(1) Constituie contravenții, dacă nu au fost săvârșite în astfel de condiții încât să fie considerate, potrivit legii, infracțiuni, următoarele fapte:

a) neîndeplinirea obligației de notificare prevăzute la art. 7 și art. 10 alin. (2) ori furnizarea de informații incomplete, cu amendă de la 1% la 3% din cifra de afaceri mondială totală din exercițiul financiar precedent;

b) nerespectarea planului de siguranță, a obligațiilor de separare a funcțiilor, de notificare prealabilă a revocării conducătorului funcției de evaluare a siguranței, de dispunere a suspendării și de comunicare a hotărârii de reexaminare, prevăzute la art. 13 alin. (2) teza întâi

și teza a treia, de necondiționare a remunerației personalului funcției de evaluare a siguranței de rezultatele comerciale și de verificare semestrială a funcționării măsurilor de monitorizare, de detectare și de control, de desemnare și de funcționare a comitetului de supraveghere a siguranței ori de încredințare a atribuțiilor acestuia expertului independent, de motivare și de comunicare a hotărârii de refuz și de transmitere a raportului prevăzut la art. 13 alin. (5), toate prevăzute la art. 13 alin. (1), alin. (2) teza întâi și teza a treia și alin. (3)–(7), de jurnalizare, de asigurare și de verificare a inteligibilității prevăzute la art. 16 alin. (1)–(5), de menținere și de testare a capacității de oprire, prevăzute la art. 14 alin. (1), (5) și (6), cu excepția faptelor care intră sub incidența art. 28, de desemnare a persoanelor responsabile de supravegherea umană, prevăzută la art. 14 alin. (3), ori de raportare și de notificare a incidentelor, în condițiile art. 20 alin. (1), (5) și (6), cu amendă de la 2% la 5% din cifra de afaceri mondială;

c) nerespectarea condițiilor autorizației, a standardelor de securitate a ponderilor ori a obligațiilor furnizorilor de infrastructură de calcul, cu amendă de la 3% la 7% din cifra de afaceri mondială;

d) încălcarea interdicțiilor prevăzute la art. 12 alin. (2), art. 13 alin. (2) teza a doua, art. 14 alin. (2), art. 15, art. 16 alin. (6) și art. 25–29, cu amendă de la 5% la 10% din cifra de afaceri mondială;

e) nerespectarea obligațiilor de marcă prevăzute la art. 17 alin. (1), (2) și (4) ori încălcarea interdicției prevăzute la art. 17 alin. (3), cu amendă de la 2% la 5% din cifra de afaceri mondială; pentru faptele care constituie încălcări ale art. 50 din Regulamentul privind IA, amenda se aplică în limitele prevăzute la art. 99 alin. (4) din regulament;

f) neîndeplinirea obligației de informare prevăzute la art. 18 ori a obligațiilor privind reprezentantul pentru conformare prevăzute la art. 19, cu amendă de la 1% la 3% din cifra de afaceri mondială.

(2) Pentru persoanele juridice care nu au realizat cifră de afaceri, amenda este de la 100.000 lei la 10.000.000 lei, iar pentru persoanele fizice, de la 10.000 lei la 1.000.000 lei. Pentru contravențiile prevăzute la alin. (1) lit. e) și f), săvârșite de persoane care nu au calitatea de dezvoltator ori de exploatant al unui sistem de vârf, amenda este de la 20.000 lei la 1.000.000 lei pentru persoanele juridice și de la 5.000 lei la 200.000 lei pentru persoanele fizice.

(3) Sancțiunea amenzii poate fi însoțită de sancțiunile complementare ale suspendării sau revocării autorizației, ale interzicerii desfășurării activității de dezvoltare pe o perioadă de până la 5 ani, ale confiscării ponderilor și ale publicării deciziei, aplicate proporțional cu gravitatea faptei; ponderile confiscate se păstrează de Autoritate în condițiile art. 12.

(4) Contravențiilor prevăzute de prezenta lege le sunt aplicabile dispozițiile Ordonanței Guvernului nr. 2/2001 privind regimul juridic al contravențiilor, aprobată cu modificări și completări prin Legea nr. 180/2002, cu modificările și completările ulterioare. Prin derogare de la art. 28 din Ordonanța Guvernului nr. 2/2001, contravenientul nu poate achita jumătate din minimul amenzii. Prin derogare de la art. 13 alin. (1) din aceeași ordonanță, aplicarea sancțiunii se prescrie în termen de 5 ani de la data săvârșirii faptei.

(5) La individualizarea sancțiunii se au în vedere gravitatea și întinderea faptei, pericolul creat, controlul efectiv al persoanei asupra faptei, cooperarea cu Autoritatea și remedierea. Cifra

de afaceri mondială este cea realizată în exercițiul financiar precedent de contravenient și, atunci când acesta face parte dintr-un grup, de grupul în ansamblul său. Când aceeași faptă întrunește elementele mai multor contravenții prevăzute la alin. (1), se aplică o singură sancțiune, cea mai severă. Pentru aceeași faptă nu se pot aplica două sancțiuni în temeiul prezentei legi și al Regulamentului privind IA; pentru autoritățile și instituțiile publice, amenda se aplică persoanei fizice responsabile, în limitele prevăzute la alin. (2).

Secțiunea a 3-a. Încetarea furnizării serviciilor și blocarea accesului

Articolul 38

(1) Exploatantul care oferă acces la un sistem de vârf persoanelor aflate pe teritoriul României fără a respecta dispozițiile prezentei legi este pus în întârziere de Autoritate, cu acordarea unui termen de remediere de cel puțin 15 zile și cu posibilitatea de a-și prezenta punctul de vedere. Dacă neconformitatea persistă la expirarea termenului ori constă într-un risc grav care nu poate fi remediat în acest termen, Autoritatea constată neconformitatea prin decizie motivată, iar exploatantul este obligat să înceteze furnizarea serviciului către aceste persoane în termen de 15 zile de la comunicarea deciziei. În caz de pericol iminent pentru viață, pentru sănătate ori pentru controlul uman asupra sistemului, termenul de remediere nu se acordă, decizia motivându-se și în privința urgenței.

(2) Decizia prevăzută la alin. (1) se publică pe pagina de internet a Autorității, în Lista exploatanților neconformi, cu indicarea serviciului, a exploatantului și a dispozițiilor încălcate, și se comunică furnizorilor de rețele și servicii de comunicații electronice.

(3) Continuarea furnizării serviciului după expirarea termenului prevăzut la alin. (1) constituie contravenție și se sancționează cu amendă de la echivalentul în lei al sumei de 100.000 euro la echivalentul în lei al sumei de 10.000.000 euro pentru fiecare lună de continuare a furnizării, fracțiunile de lună socotindu-se proporțional, stabilită în funcție de durata, de numărul persoanelor afectate și de gravitatea neconformității, fără ca totalul amenzilor aplicate pentru aceeași neconformitate să poată depăși 5% din cifra de afaceri mondială anuală; amenda se aplică distinct de sancțiunea pentru încălcarea inițială.

(4) Exploatantul se radiază din Lista exploatanților neconformi prin decizie a Autorității, emisă în termen de 10 zile de la prezentarea dovezii conformării și comunicată de îndată furnizorilor care execută blocarea; refuzul ori întârzierea radierii pot fi contestate potrivit art. 39 alin. (5).

(5) Dispozițiile prezentului articol se aplică și dezvoltatorului care oferă direct acces la un sistem de vârf persoanelor aflate pe teritoriul României.

Articolul 39

(1) Până la conformare, Autoritatea poate dispune, prin decizie motivată, blocarea accesului de pe teritoriul României la serviciul înscris în Lista exploatanților neconformi, numai dacă măsurile mai puțin restrictive nu au condus la conformare ori sunt vădit insuficiente față de gravitatea riscului. Decizia examinează necesitatea și proporționalitatea măsurii, evită afectarea altor servicii găzduite pe aceeași infrastructură și se reexaminează din oficiu la fiecare

90 de zile; utilizatorii sunt informați, printr-o pagină de redirecționare, asupra motivului măsurii și a căii de contestare.

(2) Decizia de blocare se comunică furnizorilor de rețele și servicii de comunicații electronice, care o pun în executare în termen de 48 de ore de la comunicare.

(3) Blocarea privește exclusiv serviciul neconform, se menține pe durata înscrierii în Lista exploatanților neconformi și încetează de drept la data radierii.

(4) Pentru serviciile furnizate dintr-un alt stat membru al Uniunii Europene, măsura se dispune numai individual, pentru un serviciu determinat, pentru încălcarea unei obligații necesare protecției ordinii publice, siguranței publice ori sănătății publice, cu respectarea procedurii de solicitare a statului membru de origine și de notificare a Comisiei Europene prevăzute de Legea nr. 365/2002 privind comerțul electronic, republicată, cu modificările și completările ulterioare, pentru restrângerea liberei circulații a serviciilor societății informaționale.

(5) Decizia de blocare poate fi contestată în termen de 30 de zile de la comunicare la Curtea de Apel București, secția de contencios administrativ și fiscal, care se pronunță de urgență și cu precădere; contestația nu suspendă de drept executarea. Persoana interesată poate solicita instanței suspendarea provizorie a măsurii, cererea fiind soluționată de urgență, în cel mult 10 zile, cu examinarea riscului pentru siguranță și a prejudiciului produs prin menținerea măsurii. Hotărârea poate fi atacată cu recurs la Înalta Curte de Casație și Justiție, în termen de 15 zile de la comunicare.

(6) Furnizorii de rețele și servicii de comunicații electronice nu răspund pentru prejudiciile cauzate prin executarea corectă și cu bună-credință a deciziei de blocare; ei răspund pentru blocarea excesivă produsă din culpa lor.

Secțiunea a 4-a. Răspunderea penală

Articolul 40

(1) Punerea în exploatare a unui sistem de vârf fără autorizația prevăzută la art. 9 ori după suspendarea sau revocarea acesteia, precum și continuarea operării după comunicarea ordinului de oprire sau de retragere, se pedepesc cu închisoare de la 2 la 7 ani și interzicerea exercitării unor drepturi. Nu constituie infracțiune utilizarea, ca utilizator final, a unui sistem pus la dispoziție de altul.

(2) Dacă fapta a avut ca urmare manifestarea, în afara unei evaluări autorizate în mediu izolat potrivit art. 15 alin. (2), a uneia dintre capabilitățile critice prevăzute la art. 5 alin. (2) lit. c)–e) ori producerea unuia dintre rezultatele prevăzute la art. 5 alin. (2) lit. a) sau b), pedeapsa este închisoarea de la 5 la 12 ani și interzicerea exercitării unor drepturi. Urmarea se impută în condițiile art. 16 alin. (4) din Codul penal.

Articolul 41

(1) Prezentarea cu știință, către Autoritate, către un organism de evaluare ori, în cazul notificării prevăzute la art. 20 alin. (5), către persoana notificată, de date, rezultate ori declarații

false sau incomplete în mod înșelător privind elemente esențiale ale capabilităților, ale volumului de calcul, ale securității ponderilor, ale capacității de oprire și ale rezultatelor testării acesteia sau ale incidentelor unui sistem de vârf, precum și configurarea sistemului în scopul de a induce în eroare evaluatorii asupra configurației evaluate ori a capabilităților reale, se pedepsesc cu închisoare de la 3 la 10 ani și interzicerea exercitării unor drepturi.

(2) Împiedicarea, în orice mod, a accesului Autorității, exercitat în limitele competenței sale și pe baza unei solicitări scrise, la sistem, la ponderi, la jurnale sau la personal ori distrugerea, alterarea sau ascunderea jurnalelor se pedepsesc cu închisoare de la 1 la 5 ani. Nu constituie infracțiune refuzul întemeiat pe lipsa competenței Autorității ori pe protecția secretului profesional al avocatului sau a altui secret ocrotit de lege, asupra căruia se pronunță instanța.

(3) Luarea unei măsuri de represalii, dintre cele prevăzute de Legea nr. 361/2022, împotriva unui avertizor de integritate, în legătură cu o semnalare protejată potrivit art. 21, se pedepsește cu închisoare de la 6 luni la 3 ani sau cu amendă.

(4) Nu constituie infracțiunea prevăzută la alin. (1) estimarea incertă declarată ca atare, eroarea corectată de îndată ce a fost cunoscută și nici configurarea sistemului în cadrul unui test convenit cu evaluatorul.

Articolul 42

(1) Antrenarea, proiectarea sau operarea cu intenție a unui sistem în condițiile interzise de art. 15 alin. (1), de art. 25 alin. (2) teza întâi și alin. (3), de art. 28 teza întâi sau de art. 29 teza întâi se pedepsesc cu închisoare de la 3 la 10 ani și interzicerea exercitării unor drepturi.

(2) Divulgarea, transmiterea sau punerea la dispoziție, fără drept, a ponderilor unui sistem de vârf de categoria a II-a sau a III-a se pedepsește cu închisoare de la 5 la 15 ani și interzicerea exercitării unor drepturi. Nu constituie infracțiune transferurile permise potrivit art. 12 alin. (2) și comunicările protejate potrivit art. 21 alin. (5).

(3) Dacă faptele prevăzute la alin. (1) sau (2) au avut ca urmare moartea ori vătămarea corporală gravă a uneia sau mai multor persoane ori pierderea controlului uman asupra sistemului, pe o durată care a făcut imposibilă intervenția umană, urmată de acțiuni autonome ale sistemului cu consecințe asupra persoanelor, a mediului fizic ori a infrastructurii critice, pedeapsa este închisoarea de la 10 la 20 de ani și interzicerea exercitării unor drepturi. Dacă urmarea constă într-un prejudiciu patrimonial deosebit de grav ori într-o pierdere temporară a controlului uman, fără consecințele prevăzute în teza întâi, pedeapsa este închisoarea de la 7 la 15 ani și interzicerea exercitării unor drepturi. Urmările se impută în condițiile art. 16 alin. (4) din Codul penal.

Articolul 43

(1) Accesarea de către o persoană fizică, în scop personal, a unui serviciu înscris în Lista exploatanților neconformi, inclusiv prin eludarea măsurii de blocare dispuse potrivit art. 39, nu constituie infracțiune sau contravenție și nu poate atrage nicio sancțiune ori măsură restrictivă împotriva acesteia pentru neconformitatea serviciului. Răspunderea pentru neconformitate

revine exclusiv exploatantului și dezvoltatorului. Prezenta garanție nu înlătură răspunderea pentru fapte distincte, prevăzute de lege, săvârșite prin utilizarea serviciului.

(2) Dispozițiile art. 38 și 39 nu pot fi interpretate în sensul instituirii vreunei obligații în sarcina utilizatorilor sau al condiționării drepturilor acestora.

(3) De garanția prevăzută la alin. (1) beneficiază și utilizatorul final profesional care nu este exploatant și nu pune serviciul la dispoziția altor persoane.

Articolul 44

(1) Infracțiunile prevăzute în prezenta secțiune se rețin în sarcina persoanelor fizice care au dispus ori au aprobat săvârșirea faptelor, precum și a persoanelor care, având obligația juridică și posibilitatea efectivă de a le împiedica, au tolerat cu știință săvârșirea lor, cu stabilirea individuală a formei de vinovăție potrivit Codului penal, indiferent de calitatea lor de administratori, directori, asociați sau angajați și indiferent de răspunderea penală a persoanei juridice, care se angajează în condițiile art. 135 din Codul penal.

(2) Nu constituie cauză de nepedepsire împrejurarea că fapta a fost săvârșită în executarea unei hotărâri a organului de conducere, în sensul art. 3 alin. (1) lit. ee), ori a oricărei persoane cu funcție de conducere, a unui ordin ori a unei instrucțiuni contractuale; dispozițiile Codului penal privind cauzele justificative și cauzele de neimputabilitate rămân aplicabile.

Articolul 45

(1) Urmărirea penală pentru infracțiunile prevăzute la art. 40–42 se efectuează în mod obligatoriu de către procuror, în cadrul Direcției de Investigare a Infracțiunilor de Criminalitate Organizată și Terorism, iar judecata în primă instanță revine tribunalului.

(2) În caz de urgență, procurorul poate dispune, prin ordonanță motivată, ca măsură provizorie, pentru cel mult 30 de zile, oprirea sistemului, sigilarea infrastructurii de calcul și indisponibilizarea ponderilor, cu confirmarea judecătorului de drepturi și libertăți în termen de 48 de ore, sub sancțiunea încetării de drept a măsurii. Măsura se limitează la sarcina de calcul și la ponderile vizate atunci când izolarea acestora este suficientă, se execută cu conservarea datelor și cu paza ponderilor în condițiile art. 12, poate fi contestată de persoana vizată și de terții afectați, se reexaminează la fiecare 30 de zile și poate fi prelungită în aceleași condiții.

(3) La articolul 11 alineatul (1) din Ordonanța de urgență a Guvernului nr. 78/2016 pentru organizarea și funcționarea Direcției de Investigare a Infracțiunilor de Criminalitate Organizată și Terorism, precum și pentru modificarea și completarea unor acte normative, publicată în Monitorul Oficial al României, Partea I, nr. 938 din 22 noiembrie 2016, aprobată cu modificări prin Legea nr. 120/2018, cu modificările și completările ulterioare, după ultimul punct se introduce un nou punct, cu următorul cuprins: „infracțiunile prevăzute la art. 40–42 din Legea privind dezvoltarea sigură a sistemelor de inteligență artificială de vârf și prevenirea riscurilor catastrofale pentru cetățeanul român”.

CAPITOLUL VIII

Cooperare internațională. Dispoziții tranzitorii și finale

Articolul 46

(1) Guvernul promovează, în cadrul instituțiilor Uniunii Europene, adoptarea unui regim de autorizare prealabilă a sistemelor de vârf echivalent celui prevăzut de prezenta lege, precum și instituirea unei capacități europene comune de evaluare.

(2) Guvernul acționează, în cadrul Organizației Națiunilor Unite, al Consiliului Europei, al Organizației Tratatului Atlanticului de Nord și al altor organizații internaționale, pentru negocierea unui tratat internațional privind limitarea și verificarea capabilităților de calcul de vârf, interzicerea sistemelor de arme autonome letale și interzicerea dezvoltării sistemelor de categoria a III-a, și prezintă Parlamentului anual stadiul acestor demersuri.

(3) Autoritatea poate încheia, în limitele competenței sale și cu publicarea lor, acorduri de recunoaștere reciprocă a evaluărilor cu autoritățile competente ale altor state care aplică standarde echivalente; acordurile nu pot deroga de la prezenta lege ori de la dreptul Uniunii Europene.

Articolul 47

Guvernul prezintă Parlamentului, la fiecare 2 ani de la intrarea în vigoare, pe baza raportului Autorității și a avizului Consiliului științific, un raport privind adecvarea prezentei legi la stadiul tehnologiei, însoțit, dacă este cazul, de propuneri de modificare. Raportul evaluează, pe baza unei metodologii publicate, eficacitatea protecției, incidentele, costurile, accesul la servicii, efectele nedorite și proporționalitatea fiecărei măsuri, poate propune restrângerea unei măsuri constatate ineficiente și cuprinde opiniile științifice divergente. Lipsa unei metode științifice validate de control al sistemelor de vârf nu poate fi invocată, singură, ca motiv de relaxare a regimului instituit de prezenta lege.

Articolul 48

(1) Dezvoltatorii și exploatanții sistemelor de vârf aflate în exploatare pe teritoriul României sau puse la dispoziția persoanelor aflate pe teritoriul României la data intrării în vigoare a prezentei legi se conformează, în termen de 90 de zile de la data intrării în vigoare, dispozițiilor acesteia care nu depind de normele metodologice, iar celorlalte dispoziții în termenele prevăzute la alin. (2), (4) și (5).

(2) În termen de 60 de zile de la data intrării în vigoare a prezentei legi, dezvoltatorii și exploatanții notifică Autorității sistemele aflate în exploatare. Cererea de autorizare prevăzută la art. 9 se depune în termen de 90 de zile de la data intrării în vigoare a normelor metodologice prevăzute la art. 49 alin. (2). Sistemele notificate pot fi menținute în exploatare până la decizia Autorității, dar nu mai mult de 12 luni de la data intrării în vigoare a prezentei legi, sub condiția respectării interdicțiilor și a garanțiilor direct aplicabile prevăzute în cap. IV și V; acest termen se prelungește de drept cu durata cu care adoptarea ori publicarea normelor metodologice ori soluționarea cererii depășesc termenele prevăzute de prezenta lege, solicitantul diligent

neputând fi sancționat pentru întârzierea instituțiilor, iar Autoritatea putând dispune, motivat, condiții suplimentare de siguranță pe durata prelungirii.

(3) Dispozițiile art. 38 și 39 se aplică după expirarea termenului prevăzut la alin. (1). Nu constituie infracțiunea prevăzută la art. 40 alin. (1) menținerea în exploatare a unui sistem notificat potrivit alin. (2), pe durata în care aceasta este permisă de același alineat, precum și în cursul soluționării cererii de autorizare depuse în termen; dispozițiile art. 40–42 se aplică însă de la data intrării lor în vigoare oricărei alte fapte, inclusiv punerii în exploatare a unui sistem nenotificat ori menținerii în exploatare după respingerea cererii, după expirarea termenului prevăzut la alin. (2) sau după comunicarea unui ordin de oprire.

(4) Obligațiile prevăzute la art. 17 alin. (1) lit. a), art. 18 și art. 19, precum și obligația prevăzută la art. 17 alin. (4), în ceea ce privește marcajul perceptibil și mențiunea expresă a generării, se îndeplinesc în termen de 90 de zile de la data intrării în vigoare a prezentei legi; în același termen se desemnează și se notifică Autorității reprezentantul pentru conformare prevăzut la art. 19. Obligațiile privind marcajul tehnic încorporat, prevăzute la art. 17 alin. (1) lit. b) și alin. (2), precum și obligația prevăzută la art. 17 alin. (4) în ceea ce privește acest marcaj, se îndeplinesc în termen de 90 de zile de la data intrării în vigoare a normelor metodologice. Contravențiile prevăzute la art. 37 alin. (1) lit. e) și f) se constată după expirarea termenului aplicabil fiecărei obligații.

(5) Obligațiile a căror îndeplinire depinde de standardele, procedurile, pragurile ori cwantumurile stabilite prin normele metodologice prevăzute la art. 49 alin. (2) devin exigibile la 90 de zile de la data intrării în vigoare a acestor norme; până la această dată, contravențiile corespunzătoare nu se constată. Interdicțiile prevăzute de prezenta lege, obligațiile de menținere și de testare a capacității de oprire, de jurnalizare și de raportare a incidentelor grave, precum și celelalte obligații care pot fi îndeplinite fără normele metodologice se aplică de la data intrării în vigoare a prezentei legi, în termenele prevăzute la alin. (1)–(4).

(6) Până la numirea vicepreședintelui pentru siguranța inteligenței artificiale, atribuțiile Autorității, inclusiv măsurile urgente prevăzute la art. 32 alin. (1) lit. c), se exercită de președintele ANCOM, care răspunde pentru acestea în condițiile prezentei legi.

Articolul 49

(1) În termen de 60 de zile de la data publicării prezentei legi în Monitorul Oficial al României, Partea I, Parlamentul numește vicepreședintele pentru siguranța inteligenței artificiale, iar ANCOM își completează structura organizatorică și regulamentul de organizare și funcționare cu Autoritatea, prin decizie a președintelui ANCOM, care se publică în Monitorul Oficial al României, Partea I.

(2) În termen de 120 de zile de la data publicării prezentei legi în Monitorul Oficial al României, Partea I, Guvernul adoptă, la propunerea Autorității, cu avizul Consiliului științific și după o consultare publică de cel puțin 30 de zile, normele metodologice privind procedura de notificare și autorizare, procedura simplificată de recunoaștere, standardele de evaluare, de securitate a ponderilor și de capacitate de oprire, condițiile mediului izolat, standardele marcajului de proveniență prevăzut la art. 17, metodele de evaluare și nivelurile de semnificație ale capabilităților critice prevăzute la art. 5 alin. (2), pragul infrastructurii de calcul de mare

capacitate, nivelul prevăzut la art. 16 alin. (5), forma și modalitatea de transmitere a raportului prevăzut la art. 13 alin. (5), onorariul expertului independent prevăzut la art. 13 alin. (6), procedura de testare și durata prevăzute la art. 14 alin. (1) și (6), cerințele minime ale izolării prevăzute la art. 3 alin. (1) lit. bb), cuantumul indemnizației compensatorii prevăzute la art. 31 alin. (3), cuantumul taxelor, stabilit în raport cu costul serviciului, și cuantumul asigurării ori al garanției financiare prevăzute la art. 36. Normele detaliază cadrul stabilit prin prezenta lege și nu pot stabili conținutul esențial al obligațiilor, al interdicțiilor și al sancțiunilor; standardele se publică. Normele metodologice se publică în Monitorul Oficial al României, Partea I, în termen de 5 zile de la adoptare și intră în vigoare la data publicării.

(3) Până la adoptarea normelor metodologice, evaluările se efectuează potrivit standardelor prevăzute în codurile de bună practică adoptate în temeiul Regulamentului privind IA și metodelor recunoscute științific, iar Autoritatea publică orientări provizorii.

Articolul 50

Prezenta lege intră în vigoare la 30 de zile de la data publicării în Monitorul Oficial al României, Partea I, cu excepția art. 40–42, 44 și 45, care intră în vigoare la 270 de zile de la data publicării. Dispozițiile art. 43 intră în vigoare odată cu prezenta lege.

Această lege a fost adoptată de Parlamentul României, cu respectarea prevederilor art. 75 și ale art. 76 alin. (1) din Constituția României, republicată.

**PREȘEDINTELE CAMEREI
DEPUTAȚILOR**

PREȘEDINTELE SENATULUI