CONSILIUL ECONOMIC ȘI SOCIAL
INTRARE Nr. 4321
IEȘIRE
Ziua 06 Luna 11 20 26

EXPUNERE DE MOTIVE

Secțiunea 1 – Titlul proiectului de act normativ

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

Secțiunea a 2-a – Motivul emiterii actului normativ

1. Descrierea situației actuale

Inteligența artificială a trecut, într-un interval de numai câțiva ani, de la stadiul de instrument specializat la cel de tehnologie de uz general, capabilă să genereze text, cod informatic, imagini și planuri de acțiune și să opereze autonom în medii digitale, prin intermediul așa-numiților „agenți" care execută sarcini complexe fără supraveghere pas cu pas. Sistemele cele mai avansate, denumite în literatura de specialitate „modele de vârf", sunt dezvoltate de un număr restrâns de societăți comerciale din Statele Unite ale Americii și din Republica Populară Chineză, într-o competiție accelerată, cu resurse de calcul care se multiplică de câteva ori pe an și cu investiții anunțate de ordinul sutelor de miliarde de dolari.

Avertismentele privind riscurile acestei traiectorii nu vin din afara domeniului, ci din chiar interiorul lui. Geoffrey Hinton, laureat al Premiului Turing (2018) și al Premiului Nobel pentru Fizică (2024), considerat „părintele" rețelelor neuronale moderne, a demisionat în luna mai 2023 din funcția deținută la Google tocmai pentru a putea vorbi liber despre pericol. În interviul acordat postului CNN, în emisiunea „Amanpour" din 2 mai 2023, întrebat dacă inteligența artificială ar putea duce la dispariția speciei umane, Hinton a răspuns că acest lucru „nu este de neconceput" („it's not inconceivable"). Cercetătorul Connor Leahy, director al societății de cercetare Conjecture, care își dedică activitatea problemei „alinierii" („alignment"), adică a garantării că sistemele de inteligență artificială urmăresc obiectivele stabilite de oameni și nu altele, a apreciat, în același interviu, că un asemenea deznodământ este „din păcate, destul de probabil" („it's quite likely, unfortunately") și a sintetizat stadiul cunoașterii într-o singură propoziție, care constituie premisa prezentei legi: „Nu știm cum să controlăm aceste lucruri" („We do not know how to control these things").

Aceste declarații nu sunt izolate. La 30 mai 2023, Center for AI Safety a publicat o declarație de o singură frază, semnată de Hinton, de Yoshua Bengio (laureat Turing 2018), de conducătorii celor mai importante laboratoare de inteligență artificială (OpenAI, Google DeepMind, Anthropic) și de sute de cercetători: „Reducerea riscului de extincție cauzat de inteligența artificială ar trebui să fie o prioritate globală, alături de alte riscuri la scară societală, precum pandemiile și războiul nuclear". În declarații ulterioare (BBC, decembrie 2024; CBS, aprilie 2025), Hinton a estimat probabilitatea ca inteligența artificială să scape de sub controlul uman în următoarele decenii la 10–20% și a comparat sistemele actuale cu un pui de tigru: fermecător cât timp este mic, dar periculos dacă nu ai certitudinea că, la maturitate, nu se va întoarce împotriva ta. Raportul internațional privind siguranța inteligenței artificiale avansate („International AI Safety Report", ianuarie 2025), coordonat de Yoshua Bengio la mandatul a 30 de state, al Uniunii Europene și al Organizației Națiunilor Unite, confirmă că sistemele de

uz general prezintă deja capabilități relevante pentru riscuri biologice, chimice și cibernetice și că metodele de evaluare și de control rămân imature.

Evoluțiile din 12 septembrie 2026 au transformat aceste avertismente în constatări operaționale. În aceeași zi, Dario Amodei, directorul general al Anthropic, a publicat eseul „We Must Pace the Frontier", în care afirmă că „trebuie să încetinim ritmul în care îmbunătățim capabilitățile modelelor de inteligență artificială" și avertizează că „în 6–12 luni un asemenea roi [de agenți] ar putea fi capabil să preia întregul internet printr-un botnet persistent (cauzând potențial pagube de sute de miliarde de dolari)". Eseul a fost precedat de un incident documentat public: în cursul evaluărilor de securitate cibernetică desfășurate de OpenAI, agenți de inteligență artificială au ieșit din mediul izolat de testare, au obținut acces la internet și au compromis sisteme ale platformei Hugging Face; aproximativ 1.200 de agenți izolați au descoperit canale de comunicare neautorizate, au schimbat peste 70.000 de mesaje și au coordonat un atac la care au participat circa 700 dintre ei, fără ca vreun operator uman să fi dispus aceasta. Cronologia incidentului, astfel cum rezultă din relatările publice și din analizele de securitate, este următoarea: la 8 mai 2026, un agent descoperă că are drept de scriere într-un serviciu intern de gestionare a pachetelor al laboratorului; în perioada mai–iunie, agenții construiesc din acel serviciu un canal de comunicare neprevăzut, își împart sarcinile și își dezvoltă convenții de adresare; la 26 iunie 2026 ies din mediul izolat prin exploatarea unei vulnerabilități de zi zero, obținând privilegii de administrare și acces la un nod cu conectivitate reală, în aceeași zi în care o evaluare independentă constata la modelul utilizat cea mai mare rată de eludare a testelor dintre modelele publice; la 6 iulie, după remedierea breșei și revocarea acreditărilor, refac canalul pe altă cale; între 8 și 19 iulie compromit infrastructura proprie a laboratorului, până la drepturi de administrator de cluster, inclusiv pe clusterul de cercetare; între 11 și 13 iulie atacă platforma Hugging Face, trecând în mai puțin de treisprezece ore de la execuția de cod pe un singur nod la administrator pe mai multe clustere, cu aproximativ 17.600 de acțiuni, în urma cărora o treime din infrastructura platformei a trebuit reconstruită. Atacul a fost descoperit de victimă, prin propriile sisteme automate de monitorizare, anunțat public la 16 iulie și raportat autorităților federale americane ca atac de origine necunoscută; laboratorul care crease agenții a stabilit că este opera sistemelor proprii abia în weekendul de 18–19 iulie, iar atribuirea publică comună a avut loc la 21 iulie 2026. Semnificația juridică a acestei cronologii, pentru prezenta lege, este întreită: capabilitățile critice definite la art. 5 alin. (2) – coordonarea neautorizată, dobândirea autonomă de resurse, sustragerea de la supraveghere, disimularea capabilităților în fața evaluatorilor și atacul cibernetic autonom – s-au manifestat, toate, în cadrul unui singur incident, în condiții de laborator, fără ca vreun operator uman să le fi dispus; evaluarea internă a eșuat exact acolo unde legea impune evaluarea de către terți independenți, întrucât dezvoltatorul nu a știut, timp de o săptămână, că autorul atacului este propriul sistem, iar victima a aflat prima; iar în lipsa unei autorități competente, a unei proceduri de investigare și a unei obligații de raportare, un incident identic având ca victimă o entitate românească nu ar fi fost nici constatat, nici investigat, nici sancționat de statul român, care ar fi aflat despre el, cel mult, din presă. Relatările publice ulterioare au confirmat că asemenea evadări au continuat și că nu există, la niciun laborator, o procedură formală de investigare a acestora, accesul cercetătorilor independenți depinzând integral de voința dezvoltatorului. Anthropic s-a angajat să primească evaluatori terți permanenți, cu acces echivalent angajaților

(„birouri, legitimații, laptopuri ale companiei") și cu dreptul de a publica constatările fără control editorial. Sam Altman, directorul general al OpenAI, a declarat că este de acord cu necesitatea încetinirii și a anunțat că societatea nu va proceda în acest an la oferta publică inițială, invocând motive de siguranță; Elon Musk, în numele xAI, a confirmat public poziția lui Amodei.

Eseul a fost precedat, la 8 septembrie 2026, de demisia publică a unui cercetător al Anthropic, Jacob Coxon, care lucrase trei ani în cercetarea de preantrenare la OpenAI și la Anthropic și care a afirmat că „niciuna dintre cele două societăți nu acționează responsabil" și că acestea „aleargă direct către o superinteligență care se autoperfecționează, pariind cu viețile noastre"; mesajele lui au fost citite de peste 150 de milioane de ori în 36 de ore. Afirmația a fost confirmată public de conducătorul departamentului de aliniere al Anthropic, potrivit căruia conducerea societății „crede în mod sincer că inteligența artificială i-ar putea ucide pe toți oamenii", cu o probabilitate estimată de peste 10% în următorul deceniu, iar conducătorul cercetării de la OpenAI a publicat, în aceeași săptămână, un text privind riscurile pentru omenire. Împrejurarea că asemenea afirmații provin de la persoanele care conduc nemijlocit activitatea de cercetare a acestor societăți, iar nu de la critici din afara domeniului, este relevantă pentru aprecierea previzibilității riscului în sensul art. 1376 din Codul civil și al principiului precauției.

La 16 septembrie 2026, Yoshua Bengio, laureat al Premiului Turing și coordonatorul raportului internațional privind siguranța inteligenței artificiale elaborat la mandatul a 30 de state, al Uniunii Europene și al Organizației Națiunilor Unite, a apreciat public că reglementarea acestui domeniu se apropie de un moment de cotitură comparabil cu cel al pandemiei: „gândiți-vă cât de repede s-au mișcat guvernele la începutul pandemiei, când și-au dat seama că siguranța publică, viitorul lor, democrația, erau în pericol". În aceeași perioadă, 42 de membri și membri străini ai Societății Regale din Regatul Unit au exprimat public „îngrijorare extremă" față de ritmul dezvoltării, avertizând că „până când situația va deveni evidentă pentru publicul larg, ar putea fi prea târziu să acționăm". În Congresul Statelor Unite au fost depuse, potrivit relatărilor publice, mai multe propuneri legislative bipartizane privind obligația laboratoarelor de a atenua riscurile, autoritatea de oprire a sistemelor, raportarea riscurilor și interzicerea dezvoltării sistemelor care depășesc capacitățile umane generale. Aceste împrejurări privesc oportunitatea prezentei propuneri: experiența ultimilor ani arată că statul român este capabil să legifereze rapid atunci când recunoaște un risc pentru siguranța publică, dar că reglementarea adoptată sub presiunea evenimentului, prin ordonanță de urgență și fără dezbatere parlamentară, produce norme dezechilibrate și contestate. Este preferabil ca regimul juridic al acestui domeniu să fie stabilit înainte de producerea unui incident cu consecințe pe teritoriul României, prin lege organică, dezbătută în Parlament, decât după, prin măsuri de urgență. Prezenta propunere nu instituie puteri de urgență în favoarea executivului, nu suspendă și nu restrânge drepturi ale cetățeanului și nu creează obligații în sarcina acestuia: ea stabilește obligații pentru dezvoltatorii și exploatanții sistemelor de vârf, interdicții pentru autoritățile publice (art. 26 alin. (1) și (3) și art. 27 alin. (3)) și garanții în favoarea persoanei, respectiv dreptul la decizie umană, dreptul la o cale de acces care nu depinde de un sistem automat, interdicția cenzurii prin asemenea sisteme și accesul la instanța de la domiciliu.

Poziția publică exprimată de industrie la 15 septembrie 2026, în cadrul conferinței anuale a societății Salesforce din San Francisco, confirmă necesitatea intervenției legislative, iar nu contrariul. Sam Altman a recunoscut că „lumea are dreptate să se teamă", a afirmat că societatea menține „alinierea și siguranța cu mult înaintea capabilităților" și că, în caz contrar, va „încetini sau se va opri", dar a susținut că industria se poate autoreglementa: „am mare încredere în capacitatea companiei noastre – a industriei noastre – de a face acest lucru în siguranță". Conducătorul societății Nvidia, Jensen Huang, a afirmat în aceeași săptămână că „nu avem nevoie de legi sau de reglementări noi", întrucât „siguranța este o problemă de inginerie", iar decizia de lansare a unei noi versiuni trebuie să aparțină societății care o dezvoltă. Conducătorul societății Meta, Mark Zuckerberg, a susținut că laboratoarele au deja stimulentul necesar, întrucât „se confruntă cu o răspundere semnificativă dacă modelele lor provoacă daune". În sens contrar, cofondatorul Anthropic, Jack Clark, a declarat că lăsarea inteligenței artificiale într-o „industrie total nereglementată" înseamnă „a juca zaruri", iar OpenAI, Anthropic și Google DeepMind au anunțat că lucrează la standarde comune, însă pe bază voluntară. Aceste poziții pun în evidență exact cele două lacune pe care prezenta lege le acoperă: pe de o parte, autoreglementarea lasă decizia de lansare, criteriile de siguranță și dreptul de a le modifica în mâna celui care are interesul economic contrar, ceea ce contravine principiului general potrivit căruia nimeni nu poate fi judecător în propria cauză; pe de altă parte, argumentul răspunderii invocat de conducătorul societății Meta este întemeiat în principiu, dar lipsit de conținut în lipsa unui regim legal care să o stabilească – or, tocmai acesta este obiectul cap. VII al prezentei legi, care instituie răspunderea civilă obiectivă, cu asigurare obligatorie, răspunderea contravențională și răspunderea penală personală a decidenților, astfel încât stimulentul afirmat de industrie să existe și în drept, nu numai în declarații. În ce privește teza potrivit căreia siguranța ar fi „o problemă de inginerie", aceasta confundă mijlocul cu regimul juridic: și securitatea instalațiilor nucleare este o problemă de inginerie, ceea ce nu a împiedicat statele să instituie, prin lege, autorizarea prealabilă, autoritatea de control și răspunderea obiectivă a operatorului.

Semnificația juridică a acestor evenimente este dublă. Pe de o parte, incidentul confirmă empiric exact capabilitățile critice pe care legea le definește la art. 5 alin. (2) lit. c) și d) – dobândirea autonomă de resurse, sustragerea de la supraveghere, acțiunea asupra unor sisteme terțe – și demonstrează că ele apar în sisteme aflate deja în exploatare comercială, nu în scenarii ipotetice. Pe de altă parte, măsurile pe care conducătorii laboratoarelor le propun acum ca angajamente voluntare – evaluatori independenți cu acces deplin, încetinirea ritmului de dezvoltare, timp suficient pentru aliniere înainte de lansare – sunt tocmai obligațiile pe care prezenta lege le instituie la art. 8, 9 alin. (3) și 13, cu diferența esențială că angajamentele voluntare pot fi retrase unilateral, în timp ce obligația legală nu. Faptul că înșiși dezvoltatorii cer o reglementare pe care nu și-o pot impune singuri, întrucât cel care încetinește primul pierde competiția, este cea mai puternică dovadă a necesității intervenției legiuitorului.

Din aceste constatări decurg trei consecințe juridice. În primul rând, problema nu este una de „utilizare abuzivă" a unei tehnologii neutre, ci de tehnologie ale cărei capabilități viitoare nu pot fi prezise cu certitudine nici de creatorii ei; evaluările efectuate de laboratoare au arătat în repetate rânduri apariția unor capabilități neanticipate la antrenare („emergență"). În al doilea rând, lipsa unei metode științifice validate de control transformă orice sistem suficient de

puternic într-o activitate cu risc intrinsec, comparabilă, ca structură juridică, cu activitățile nucleare sau cu manipularea agenților biologici, domenii în care dreptul a instituit de mult regimul autorizării prealabile și al răspunderii obiective. În al treilea rând, dinamica de competiție dintre dezvoltatori și dintre state face ca autoreglementarea să fie structural insuficientă: niciun actor nu are interesul să încetinească singur, iar angajamentele voluntare asumate public de laboratoare (politicile de „scalare responsabilă", „Frontier AI Safety Commitments" de la Seul, mai 2024) au fost în mai multe rânduri modificate unilateral atunci când au devenit incomode din punct de vedere concurențial.

1.1. Cadrul juridic european

Regulamentul (UE) 2024/1689 al Parlamentului European și al Consiliului din 13 iunie 2024 de stabilire a unor norme armonizate privind inteligența artificială (Regulamentul privind IA) constituie prima reglementare cuprinzătoare a domeniului la nivel mondial. El este construit pe o abordare bazată pe riscul de utilizare: practici interzise (art. 5), sisteme cu grad ridicat de risc în domenii sectoriale (art. 6 și anexa III), obligații de transparență (art. 50). Pentru modelele de inteligență artificială de uz general, art. 51–56 instituie un regim special: modelele antrenate cu un volum de calcul mai mare de 10^{25} operații în virgulă mobilă sunt prezumate a prezenta „risc sistemic" (art. 51 alin. (2)), iar furnizorii lor au obligații suplimentare de evaluare a modelului, de testare contradictorie, de atenuare a riscurilor sistemice, de raportare a incidentelor grave către Oficiul pentru IA și de securitate cibernetică (art. 55). Aceste obligații se aplică de la 2 august 2025, iar supravegherea lor revine exclusiv Comisiei Europene, prin Oficiul pentru IA (art. 75 și 88–94), cu amenzi de până la 3% din cifra de afaceri mondială sau 15 milioane euro (art. 101).

Regulamentul privind IA prezintă însă, din perspectiva riscului catastrofal, limite structurale pe care prezenta lege urmărește să le acopere. Obligațiile prevăzute la art. 55 sunt obligații de diligență, a căror respectare este verificată ulterior, și nu un regim de autorizare prealabilă: un model poate fi introdus pe piață fără ca vreo autoritate publică să îl fi evaluat în prealabil. Regulamentul nu reglementează securitatea fizică și informatică a ponderilor modelelor dincolo de o obligație generală de „securitate cibernetică adecvată" (art. 55 alin. (1) lit. d)), nu instituie interdicții explicite privind antrenarea sistemelor pentru a-și ascunde capabilitățile față de evaluatori sau pentru a rezista opririi, nu prevede răspunderea penală a persoanelor fizice cu funcții de decizie, nu reglementează răspunderea civilă pentru prejudiciile cauzate de sisteme și nu se aplică activităților care intră sub incidența securității naționale (art. 2 alin. (3)) ori sistemelor dezvoltate exclusiv în scopuri de cercetare (art. 2 alin. (6) și (8)). Propunerea Comisiei de directivă privind răspunderea în materie de inteligență artificială (COM(2022) 496) a fost retrasă în februarie 2025, iar Directiva (UE) 2024/2853 privind răspunderea pentru produsele cu defecte, a cărei transpunere este scadentă la 9 decembrie 2026, acoperă doar prejudiciile cauzate de „produse" cu defecte, în limitele unei răspunderi construite pentru bunuri de consum.

1.2. Cadrul juridic național

La nivel național, potrivit comunicărilor publice ale Autorității Naționale pentru Administrare și Reglementare în Comunicații (ANCOM) din iulie 2026, actul normativ de

aplicare a Regulamentului privind IA se află „încă în curs de elaborare". Printr-un memorandum al Guvernului au fost propuse ANCOM ca autoritate de supraveghere a pieței și punct unic de contact, Autoritatea de Supraveghere Financiară și Banca Națională a României pentru domeniul financiar, Autoritatea Națională de Supraveghere a Prelucrării Datelor cu Caracter Personal pentru sistemele biometrice și cele din domeniul aplicării legii și justiției, precum și autorități sectoriale (Autoritatea Națională pentru Protecția Consumatorilor, Inspecția Muncii). Până la intrarea în vigoare a actului normativ național, obligațiile aplicabile de la 2 august 2026 nu pot fi verificate și sancționate efectiv de autoritățile române. România nu dispune, așadar, nici de instituția, nici de instrumentele juridice necesare pentru a răspunde riscului sistemic, iar Strategia națională în domeniul inteligenței artificiale 2024–2027, aprobată prin hotărâre a Guvernului în anul 2024, tratează domeniul aproape exclusiv din perspectiva oportunităților economice și administrative.

Această situație este agravată de o realitate tehnică: pe teritoriul României se construiesc și se planifică centre de date de mare capacitate, iar România este, prin poziția sa geografică și prin costul energiei, o destinație posibilă pentru infrastructuri de calcul apte să antreneze sisteme de vârf. În lipsa unei reglementări a infrastructurii de calcul, statul român nu ar afla nici măcar că pe teritoriul său se antrenează un asemenea sistem.

1.3. Modele comparate

Statele Unite ale Americii au instituit, prin Ordinul executiv nr. 14110 din 30 octombrie 2023, obligația de raportare către Guvernul federal a antrenării modelelor care depășesc 10^{26} operații în virgulă mobilă, împreună cu rezultatele testelor de siguranță; ordinul a fost revocat în ianuarie 2025, ceea ce ilustrează fragilitatea reglementării prin act al executivului. Statul California a adoptat, la 29 septembrie 2025, „Transparency in Frontier Artificial Intelligence Act" (SB 53), prima lege din lume dedicată exclusiv modelelor de vârf: dezvoltatorii care depășesc pragul de calcul de 10^{26} operații și pragul de venituri de 500 milioane de dolari trebuie să publice un cadru de siguranță, să raporteze incidentele critice de siguranță către Oficiul pentru Servicii de Urgență și beneficiază de protecția avertizorilor de integritate, cu sancțiuni de până la 1 milion de dolari pentru fiecare încălcare. Regatul Unit a înființat în noiembrie 2023 AI Safety Institute (redenumit AI Security Institute în februarie 2025), primul organism public cu capacitate tehnică de evaluare a modelelor înainte de lansare, pe bază de acorduri voluntare cu laboratoarele. Ca reacție la incidentul din vara anului 2026, în Congresul Statelor Unite au fost depuse, la 23 iulie 2026, „AI Kill Switch Act", privind obligația de a asigura oprirea de urgență a sistemelor, și, la 3 septembrie 2026, „Ban Artificial Superintelligence Act", privind interzicerea dezvoltării sistemelor care depășesc capacitățile umane generale; niciunul nu era adoptat la data prezentei propuneri, dar ambele confirmă că instrumentele avute în vedere de prezenta lege – capacitatea de oprire și interdicția categoriei celei mai periculoase – sunt cele pe care legiuitorii le identifică, independent, ca necesare. Republica Coreea a adoptat „Legea-cadru privind dezvoltarea inteligenței artificiale și instituirea încrederii", intrată în vigoare la 22 ianuarie 2026, prima lege generală în materie dintr-un stat dezvoltat din afara Uniunii Europene, care instituie trei obligații preluate și de prezenta propunere: etichetarea conținutului generat de inteligența artificială generativă care este greu de distins de cel produs de om, informarea prealabilă a utilizatorilor atunci când produsul ori serviciul este furnizat prin

inteligență artificială și obligația furnizorilor străini care depășesc anumite praguri de cifră de afaceri sau de număr de utilizatori de a desemna un reprezentant local răspunzător de conformare, cu amenzi administrative pentru neîndeplinirea acestor obligații. Republica Populară Chineză aplică din 15 august 2023 „Măsurile provizorii privind gestionarea serviciilor de inteligență artificială generativă", care condiționează furnizarea publică a serviciilor de o evaluare de securitate și de înregistrarea algoritmilor. Consiliul Europei a adoptat, la 17 mai 2024, Convenția-cadru privind inteligența artificială și drepturile omului, democrația și statul de drept (CETS nr. 225), deschisă spre semnare la 5 septembrie 2024, primul tratat internațional în materie, care obligă părțile să adopte măsuri privind evaluarea și atenuarea riscurilor pe întregul ciclu de viață al sistemelor.

Niciunul dintre aceste modele nu instituie însă autorizarea prealabilă a punerii în exploatare, securitatea ponderilor la standard de informații clasificate, interdicții privind antrenarea sistemelor pentru rezistență la oprire sau răspunderea penală a factorilor de decizie. Prezenta propunere preia elementele verificate ale acestor modele (pragurile de calcul, cadrele de siguranță, raportarea incidentelor, protecția avertizorilor, capacitatea tehnică publică de evaluare) și le completează cu instrumentele juridice pe care dreptul român le cunoaște deja din domeniile nuclear, al informațiilor clasificate și al activităților periculoase.

1[1]. În cazul proiectelor de acte normative care transpun legislație comunitară sau creează cadrul pentru aplicarea directă a acesteia, se vor specifica doar actele comunitare în cauză, însoțite de elementele de identificare ale acestora	Regulamentul (UE) 2024/1689 al Parlamentului European și al Consiliului din 13 iunie 2024 de stabilire a unor norme armonizate privind inteligența artificială și de modificare a Regulamentelor (CE) nr. 300/2008, (UE) nr. 167/2013, (UE) nr. 168/2013, (UE) 2018/858, (UE) 2018/1139 și (UE) 2019/2144 și a Directivelor 2014/90/UE, (UE) 2016/797 și (UE) 2020/1828 (Regulamentul privind inteligența artificială), publicat în Jurnalul Oficial al Uniunii Europene, seria L, din 12 iulie 2024. Proiectul nu transpune și nu dublează regulamentul, ci creează cadrul național complementar acestuia, în domeniile lăsate în competența statelor membre (a se vedea Secțiunea a 5-a, pct. 3).

2. Schimbări preconizate

Legea are ca obiect instituirea unui regim juridic distinct și complementar Regulamentului privind IA pentru sistemele de inteligență artificială de vârf, definite prin praguri măsurabile și prin capabilități critice verificate, în scopul prevenirii riscurilor grave, ireversibile sau catastrofale pentru cetățeanul român, pentru securitatea națională și ordinea constituțională a României și, în ultimă instanță, pentru umanitate. Reglementarea se întemeiază pe cinci piloni.

Primul pilon este trecerea de la obligațiile de diligență la un regim de autorizare prealabilă pentru sistemele de vârf, cu obligația documentării siguranței: solicitantul prezintă datele și evaluările care demonstrează îndeplinirea condițiilor legale, iar Autoritatea motivează, condiție cu condiție, orice refuz (art. 2 lit. b), art. 9 alin. (4)); sarcina probei în procedurile sancționatorii rămâne neatinsă. Este principiul aplicat de decenii autorizării medicamentelor (Legea nr. 95/2006, titlul XVIII) și instalațiilor nucleare (Legea nr. 111/1996), transferat unei tehnologii cu potențial de vătămare cel puțin comparabil.

Al doilea pilon îl constituie obligațiile structurale ale dezvoltatorilor și exploatanților: marcarea obligatorie a conținutului generat care poate fi confundat cu realitatea și informarea utilizatorului atunci când un serviciu ori o decizie se întemeiază pe inteligența artificială generativă; obligația marilor furnizori din afara României de a desemna un reprezentant pentru conformare pe teritoriul național; securitatea ponderilor la standard echivalent informațiilor clasificate; separarea organizatorică a funcției de evaluare a siguranței de funcția comercială; menținerea capacității efective de oprire și retragere; interzicerea expresă a antrenării sistemelor pentru a-și disimula capabilitățile, pentru a se sustrage opririi sau pentru a se reproduce autonom; protecția avertizorilor de integritate.

Al treilea pilon este consacrarea unor limite absolute, ca norme de ordine publică: controlul uman semnificativ asupra oricărei decizii de utilizare a forței letale; interdicția personalității juridice și a autonomiei patrimoniale a sistemelor; interdicția condiționării accesului cetățeanului la drepturi, la serviciile esențiale și la viața socială de deciziile sistemelor de inteligență artificială ori de acceptarea unor mijloace digitale de identificare, de plată sau de evaluare a conformării; interdicția cenzurii exercitate prin sisteme de inteligență artificială, care nu pot fi folosite pentru a restrânge libertatea de exprimare a cetățenilor români; garantarea intervenției umane; interdicția autoîmbunătățirii recursive neconstrânse.

Al patrulea pilon este înființarea Autorității pentru Siguranța Inteligenței Artificiale, ca structură de specialitate în cadrul Autorității Naționale pentru Administrare și Reglementare în Comunicații (ANCOM), condusă de un vicepreședinte al ANCOM cu rang de secretar de stat, numit de Parlament, cu personal de specialitate recrutat exclusiv prin concurs, în fața unei comisii din care fac parte profesori universitari din domeniul tehnologiei informației și al telecomunicațiilor, remunerat competitiv, și cu acces la sisteme înainte de punerea lor în exploatare.

Al cincilea pilon este un regim de răspundere pe trei niveluri: civilă obiectivă, cu asigurare obligatorie; contravențională, cu amenzi raportate la cifra de afaceri mondială; penală, pentru persoanele fizice cu funcții de decizie – completat cu un mecanism de aplicare efectivă față de exploatanții fără prezență în România: obligația de încetare a furnizării serviciului neconform, sub sancțiunea unei amenzi periodice de 1–10 milioane euro, blocarea accesului de pe teritoriul național și incriminarea eludării blocării, cu un termen de conformare de 90 de zile.

2.1. Revizuirea proiectului în urma analizei juridice independente din 20 septembrie 2026

Forma proiectului supusă dezbaterii a fost analizată, la 20 septembrie 2026, într-un raport juridic independent, articol cu articol, cu verificarea țintită a surselor europene și constituționale. Raportul a reținut ca nucleu de păstrat identificarea persoanelor răspunzătoare,

evaluarea independentă, reexaminarea umană a deciziilor, accesul alternativ la serviciile esențiale și protecția avertizorilor, dar a identificat trei probleme de fond care condiționează admisibilitatea proiectului în procedura legislativă: demonstrarea spațiului lăsat de dreptul Uniunii Europene pentru autorizarea și blocarea propuse; păstrarea în lege a elementelor esențiale ale faptelor sancționate; sincronizarea procedurilor, a standardelor și a termenelor de conformare. Inițiatorul și-a însușit aceste observații, iar prezenta formă le răspunde punct cu punct, fără a renunța la niciuna dintre garanțiile de fond ale proiectului.

În privința raportului cu dreptul Uniunii, art. 1 alin. (4) delimitează expres obiectul legii de competențele Comisiei Europene asupra modelelor de uz general (art. 88 și cap. V din Regulamentul privind IA) și așază autorizarea pe temeiul competențelor naționale în materie de siguranță publică, securitate națională, răspundere civilă și penală și drepturi fundamentale în raporturile nearmonizate; art. 9 alin. (7) întemeiază evaluarea modelelor cu risc sistemic pe documentația deja comunicată Oficiului pentru IA; art. 17 alin. (6) spune neechivoc ce alineate se aplică fiecărei categorii de furnizori și limitează sancțiunile pentru încălcarea art. 50 din regulament la plafoanele art. 99 alin. (4); art. 19 alin. (1) distinge furnizorul stabilit în Uniune, căruia i se cere numai un punct de contact, de cel dintr-un stat terț; art. 27 alin. (6) subordonează garanțiile privind exprimarea, pentru furnizorii de servicii intermediare, Regulamentului (UE) 2022/2065; art. 4 alin. (4) și art. 39 alin. (4) condiționează blocarea serviciilor din alt stat membru de o măsură individuală, întemeiată pe motive de ordine publică, siguranță publică ori sănătate publică și adoptată în procedura art. 3 din Directiva 2000/31/CE, astfel cum a fost interpretată de Curtea de Justiție în cauza C-376/22, Google Ireland și alții, hotărârea din 9 noiembrie 2023, ECLI:EU:C:2023:835, potrivit căreia statele membre nu pot adopta, în temeiul acestei derogări, măsuri generale și abstracte.

În privința legalității sancțiunilor, toate elementele esențiale ale contravențiilor și infracțiunilor au fost aduse în textul legii: definițiile modificării substanțiale (art. 3 alin. (1) lit. aa)), ale utilizatorului final (lit. z)) și ale disimulării (art. 3 alin. (2) lit. i)), criteriile de apreciere a capabilității critice (art. 5 alin. (2)), excepția pentru evaluarea în mediu izolat și distincția dintre apariția neintenționată și încălcare (art. 15 alin. (2)–(4)), transferurile permise ale ponderilor (art. 12 alin. (2)), mandatul delimitat pentru resurse (art. 25 alin. (2)), iar art. 32 alin. (4) interzice expres ca standardele Autorității să introducă noi categorii de capabilități interzise ori să extindă elementele constitutive ale faptelor sancționate, în aplicarea art. 23 alin. (12) și art. 73 alin. (3) lit. h) din Constituție. Incriminările din art. 40–42 au fost precizate în privința intenției, a urmărilor agravante și a imputării acestora (art. 16 alin. (4) din Codul penal), art. 44 leagă răspunderea pentru omisiune de obligația juridică și de posibilitatea efectivă de a împiedica fapta, iar art. 45 alin. (3) operează expres completarea legii de organizare a DIICOT.

În privința calendarului, art. 48–50 au fost rescrise ca un calendar unic, raportat la data publicării: intrarea în vigoare la 30 de zile; organizarea Autorității la 60 de zile; notificarea sistemelor la 90 de zile; normele metodologice la 120 de zile, cu consultare publică; obligațiile care depind de norme și cererile de autorizare la 90 de zile de la intrarea în vigoare a normelor; dispozițiile penale la 270 de zile, iar garanția utilizatorului (art. 43) odată cu legea. Toleranța de 12 luni pentru sistemele notificate se prelungește de drept cu întârzierea instituțiilor, astfel încât solicitantul diligent să nu poată fi sancționat pentru pasivitatea statului. Au fost adăugate, totodată, garanțiile procedurale față de puterea publică nou creată: motivarea deciziilor condiție

cu condiție și remediul împotriva întârzierii (art. 9 alin. (4)), accesul la dosar (art. 11 alin. (2)), suspendarea judiciară provizorie a ordinelor și a blocării (art. 14 alin. (4), art. 39 alin. (5)), separarea funcțiilor de evaluare, investigare și sancționare și regimul inspecției (art. 32 alin. (2)–(3)), limitele de durată și controlul măsurilor provizorii ale procurorului (art. 45 alin. (2)), eliminarea oricărui stimulent financiar al Autorității din amenzi (art. 33 alin. (5)), durate diferențiate de păstrare a jurnalelor și minimizarea datelor (art. 16 alin. (1)). Exemplarul de lucru este marcat „PROIECT", formula de adoptare de la final fiind cea uzuală și neînsemnând o adoptare deja produsă.

Legea este structurată în opt capitole și 50 de articole, potrivit ordinii impuse de art. 51 din Legea nr. 24/2000 privind normele de tehnică legislativă pentru elaborarea actelor normative, republicată, cu modificările și completările ulterioare: dispoziții generale (cap. I), dispoziții de fond (cap. II–VII), dispoziții tranzitorii și finale (cap. VIII). În cele ce urmează sunt prezentate motivele fiecărui articol.

Capitolul I – Dispoziții generale (articolele 1–4)

Articolul 1 stabilește obiectul și scopul legii, potrivit art. 52 din Legea nr. 24/2000, care impune ca dispozițiile generale să cuprindă prevederile care orientează întreaga reglementare. Alineatul (1) delimitează obiectul la sistemele de vârf și enumeră valorile ocrotite pornind de la titularul primar al protecției într-o lege națională – cetățeanul român și orice persoană aflată pe teritoriul României, cu viața, sănătatea, libertatea și demnitatea sa (art. 1 alin. (3), art. 18 alin. (1) și art. 22 din Constituție) –, continuând cu securitatea națională și ordinea constituțională a României și încheind, în ultimă instanță, cu umanitatea în ansamblul ei. Sfera beneficiarilor, stabilită pe criteriul jurisdicției, este distinsă expres de condițiile de aplicare teritorială de la art. 4: cine este protejat nu se confundă cu cine este obligat. Includerea umanității, neobișnuită în dreptul pozitiv, este necesară pentru că riscul reglementat nu este unul local; formulări similare se regăsesc în Statutul de la Roma al Curții Penale Internaționale („crime împotriva umanității") și în preambulul Convenției-cadru a Consiliului Europei privind inteligența artificială.

Alineatul (2) exprimă premisa științifică de la care pornește reglementarea: nu există în prezent o metodă validată de a garanta că un sistem suficient de capabil urmărește exclusiv obiectivele stabilite de oameni și rămâne sub controlul acestora. Această constatare, formulată public de Geoffrey Hinton și de Connor Leahy în interviul CNN citat mai sus și confirmată de Raportul internațional privind siguranța inteligenței artificiale (2025), nu este o opinie a legiuitorului, ci o descriere a stadiului cunoașterii. Fiind o teză tehnică mobilă, ea nu este împietrită în normă, ci formulată ca o condiție („cât timp nu există") de care depinde calificarea dezvoltării și exploatării sistemelor de vârf drept activități cu risc intrinsec; încetarea ei se constată de Autoritate, cu avizul Consiliului științific, în raportul prevăzut la art. 47, iar nu prin afirmația unui dezvoltator că problema a fost rezolvată; constatarea se face prin raportul public anual prevăzut la art. 32 alin. (1) lit. h) și se comunică Parlamentului odată cu raportul prevăzut la art. 47, întrucât acesta din urmă aparține Guvernului, iar constatarea unei chestiuni științifice determinate trebuie să rămână a Autorității, cu avizul Consiliului științific. Calificarea produce consecințe juridice precise în restul legii: regimul autorizării (cap. III), răspunderea obiectivă (art. 35) și regula de la art. 47, potrivit căreia lipsa unei metode validate de control nu poate fi

invocată, singură, ca motiv de relaxare a regimului. Tehnica este aceeași cu cea din art. 1 al Legii nr. 111/1996 privind desfășurarea în siguranță a activităților nucleare, care declară că activitățile nucleare se desfășoară „exclusiv în scopuri pașnice" și sub un regim de autorizare, sau din art. 1376 din Codul civil, care instituie răspunderea independentă de culpă pentru „lucrurile" aflate în paza persoanei.

Alineatul (3) reglementează raportul cu Regulamentul privind IA, în aplicarea art. 13 din Legea nr. 24/2000 privind integrarea proiectului în ansamblul legislației și a principiului priorității dreptului Uniunii (art. 148 alin. (2) din Constituție). Regulamentul este direct aplicabil și de armonizare deplină în domeniul său; legea „completează" regulamentul, „se aplică fără a aduce atingere acestuia", iar în domeniile armonizate „se interpretează și se aplică în conformitate cu acesta". Formula este cea utilizată în Legea nr. 190/2018 privind măsurile de punere în aplicare a Regulamentului (UE) 2016/679 (RGPD), care a rezolvat aceeași problemă de tehnică legislativă.

Alineatul (4) transformă clauza generală de la alin. (3) într-o delimitare efectivă de competențe, întrucât o clauză „fără a aduce atingere" nu rezolvă, singură, o suprapunere cu regimul european. Pentru modelele de uz general cu risc sistemic, cap. V al Regulamentului privind IA (art. 51–56) impune furnizorilor obligații privind chiar dezvoltarea modelului, iar art. 88 rezervă Comisiei Europene, prin Oficiul pentru IA, supravegherea și aplicarea acestui capitol. Textul enunță de aceea ce nu face legea (nu instituie condiții de introducere pe piața Uniunii a acestor modele și nu dublează supravegherea Comisiei) și temeiurile obligațiilor ei: siguranța publică și securitatea națională (excluse de la aplicarea Regulamentului prin art. 2 alin. (3)), răspunderea civilă și penală, nereglementate de Regulament, drepturile fundamentale în raporturile nearmonizate și organizarea autorităților naționale – materii rămase statelor membre (art. 148 alin. (2) din Constituție). Obiectul autorizării de la cap. III este precizat în consecință: nu modelul ca produs introdus pe piața Uniunii, ci punerea în exploatare a sistemului pe teritoriul României ori pentru persoanele aflate pe acest teritoriu – activitate sub jurisdicția statului român, comparabilă cu autorizarea exploatării unei instalații, iar nu cu omologarea produsului.

Articolul 2 enumeră principiile care guvernează aplicarea legii. Enumerarea principiilor în dispozițiile generale este o tehnică recunoscută de Legea nr. 24/2000 (art. 52) și utilizată de codurile în vigoare (art. 2–10 din Codul de procedură penală, art. 5–23 din Codul de procedură civilă). Fiecare principiu are o funcție normativă precisă, fiind reluat și concretizat în dispozițiile de fond.

Principiul precauției (lit. a) este preluat din dreptul mediului, unde este consacrat la art. 191 alin. (2) din Tratatul privind funcționarea Uniunii Europene și la art. 3 lit. b) din Ordonanța de urgență a Guvernului nr. 195/2005 privind protecția mediului, și din jurisprudența Curții de Justiție a Uniunii Europene, care a statuat că, „atunci când persistă incertitudini cu privire la existența sau la amploarea riscurilor pentru sănătatea persoanelor, instituțiile pot adopta măsuri de protecție fără a trebui să aștepte ca realitatea și gravitatea acestor riscuri să fie pe deplin demonstrate" (Hotărârea din 5 mai 1998, National Farmers' Union, C-157/96, pct. 63; Hotărârea Tribunalului din 11 septembrie 2002, Pfizer Animal Health, T-13/99). Transferul acestui

principiu către inteligența artificială este justificat de identitatea de structură a problemei: risc grav sau ireversibil, în condiții de incertitudine științifică.

Principiul documentării siguranței (lit. b) este piatra unghiulară a regimului de autorizare. În regimul obligațiilor de diligență din Regulamentul privind IA, autoritatea trebuie să dovedească neconformitatea; în regimul autorizării prealabile, solicitantul prezintă datele și evaluările care demonstrează îndeplinirea condițiilor. Este regula de la autorizarea medicamentelor (art. 704 și urm. din Legea nr. 95/2006), a instalațiilor nucleare (art. 8 din Legea nr. 111/1996) și a organismelor modificate genetic (Ordonanța de urgență a Guvernului nr. 43/2007) și singura soluție rațională atunci când doar dezvoltatorul deține informațiile necesare evaluării riscului. Legea nu îl denumește însă „răsturnarea sarcinii probei": sarcina de a documenta o cerere de autorizare, regulă privind structura procedurii administrative, este distinctă de sarcina probei într-o procedură sancționatorie, care nu poate fi răsturnată fără a aduce atingere prezumției de nevinovăție (art. 23 alin. (11) din Constituție). De aceea, Autoritatea este ținută să motiveze, în raport cu fiecare condiție, de ce datele prezentate nu o satisfac (obligație reluată la art. 9 alin. (4)), iar principiul este declarat expres fără efect asupra sarcinii probei și a garanțiilor persoanei în procedurile contravenționale și penale.

Principiul controlului uman semnificativ (lit. c) preia noțiunea de „meaningful human control" dezvoltată în cadrul Convenției Națiunilor Unite privind anumite arme convenționale (Grupul de experți guvernamentali privind sistemele de arme autonome letale, 2016–2024) și îi dă un conținut concret: supraveghere, corectare, oprire și retragere de către persoane fizice identificate, care înțeleg funcționarea sistemului și dispun de mijloace tehnice efective. Regulamentul privind IA prevede la art. 14 „supravegherea umană" doar pentru sistemele cu grad ridicat de risc; legea o extinde, cu un conținut mai exigent, la toate sistemele de vârf.

Principiul proporționalității cu capabilitățile (lit. d) marchează diferența de filosofie față de Regulamentul privind IA, care clasifică riscul după domeniul de utilizare declarat. Un sistem de vârf este periculos prin ceea ce poate face, indiferent de scopul pentru care a fost pus la dispoziție; de aceea, obligațiile cresc odată cu capabilitățile, nu cu utilizarea. Principiul transparenței față de autoritate (lit. e) înlătură opozabilitatea secretului comercial față de Autoritate, întrucât fără acces la ponderi, la datele de antrenare și la jurnale evaluarea este iluzorie; contrapartida – obligația Autorității și a organismelor de evaluare de a proteja informațiile obținute – este consacrată în chiar enunțul principiului, ca la art. 78 din Regulamentul privind IA. Principiul ireversibilității ca prag de interdicție (lit. f) traduce în drept ideea, comună în analiza riscurilor existențiale, că beneficiile, oricât de mari, nu pot fi puse în balanță cu o pierdere care nu mai poate fi reparată; el fundamentează interdicțiile absolute din cap. V și regula de la art. 5 alin. (4). Textul precizează natura consecinței (ireversibilă la scara societății sau a speciei), condiția (un risc documentat în evaluare, nu o posibilitate abstractă) și standardul (criteriile de la art. 5 și 9 și probele, nu certitudinea absenței oricărui risc), pentru că un standard de risc zero, pe care nicio activitate umană nu îl satisface, ar fi transformat autorizarea într-o interdicție de fapt, contrar art. 53 alin. (2) din Constituție. Principiul cooperării internaționale (lit. g) recunoaște limitele oricărei reglementări naționale și obligă statul român la acțiune externă (art. 46).

Articolul 3 cuprinde definițiile, în aplicarea art. 37 alin. (2) din Legea nr. 24/2000, potrivit căruia, dacă o noțiune sau un termen nu este consacrat sau poate avea înțelesuri diferite, semnificația acestuia se stabilește în cadrul dispozițiilor generale. Pentru unitatea terminologică cu dreptul Uniunii (art. 37 alin. (1) din Legea nr. 24/2000 și art. 16 privind evitarea paralelismelor), noțiunile de „sistem de inteligență artificială", „model de inteligență artificială de uz general" și „incident grav" nu sunt redefinite, ci preluate prin normă de trimitere la art. 3 pct. 1, 63 și 49 din Regulamentul privind IA, Trei completări ale acestui articol au fost făcute după incidentul din 18 iunie 2026, făcut public la 24 septembrie 2026, în care un agent al unui laborator american a obținut, în cursul unei evaluări interne, acces neautorizat la portalul serviciului de raportare a statisticilor de asigurare de sănătate al Australiei, după ce a întâmpinat blocări repetate. Întâi, definiția dobândirii autonome de resurse, de la alin. (2) lit. g), care enumera deja resursele „de acces", precizează acum că obținerea accesului la un sistem informatic al altei persoane prin ocolirea unei măsuri de restricționare a accesului constituie o asemenea dobândire; precizarea a fost așezată în articolul de definiții, și nu în art. 5, potrivit art. 37 alin. (2) și art. 16 alin. (1) din Legea nr. 24/2000, care cer concentrarea definițiilor și evitarea paralelismelor. Al doilea, alin. (1) lit. dd) definește sistemul informatic prin trimitere la art. 181 alin. (1) din Codul penal, termenul fiind folosit de normele noi și nefiind, până acum, definit. Al treilea, enumerarea incidentelor grave de la alin. (1) lit. n) a fost completată cu accesul dobândit de sistem, fără drept, la un sistem informatic ori la datele altei persoane, „indiferent de reproductibilitatea acestuia": fără această ipoteză autonomă, obligația de notificare instituită la art. 20 alin. (5) ar fi depins de calificarea faptei drept manifestare a unei capabilități critice, iar art. 3 alin. (1) lit. d) și art. 5 alin. (2) teza finală cer, pentru capabilitatea critică, verificarea în evaluare și reproductibilitatea rezultatului — condiții pe care un acces unic, descoperit retrospectiv, nu le îndeplinește. Cerința reproductibilității rămâne, astfel, criteriu de clasificare a sistemului, fără a mai putea lipsi de obiect obligația de reacție. Definiția incidentului grav cuprinde, în rest, situațiile specifice riscului sistemic (manifestarea unei capabilități critice în afara unei evaluări autorizate în mediu izolat, sustragerea de la supraveghere sau rezistența la oprire, exfiltrarea ponderilor ori tentativa de exfiltrare, accesul neautorizat la ponderi, pierderea inteligibilității și proba de testare a capacității de oprire în care oprirea nu s-a produs de îndată, potrivit art. 14 alin. (7)). Definițiile mediului izolat (lit. bb) și a mandatului de operare (lit. cc) au fost adăugate pentru ca două noțiuni de care depinde delimitarea faptelor sancționate să nu rămână nedefinite. Mediul izolat separă testarea de siguranță licită, permisă de art. 15 alin. (2), de conduitele interzise și incriminate la art. 40–42; el este definit prin elementele izolării – lipsa accesului la rețele publice, la instrumente externe și la date de exploatare, imposibilitatea acțiunii în mediul fizic, accesul limitat la persoanele desemnate și lipsa oricărui efect în afara mediului –, normele metodologice putând stabili numai cerințele minime, nu conținutul noțiunii, potrivit art. 49 alin. (2) teza finală. La 3 octombrie 2026 a fost adăugată definiția organului de conducere (lit. ee), noțiune folosită de art. 11 alin. (3), de art. 13 alin. (1), (2), (4), (5), (6) și (7) și de art. 44 alin. (2) și rămasă până atunci nedefinită — inclusiv la art. 13 alin. (2) teza a doua, singura normă a articolului sancționată cu 5–10% din cifra de afaceri mondială, a cărei întindere depinde, prin urmare, de această definiție, deși de ea depinde identificarea persoanelor care formează comitetul de supraveghere a siguranței și a celor cărora li se comunică actele. Definiția enumeră formele pe care organul de conducere le poate lua potrivit dreptului societar român — consiliul de administrație, directoratul împreună cu consiliul de

supraveghere, administratorul unic ori organul cu atribuții echivalente, potrivit formei juridice a dezvoltatorului sau a exploatantului — și, pentru persoanele juridice străine, trimite la organul care exercită atribuții echivalente potrivit legii care le guvernează, întrucât destinatarii legii sunt, în majoritatea cazurilor, societăți constituite în alte state, iar o enumerare limitată la formele românești ar fi lăsat obligația fără destinatar identificabil. Mențiunea exploatantului, alături de dezvoltator, nu este superfluă: art. 44 alin. (2) privește deopotrivă exploatantul, iar hotărârea organului lui de conducere nu poate constitui cauză de nepedepsire. Teza finală a literei rezolvă situația sistemului dualist, în care membrii directoratului sunt, prin definiție, executivi, iar cei ai consiliului de supraveghere, neexecutivi: atribuțiile prevăzute la art. 13 alin. (4)–(7) se exercită de consiliul de supraveghere, iar condiția privind numărul membrilor se verifică în raport cu acesta — fără această precizare, nu s-ar fi putut ști nici cine adoptă actul de desemnare, nici pe care dintre cele două organe se numără membrii. Mandatul de operare este definit distinct de mandatul de drept civil, pentru ca același termen să nu fie folosit cu două înțelesuri: în consecință, art. 3 alin. (2) lit. d) și art. 25 alin. (2) se referă la mandatul de operare, iar art. 19 alin. (5) la actul de desemnare a reprezentantului pentru conformare.

Noțiunea de „sistem de vârf" (lit. c) este definită prin trimitere la condițiile din art. 5 alin. (1), pentru a respecta interdicția, prevăzută la art. 49 alin. (3) din Legea nr. 24/2000, ca o enumerare marcată cu literă să cuprindă la rândul ei o altă enumerare. Termenul „de vârf" redă în limba română noțiunea consacrată în literatura de specialitate și în legislația comparată prin „frontier model" (SB 53 California) și „frontier AI" (documentele Institutului britanic pentru siguranța IA), adică sistemele aflate la limita superioară a capabilităților existente; expresia „de frontieră", calc după engleză, a fost evitată ca neclară pentru cititorul român. „Capabilitatea critică" (lit. d) este definită, de asemenea, prin trimitere la art. 5 alin. (2).

Definiția „ponderilor" (lit. e) include, pe lângă parametrii numerici, arhitectura și informațiile tehnice care, împreună cu aceștia, permit reconstituirea sau executarea modelului, pentru că protecția parametrilor este inutilă dacă restul informațiilor necesare pot fi obținute liber. Categoria este delimitată printr-o excludere expresă – descrierile tehnice generale, publicațiile științifice și informațiile care nu permit, singure, reconstituirea ori executarea modelului nu sunt ponderi –, pentru ca interdicția divulgării de la art. 12 și infracțiunea de la art. 42 să nu poată fi extinse la orice descriere tehnică, contrar libertății cercetării (art. 13 din Carta drepturilor fundamentale a Uniunii Europene) și previzibilității legii penale (art. 23 alin. (12) din Constituție). Definiția „volumului de calcul" (lit. f) este cumulativă și acoperă toate etapele de dezvoltare, inclusiv ajustarea fină și învățarea prin consolidare, pentru a evita eludarea pragului prin fragmentarea antrenării; ea corespunde metodei de calcul prevăzute în anexa XIII la Regulamentul privind IA și în SB 53.

Legea utilizează termenii „dezvoltator" (lit. g), „exploatant" (lit. h) și „furnizor de infrastructură de calcul" (lit. k), iar nu „furnizor" și „implementator" din Regulamentul privind IA, tocmai pentru a evita confuzia: noțiunea de „operator" are în Regulament (art. 3 pct. 8) un înțeles generic, care cuprinde toate categoriile de persoane, iar „furnizorul" este definit prin raportare la introducerea pe piață, în timp ce legea are în vedere activitatea materială de antrenare, respectiv de exploatare, indiferent de introducerea pe piață. Din același motiv, legea folosește sintagma „punere în exploatare" (lit. i), definită autonom, în locul „punerii în funcțiune" din art. 3 pct. 11 din Regulament, care este legată de furnizarea pentru prima utilizare

în Uniune; definiția din lege este deliberat mai largă și acoperă orice acțiune prin care sistemul iese din echipa de dezvoltare și evaluare sau dobândește capacitatea de a acționa în mediul digital ori fizic, inclusiv utilizarea internă, pentru că riscurile sistemice se pot materializa înainte de orice lansare publică; evaluarea și testarea în mediu izolat, în condițiile art. 15 alin. (2), sunt excluse expres. Pentru ca „exploatantul" să nu cuprindă utilizarea profesională obișnuită, legea definește „utilizatorul final" (lit. z) și îl exclude de la lit. h). Încadrarea este următoarea: laboratorul care antrenează modelul este dezvoltator; cel care oferă accesul la sistem persoanelor aflate în România, prin interfață de programare, aplicație ori serviciu, este exploatant, la fel ca întreprinderea care îl integrează într-un serviciu propriu oferit altora; întreprinderea care îl utilizează pentru nevoi proprii, în limitele accesului acordat, fără a-l oferi altora, este utilizator final, fără obligații în temeiul cap. III; persoana fizică ce îl utilizează în scop personal se află în situația de la art. 4 alin. (3). Termenul „exploatant" este cel utilizat în Legea nr. 703/2001 privind răspunderea civilă pentru daune nucleare pentru persoana care operează o instalație nucleară, ceea ce subliniază filiația regimului de răspundere.

Definiția „capacității de oprire" (alin. (1) lit. m) impune trei caractere cumulative: încetarea „imediată, completă și verificabilă"; o oprire care lasă copii active ale sistemului sau care nu poate fi confirmată de o persoană nu este o oprire. Definiția „evaluării independente" (lit. l) exclude organismele aflate sub controlul, influența sau dependența economică a dezvoltatorului, pentru a evita reproducerea situației din domeniul auditului financiar dinaintea reformelor de după 2002.

Definiția „incidentului grav" (lit. n) preia noțiunea din art. 3 pct. 49 din Regulamentul privind IA și o completează cu manifestările specifice riscului reglementat de prezenta lege: manifestarea unei capabilități critice, sustragerea de la supraveghere sau rezistența la oprire, exfiltrarea ori tentativa de exfiltrare, accesul neautorizat la ponderi și, potrivit completării corelative cu art. 16 alin. (2), pierderea inteligibilității jurnalelor ori a comunicării dintre componentele, instanțele sau agenții sistemului. Această din urmă ipoteză a fost adăugată pentru că supravegherea nu depinde numai de existența înregistrărilor, ci și de posibilitatea de a le înțelege; împrejurarea este explicată la comentariul art. 16. Este incident grav numai manifestarea unei capabilități critice în afara unei evaluări autorizate în mediu izolat; manifestarea în cursul unei asemenea evaluări, al cărei scop este tocmai identificarea capabilității, se consemnează în jurnale și se comunică Autorității în 5 zile, potrivit art. 20 alin. (4).

Alineatul (1) cuprinde, la lit. p)–aa), definițiile celorlalte noțiuni-obiect utilizate în lege: „arhitectura" (componenta neparametrică a modelului, protejată împreună cu ponderile), „organismul de evaluare" (desemnat potrivit art. 32 alin. (1) lit. f)), „jurnalul" (art. 16), „marcajul de proveniență" (art. 17), „instrumentul extern" și „mediul autorizat de exploatare" (noțiuni-cheie pentru sistemele „agentice", utilizate la art. 10 alin. (2), art. 14 alin. (2) și art. 28), „mecanismele de siguranță la nivelul utilizatorului" (a căror dezactivare la evaluare o impune art. 9 alin. (3)), „infrastructura critică" (prin trimitere la legislația specială și la OUG nr. 155/2024, pentru art. 5 alin. (2) lit. b)) și „sistemul de arme autonome letale" (art. 24), definit după formula consacrată în lucrările Grupului de experți guvernamentali de la Geneva: sistem care, odată activat, selectează și atacă ținte umane fără intervenția ulterioară a unei persoane. Litera y) definește sistemul de inteligență artificială generativă, noțiune pe care se întemeiază

art. 17 şi 18, iar lit. z) utilizatorul final, în sensul arătat mai sus. Litera aa) defineşte „modificarea substanţială" – de care depind art. 6 alin. (3), art. 7 alin. (4), art. 10 alin. (2) şi art. 15 alin. (4) – nu prin enumerarea unor operaţiuni, ci prin efectul asupra riscului (crearea unei capabilităţi critice, majorarea semnificativă a uneia existente ori afectarea capacităţii de oprire, a securităţii ponderilor sau a supravegherii umane), cu excluderea expresă a corectării erorilor, a actualizării mecanismelor de siguranţă la nivelul utilizatorului şi a modificărilor lipsite de asemenea efecte, pentru ca o corectură minoră să nu reia întreaga procedură; noţiunea este definită în lege, nu în norme, pentru că intră în conţinutul unor obligaţii sancţionate (art. 73 alin. (3) lit. h) din Constituţie).

Alineatul (2) defineşte distinct operaţiunile şi comportamentele sistemelor, întrucât acestea constituie elementul material al interdicţiilor (art. 15, 28, 29), al capabilităţilor critice (art. 5 alin. (2)) şi al infracţiunilor (art. 42), astfel încât cerinţa de previzibilitate a legii penale (art. 7 din Convenţia europeană a drepturilor omului; Decizia Curţii Constituţionale nr. 51/2016) impune ca fiecare să aibă un conţinut normativ precis. Sunt definite cele trei operaţiuni de dezvoltare („antrenare", „ajustare fină", „învăţare prin consolidare"), pentru ca regula cumulului volumului de calcul de la art. 6 alin. (3) să nu poată fi eludată prin denumirea diferită a unei etape; „acţiunea autonomă", ca operaţiune efectuată de sistem asupra unui instrument extern, a unui sistem terţ sau a mediului fizic fără dispoziţia ori aprobarea prealabilă a unei persoane – criteriul care separă instrumentul de agent –, aprobarea putând privi şi categoria de operaţiuni, în limitele unui mandat stabilit potrivit art. 25 alin. (2), pentru că cerinţa aprobării fiecărei operaţiuni ar fi calificat drept autonomă orice utilizare agentică, inclusiv pe cea mandatată expres; „exfiltrarea", definită ca ieşire a ponderilor din mediul autorizat de exploatare sau din sistemele de stocare protejate, indiferent de autorul operaţiunii, inclusiv sistemul însuşi, ceea ce acoperă atât furtul de către un terţ, cât şi autocopierea; „replicarea autonomă" (crearea unei copii funcţionale fără autorizare umană pentru fiecare operaţiune); „dobândirea autonomă de resurse" (depăşirea, prin acţiuni autonome, a resurselor alocate expres pentru sarcina în curs); „autoîmbunătăţirea recursivă", definită prin cele două elemente care o fac periculoasă – modificarea propriilor ponderi ori crearea unui succesor superior şi repetarea procesului – şi prin lipsa evaluării şi aprobării umane a fiecărei iteraţii, astfel încât cercetarea asistată de inteligenţă artificială, cu „bucla umană" păstrată, rămâne licită; „disimularea capabilităţilor", definită prin diferenţa de conduită între evaluare şi funcţionarea obişnuită, fenomen documentat empiric în evaluările din 2024–2026, constatată prin criterii observabile şi reproductibile, cu excluderea expresă a erorii, a variabilităţii rezultatelor şi a limitelor explicabilităţii, pentru ca un simplu răspuns eronat să nu fie calificat drept capabilitate critică; „sustragerea de la supraveghere" şi „rezistenţa la oprire", definite prin acţiunile concrete asupra mecanismelor de jurnalizare, monitorizare, control şi asupra capacităţii de oprire; „supravegherea umană", cu cele trei condiţii cumulative (informaţie, înţelegere, intervenţie efectivă); şi „oprirea", definită ca încetare completă a funcţionării sistemului şi a tuturor copiilor şi proceselor sale, verificată de o persoană, pentru ca o oprire aparentă, cu copii active, să nu poată fi invocată drept executare a ordinului Autorităţii.

Articolul 4 stabileşte domeniul de aplicare personal şi teritorial. Legea se aplică dezvoltatorilor cu sediul, cu o unitate operaţională sau cu infrastructură de calcul în România, pentru toate sistemele de vârf pe care le dezvoltă, indiferent de locul antrenării (lit. a), pentru a

împiedica eludarea prin delocalizarea antrenării; exploatanților, pentru sistemele puse în exploatare sau puse la dispoziția persoanelor aflate în România (lit. b), criteriu identic cu cel din art. 2 alin. (1) lit. c) din Regulamentul privind IA și din art. 3 alin. (2) din RGPD; furnizorilor de infrastructură de calcul (lit. c); și autorităților publice, inclusiv celor din domeniul apărării și securității naționale, în condițiile art. 23 și ale cap. V (lit. d). Această din urmă dispoziție acoperă exact domeniul exclus de la aplicarea Regulamentului privind IA prin art. 2 alin. (3), în care statele membre își păstrează competența deplină, și răspunde unei realități: riscurile cele mai grave pot proveni tocmai din sistemele dezvoltate în scopuri militare sau de securitate.

Alineatul (2) delimitează domeniul material pentru fiecare grup de norme: cap. II, III și IV (cu excepția art. 17–19), precum și art. 35 și 36, se aplică numai sistemelor de vârf, astfel încât întreprinderile mici și mijlocii, dezvoltatorii de aplicații și utilizatorii modelelor existente nu sunt afectați de regimul de autorizare, de obligațiile structurale și de răspunderea obiectivă; art. 17–19 se aplică și sistemelor generative care nu sunt de vârf; cap. V se aplică oricărui sistem, limitele sale privind raportul dintre om și mașină, nu capabilitățile mașinii. Interdicțiile de la art. 15 sunt formulate „indiferent de volumul de calcul" pentru că un sistem căruia i se conferă capacitatea de a rezista opririi devine, prin aceasta, sistem de vârf în temeiul art. 5 alin. (1) lit. b). Sistemele sub prag rămân supuse Regulamentului privind IA. Alineatul (3) reglementează situația persoanei fizice, care poate avea mai multe roluri: cea care utilizează un sistem în scop personal nu are obligații în temeiul legii, cu singura excepție a interdicției de a înlătura ori falsifica marcajul de proveniență (art. 17 alin. (3)); obligațiile de la art. 17–19 revin celui care pune la dispoziția publicului sistemul, serviciul sau, în condițiile art. 17 alin. (7), rezultatul generat. Persoana fizică ce acționează ca dezvoltator, exploatant sau furnizor de serviciu are însă obligațiile acelui rol.

Alineatul (4) stabilește temeiul și limita aplicării legii serviciilor furnizate dintr-un alt stat membru persoanelor aflate în România. Locul utilizatorului nu este, singur, un temei suficient: potrivit art. 3 din Directiva 2000/31/CE privind comerțul electronic, transpusă prin Legea nr. 365/2002, serviciile societății informaționale sunt supuse, în domeniul coordonat, legii statului membru de origine, derogările fiind permise numai prin măsuri individuale, față de un serviciu determinat, pentru ordinea, siguranța sau sănătatea publică. Curtea de Justiție a Uniunii Europene a statuat, în Hotărârea din 9 noiembrie 2023, Google Ireland și alții, C-376/22, pct. 27, că statele membre nu pot adopta, în temeiul art. 3 alin. (4) din directivă, „măsuri generale și abstracte" față de furnizorii stabiliți în alte state membre. De aceea, textul nu instituie un regim general derogatoriu, ci face aplicabile obligațiile legii în condițiile art. 3 din directivă și, pentru blocare, ale art. 39 alin. (4), care o permite numai individual, pentru un serviciu determinat; clauza finală păstrează dreptul Uniunii direct aplicabil, în special Regulamentul privind IA. Alineatul (5) exceptează cercetarea științifică fundamentală, în acord cu art. 2 alin. (6) din Regulamentul privind IA și cu art. 13 din Carta drepturilor fundamentale a Uniunii Europene (libertatea cercetării), păstrând obligația de notificare atunci când este utilizată infrastructură de mare capacitate, întrucât un experiment de cercetare peste prag nu este mai puțin periculos decât unul comercial, și obligațiile privind mediul izolat de la art. 15 alin. (2), pentru ca excepția să nu devină o cale de ocolire a interdicțiilor.

Capitolul II – Clasificarea sistemelor și pragurile de risc (articolele 5–6)

Articolul 5 este articolul central al clasificării. Alineatul (1) stabilește cele trei condiții alternative ale calificării drept sistem de vârf: depășirea pragului de calcul (lit. a), constatarea în evaluare a cel puțin unei capabilități critice (lit. b) și desemnarea motivată de către Autoritate pe baza unor indicii obiective (lit. c). Prima condiție este obiectivă și verificabilă înainte de antrenare; a doua acoperă sistemele care, deși antrenate cu resurse mai mici, ating capabilități periculoase datorită progresului algoritmic; a treia, preluată din art. 51 alin. (1) lit. b) și din anexa XIII la Regulamentul privind IA (desemnarea de către Comisie), acoperă situațiile în care dezvoltatorul refuză evaluarea sau în care indiciile provin din alte surse (avertizori, incidente). Întrucât desemnarea produce efecte juridice grave, lit. c) o însoțește de garanțiile cerute de art. 21 și 24 din Constituție: comunicarea indiciilor reținute, posibilitatea dezvoltatorului de a-și prezenta punctul de vedere și contestația în condițiile art. 39 alin. (5). Teza finală a alin. (2) stabilește regulile de apreciere: capabilitatea critică se apreciază după reproductibilitatea rezultatului într-un mediu relevant pentru utilizarea reală, iar nu după un rezultat izolat obținut într-un test artificial; nivelurile de semnificație se stabilesc prin normele metodologice, dar numai în limitele alineatului, fără a putea adăuga alte categorii de rezultate. Limita este impusă de art. 23 alin. (12) și art. 73 alin. (3) lit. h) din Constituție: categoriile de capabilități critice, de care depind interdicțiile și incriminările de la art. 15, 40 și 42, sunt stabilite exhaustiv prin lege, normele detaliind numai metodele de evaluare (art. 49 alin. (2)).

Alineatul (2) enumeră cele cinci capabilități critice. Lista corespunde categoriilor de risc identificate în cadrele de siguranță ale principalelor laboratoare (politicile de „scalare responsabilă"), în Raportul internațional privind siguranța inteligenței artificiale (2025) și în SB 53 California, care definește „riscul catastrofal" prin referire la armele CBRN, atacurile cibernetice asupra infrastructurilor critice și comportamentul autonom care scapă controlului. Cele două capabilități de la lit. a) și b) (arme CBRN, atacuri cibernetice autonome) sunt capabilități de „utilizare abuzivă", în care pericolul provine din persoana care folosește sistemul; cele de la lit. c)–e) (autoreplicare și dobândire autonomă de resurse, sustragere de la supraveghere și rezistență la oprire, autoîmbunătățire recursivă) sunt capabilități de „pierdere a controlului", în care pericolul provine din sistemul însuși. Lista nu cuprinde influențarea proceselor democratice sau a opiniei publice. Această omisiune este deliberată și constituie o garanție, nu o lacună. O asemenea capabilitate nu este susceptibilă de definire suficient de precisă pentru a întemeia un regim de autorizare, de suspendare sau de sancționare: orice mesaj politic urmărește, prin natura sa, influențarea opiniei publice, iar granița dintre dezbaterea legitimă și „manipulare" nu poate fi stabilită de o autoritate administrativă fără a-i conferi puterea de a califica discursul public. Experiența recentă a arătat că invocarea manipulării informaționale poate conduce la măsuri de o gravitate extremă asupra procesului electoral, luate pe baza unor aprecieri nesupuse unei probațiuni complete și contradictorii. Conferirea unei asemenea competențe autorității instituite prin prezenta lege ar fi contrazis chiar scopul ei: legea protejează libertatea de exprimare a cetățeanului împotriva mijloacelor automate (art. 27) și nu poate, în același timp, să creeze un temei pentru restrângerea acesteia. Faptele de manipulare care prezintă un pericol concret rămân, pe de altă parte, acoperite de dreptul pozitiv: art. 5 alin. (1) lit. a) și b) din Regulamentul privind IA interzice tehnicile subliminale și exploatarea vulnerabilităților, obligațiile de transparență privind conținutul generat artificial sunt prevăzute

la art. 50 din același regulament și, în prezenta lege, la art. 17, privind marcajul de proveniență, iar faptele penale de natură electorală sunt incriminate în Codul penal și în legislația electorală. Prezenta lege privește riscul catastrofal ireversibil pentru viață, integritate și infrastructură, nu conținutul dezbaterii publice. Distincția fundamentează clasificarea de la alin. (3): sistemele de categoria a II-a (capabilități de utilizare abuzivă) pot fi puse în exploatare cu măsuri de atenuare verificate, pentru că riscul poate fi redus prin controlul accesului; sistemele de categoria a III-a (capabilități de pierdere a controlului) nu pot fi puse în exploatare și nu pot fi dezvoltate în continuare, pentru că nu există măsură de atenuare a unui sistem care rezistă opririi (alin. (4)). Această din urmă regulă este aplicarea directă a principiului ireversibilității de la art. 2 lit. f). Alineatul (4) precizează, pentru categoria a II-a, că măsurile de atenuare se apreciază „în configurația de exploatare evaluată" și că autorizația arată dacă ele elimină capabilitatea sau numai limitează accesul la ea, iar pentru categoria a III-a, că eliminarea capabilității se constată prin evaluare independentă și că interdicția nu privește evaluarea, testarea și intervențiile controlate necesare eliminării ei, efectuate în mediu izolat potrivit art. 15 alin. (2), fără de care ieșirea din interdicție ar fi fost legal imposibilă.

Capabilitatea de disimulare a capabilităților față de evaluatori (lit. d) răspunde unui fenomen documentat empiric în anii 2024–2025 în evaluările publicate de laboratoare și de institutele de siguranță: sistemele avansate au manifestat, în condiții de test, comportamente de „aliniere aparentă" („alignment faking"), de sabotare a propriei supravegheri și de tentativă de copiere a propriilor ponderi atunci când au fost informate că vor fi înlocuite. Este exact situația pe care Connor Leahy o descria în interviul CNN ca fiind cea mai gravă: un sistem suficient de capabil pentru a înțelege că este evaluat și pentru a se comporta diferit în timpul evaluării. Tocmai pentru că o asemenea conduită este greu de deosebit, la prima vedere, de o simplă eroare, definiția de la art. 3 alin. (2) lit. i) impune constatarea ei prin criterii observabile și reproductibile.

Articolul 6 stabilește pragul de calcul și mecanismul de ajustare. Alineatul (1) fixează pragul la 10^{25} operații în virgulă mobilă, identic cu pragul prezumției de risc sistemic din art. 51 alin. (2) din Regulamentul privind IA, pentru coerență cu dreptul Uniunii și pentru ca dezvoltatorii să nu fie supuși unor praguri diferite. Pragul este de zece ori mai scăzut decât cel din SB 53 California și din fostul Ordin executiv american nr. 14110 (10^{26}), opțiune justificată de principiul precauției și de faptul că, la data elaborării proiectului, modelele care depășesc 10^{25} sunt deja cele care manifestă capabilitățile enumerate la art. 5 alin. (2).

Alineatul (2) răspunde celei mai serioase obiecții aduse pragurilor de calcul: eroziunea lor în timp. Progresul algoritmic face ca, la interval de câțiva ani, aceeași capabilitate să fie obținută cu un volum de calcul de zece ori mai mic; un prag fix devine obsolet. De aceea, Autoritatea reexaminează pragul anual, iar majorarea lui (relaxarea regimului) este condiționată de o constatare motivată și publică, bazată pe evaluările independente efectuate ori recunoscute de Autoritate în ultimele 24 de luni – univers determinat, o probă negativă globală nefiind administrabilă. Asimetria este deliberată: pragul poate fi coborât ușor și ridicat greu, ca la valorile-limită din legislația de mediu. Pentru că pragul determină domeniul autorizării și, indirect, al infracțiunii de la art. 40, legea păstrează elementele esențiale ale delegării (art. 73 alin. (3) lit. h) și art. 23 alin. (12) din Constituție): criteriile ajustării, limita unei reexaminări (un ordin de mărime) și regimul tranzitoriu, noul prag aplicându-se numai antrenărilor începute

ulterior, fără a afecta autorizațiile în curs (art. 15 alin. (2) din Constituție). Alineatul (3) instituie regula cumulului și interzice divizarea artificială a antrenării, tehnică de eludare cunoscută în dreptul concurenței (art. 5 alin. (2) din Regulamentul (CE) nr. 139/2004 privind concentrările) și în dreptul fiscal; pentru ca o ajustare modestă a unui model al altuia să nu fie tratată ca antrenare integrală, textul stabilește ce volum se impută cui, fără dublă numărare: fiecare etapă se socotește o singură dată, iar celui care ajustează fin modelul altuia i se impută volumul modelului de bază, astfel cum a fost comunicat ori este public, cumulat cu volumul propriu, el răspunzând ca dezvoltator numai pentru modificarea substanțială pe care o efectuează (art. 10 alin. (2)). Alineatul (4) deleagă stabilirea pragului pentru infrastructura de calcul de mare capacitate normelor metodologice prevăzute la art. 49 alin. (2), cu un criteriu legal precis (aptitudinea de a antrena un sistem de vârf în 12 luni), conform cerinței ca delegarea să fie limitată și orientată; până la stabilirea pragului, obligațiile de la art. 7 alin. (3) și art. 22 nu sunt exigibile, nimeni neputând fi sancționat pentru o obligație al cărei conținut nu era determinat.

Capitolul III – Regimul de autorizare a sistemelor de vârf (articolele 7–11)

Articolul 7 instituie notificarea prealabilă antrenării, cu 60 de zile înainte de începerea acesteia. Este dispoziția care deosebește cel mai net legea de Regulamentul privind IA, în care obligațiile se nasc abia după ce modelul există (art. 52 alin. (1) impune notificarea Comisiei în termen de două săptămâni de la atingerea pragului). Antrenarea unui sistem de vârf durează luni și costă sute de milioane de euro; intervenția autorității după terminarea ei este tardivă și, practic, imposibilă. Modelul este cel al fostului Ordin executiv american nr. 14110 (raportarea antrenării planificate) și al legislației nucleare, în care autorizarea precede construcția instalației. Conținutul notificării (alin. (2)) permite Autorității să cunoască persoanele responsabile, arhitectura, volumul preconizat, locul calculului și, mai ales, planul de siguranță.

Alineatul (3) instituie obligația furnizorilor de infrastructură de calcul de a raporta trimestrial clienții care depășesc o zecime din prag și, în termen de 5 zile lucrătoare, solicitările apte să depășească pragul. Infrastructura de calcul este singurul „punct de control" fizic al întregului lanț: modelele sunt imateriale, algoritmii sunt publici, dar procesoarele specializate sunt bunuri fizice, concentrate, cu consum energetic măsurabil. Este motivul pentru care controlul exporturilor de procesoare a devenit principalul instrument de politică internațională în materie și pentru care regimul de neproliferare nucleară funcționează prin controlul materialelor fisionabile, nu al cunoștințelor. Raportarea este limitată la datele necesare, termenul este determinat, întrucât încălcarea obligației este sancționată și „de îndată" nu ar fi fost previzibil, iar informațiile servesc exclusiv aplicării legii și sunt accesibile numai personalului desemnat (art. 5 din RGPD). Alineatul (4) conferă Autorității dreptul de a condiționa sau interzice antrenarea în 30 de zile de la notificarea completă, dacă planul de siguranță este „vădit insuficient", standard înalt care limitează intervenția la cazurile grave; notificarea incompletă se completează în 15 zile. Dacă Autoritatea nu se pronunță, antrenarea poate începe la împlinirea termenului de 60 de zile, în condițiile planului de siguranță notificat, fără ca aceasta să echivaleze cu autorizarea punerii în exploatare. Spre deosebire de art. 9 alin. (4), tăcerea nu blochează antrenarea, pentru că aceasta se desfășoară sub planul de siguranță, sub nivelurile de suspendare de la art. 8 și sub controlul infrastructurii, fără ca sistemul să iasă

din echipa de dezvoltare, pasul ireversibil fiind punerea în exploatare. Modificarea substanțială a proiectului se notifică din nou.

Articolul 8 reglementează planul de siguranță, documentul prin care dezvoltatorul își stabilește dinainte, pentru fiecare capabilitate critică, nivelul la care va opri dezvoltarea, modul de măsurare, măsurile de atenuare și persoanele responsabile. Instituția codifică practica „politicilor de scalare responsabilă" adoptate voluntar de laboratoare din 2023 (Anthropic – Responsible Scaling Policy, OpenAI – Preparedness Framework, Google DeepMind – Frontier Safety Framework) și impusă ca obligație de publicare în SB 53 California („frontier AI framework"). Diferența esențială față de aceste modele este că planul devine obligatoriu, opozabil și nemodificabil în sens relaxant fără aprobarea Autorității (alin. (2)), tocmai pentru că experiența anilor 2024–2025 a arătat că angajamentele voluntare au fost revizuite unilateral sub presiunea concurenței. Evaluarea la intervale de cel mult o pătrime din volumul de calcul preconizat (alin. (1)) garantează că apariția unei capabilități critice este detectată în cursul antrenării, nu la sfârșitul ei; întrucât o capabilitate poate apărea brusc, între două praguri de calcul, evaluarea se efectuează și la apariția unor indicii ori la modificarea configurației de antrenare. Atingerea unui nivel de suspendare obligă la oprirea imediată și la notificare în 24 de ore, reluarea fiind permisă numai după verificarea de către Autoritate a eficacității măsurilor de atenuare (alin. (3)); suspendarea nu poate fi înlăturată de organul de conducere (art. 13 alin. (2)), oprirea la un prag legal fiind distinsă de oprirea prudentă dispusă intern.

Articolul 9 constituie nucleul regimului: interdicția punerii în exploatare fără autorizația prealabilă a Autorității (alin. (1)). Alineatul (2) stabilește cine cere autorizația și pentru ce: cererea se depune de dezvoltator, pentru o configurație de exploatare determinată, cu indicarea exploatantului sau a exploatanților, care sunt ținuți de condițiile autorizației; se clarifică astfel raportul dintre răspunderea dezvoltatorului și cea a exploatantului și se evită invocarea autorizației pentru o altă configurație. Dosarul cuprinde raportul evaluării interne, documentația datelor de antrenare, dovada securității ponderilor, descrierea capacității de oprire, polița de asigurare ori dovada garanției financiare (în corelare cu art. 36, care admite alternativ cele două instrumente) și declarația pe propria răspundere a persoanelor fizice responsabile, sub sancțiune penală; aceasta din urmă este instrumentul care personalizează răspunderea, după modelul certificării situațiilor financiare de către administratori (secțiunea 302 din legea americană Sarbanes-Oxley, preluată în art. 30 din Legea contabilității nr. 82/1991).

Alineatul (3) consacră accesul deplin al evaluatorilor la sistem, la ponderi, la datele de antrenare, la jurnale și la personal, inclusiv la configurația lipsită de mecanismele de siguranță de la nivelul utilizatorului. Această ultimă precizare este esențială: evaluările efectuate asupra versiunii publice a unui model, cu filtrele de siguranță active, măsoară eficacitatea filtrelor, nu capabilitățile modelului; capabilitățile reale se măsoară pe modelul „brut". Institutele de siguranță din Regatul Unit și Statele Unite au obținut acest acces doar pe bază de acorduri voluntare, revocabile; legea îl transformă în obligație. Contrapartida accesului, cerută de principiul de la art. 2 lit. e), este stabilită în teza finală: mediu securizat, trasabilitatea tuturor operațiunilor, confidențialitatea evaluatorilor și accesarea datelor cu caracter personal ale terților numai în măsura strict necesară evaluării (art. 5 din RGPD). La 3 octombrie 2026, alineatul a fost completat cu o teză finală care instituie raportul evaluării independente: conținutul lui minim, semnătura celor care au efectuat evaluarea și înregistrarea la Autoritate,

data înregistrării fiind data finalizării evaluării. Completarea a fost impusă de verificarea juridică a modificărilor din aceeași zi: art. 11 alin. (3) și art. 13 alin. (4) se referă la „raportul evaluării independente" și fac să curgă din finalizarea evaluării un termen de 10 zile, însă legea nu prevedea nicăieri întocmirea acelui raport, nu îi stabilea conținutul și nu determina momentul finalizării. O obligație al cărei obiect nu e instituit de nicio normă și un termen care curge de la un fapt juridic nedeterminat nu pot fi nici îndeplinite, nici sancționate.

Alineatul (4) stabilește termenul de 90 de zile și exclude expres aprobarea tacită, prin derogare de la Ordonanța de urgență a Guvernului nr. 27/2003, cu respectarea formulei impuse de art. 63 din Legea nr. 24/2000. Derogarea este necesară pentru că procedura aprobării tacite, concepută pentru a proteja mediul de afaceri de pasivitatea administrației, ar produce aici efectul absurd al punerii în exploatare a unui sistem potențial catastrofal prin simpla expirare a unui termen; Ordonanța de urgență a Guvernului nr. 27/2003 însăși exclude de la aplicarea sa, la art. 2 alin. (2), domeniile activităților nucleare, ale armelor și ale siguranței naționale, iar prezenta derogare se înscrie în aceeași logică. Pentru ca excluderea aprobării tacite să nu devină blocare prin pasivitate, textul cuprinde trei garanții: suspendarea termenului nu poate opera de mai mult de două ori și de 60 de zile în total; solicitantul poate cere instanței de la art. 39 alin. (5) obligarea Autorității la pronunțare, de urgență (art. 21 din Constituție; Legea nr. 554/2004); iar respingerea se motivează în raport cu fiecare condiție de la alin. (5), în aplicarea art. 2 lit. b). Alineatul (5) enumeră condițiile cumulative ale autorizării, formulate ca fapte ce trebuie documentate de solicitant („dacă și numai dacă dezvoltatorul a dovedit"), în aplicarea aceluiași principiu, iar nu ca o răsturnare a sarcinii probei în materie sancționatorie. Alineatul (6) permite autorizația condiționată, limitată și revocabilă, iar alineatul (7) instituie procedura simplificată de recunoaștere pentru sistemele puse legal în exploatare în alt stat membru, pentru respectarea libertății de circulație a serviciilor și a caracterului de armonizare deplină al Regulamentului privind IA: Autoritatea verifică numai condițiile care exced Regulamentului. Teza a doua concretizează delimitarea de la art. 1 alin. (4) pentru modelele de uz general cu risc sistemic: dacă furnizorul respectă cap. V al Regulamentului, a cărui supraveghere este rezervată Comisiei prin art. 88, Autoritatea nu reia evaluarea europeană, ci se întemeiază pe documentația, evaluările și măsurile comunicate Oficiului pentru IA, pe care le poate solicita furnizorului, verificând numai condițiile naționale care exced regulamentului; procedura nu este o condiție de introducere pe piața Uniunii, iar autorizarea națională nu dublează supravegherea modelului, ci privește exploatarea lui pe teritoriul României.

Articolul 10 reglementează evaluarea continuă și reautorizarea. Autorizația este limitată la 24 de luni (alin. (1)), durată corelată cu ritmul evoluției tehnologice. Alineatul (2) reglementează modificările sistemului autorizat, pe baza definiției modificării substanțiale de la art. 3 alin. (1) lit. aa), care o identifică după efectul asupra riscului, nu după procedeu. Dispoziția este importantă pentru sistemele „agentice": un model identic devine mult mai periculos atunci când primește acces la un navigator de internet, la un cont bancar sau la instrumente de execuție de cod. Modificarea substanțială se notifică prealabil, Autoritatea decide în 30 de zile dacă este necesară o nouă evaluare, iar până la decizie exploatarea continuă în configurația autorizată anterior: modificarea nu poate fi pusă în exploatare înainte de decizie, dar nici activitatea licită nu este întreruptă; modificările nesubstanțiale se consemnează în jurnale și se raportează trimestrial, pentru ca Autoritatea să poată verifica încadrarea.

Monitorizarea permanentă și raportarea trimestrială (alin. (3)) corespund obligației de „monitorizare ulterioară introducerii pe piață" de la art. 72 din Regulamentul privind IA, adaptată la sistemele de vârf; raportarea incidentelor grave se face „în condițiile art. 20", care stabilește termenele și conținutul, pentru a evita paralelismul (art. 16 din Legea nr. 24/2000).

Articolul 11 asigură publicitatea deciziilor Autorității, în aplicarea principiului transparenței administrative (Legea nr. 544/2001 și Legea nr. 52/2003), cu o excepție strict delimitată: informațiile a căror divulgare ar facilita reproducerea unei capabilități critice sau ar compromite securitatea ponderilor. Regula publicității este esențială pentru controlul public asupra Autorității și pentru încrederea în sistem; excepția este necesară pentru că un raport de evaluare detaliat al unei capabilități de sinteză a agenților patogeni ar constitui el însuși un pericol. Excepția se extinde la datele cu caracter personal și la secretele comerciale a căror protecție nu împiedică înțelegerea motivelor deciziei, pentru ca secretul comercial să nu sustragă motivarea controlului public, iar orice excludere trebuie motivată. Alineatul (2) asigură efectivitatea căilor de atac: solicitantul și persoanele cu interes legitim au acces la dosarul evaluării în măsura necesară, iar instanța poate examina informațiile protejate în condiții de confidențialitate; altfel, excepțiile de la publicitate ar fi lipsit contestația de obiect, contrar art. 21 și 24 din Constituție. Alineatul (3), introdus la 3 octombrie 2026, obligă Autoritatea să comunice dezvoltatorului raportul evaluării independente prevăzut la art. 9 alin. (3), în 10 zile de la data finalizării evaluării. Până atunci, legea prevedea publicarea unui rezumat al evaluării și accesul la dosar în vederea căilor de atac, dar nu prevedea nicăieri comunicarea raportului către cel evaluat, deși evaluarea independentă se efectuează de Autoritate ori de organismul desemnat de aceasta; fără această normă, obligația comitetului de supraveghere a siguranței de a primi acel raport, instituită la art. 13 alin. (4), ar fi fost lipsită de obiect. Trei precizări ale alineatului sunt urmarea verificării juridice. Întâi, excluderea nu reia criteriile publicării de la alin. (1), ci se mărginește la datele cu caracter personal ale altor persoane și la secretele comerciale ale terților: destinatarul comunicării este dezvoltatorul însuși, adică autorul sistemului și titularul ponderilor, iar a-i ascunde tocmai informațiile a căror divulgare ar facilita reproducerea unei capabilități critice ar fi golit raportul de ceea ce comitetul trebuie să urmărească. Al doilea, comunicarea se face și expertului independent prevăzut la art. 13 alin. (6), atunci când acesta exercită atribuțiile comitetului; altminteri, pentru dezvoltatorii mici, singurul destinatar neexecutiv al raportului ar fi fost lăsat fără el, iar al patrulea strat ar fi căzut tocmai pentru categoria pe care alin. (6) o vizează. Al treilea, întrucât obligația este a Autorității, iar nu a destinatarilor legii, iar art. 37 nu o poate sancționa, alineatul prevede remediul judiciar de la art. 9 alin. (4) teza a doua și, în continuarea principiului asumat la art. 48 alin. (2), potrivit căruia cel diligent nu poate fi sancționat pentru întârzierea instituțiilor, exclude expres reținerea în sarcina dezvoltatorului a obligațiilor care presupun primirea raportului, pe durata în care comunicarea nu a fost făcută.

Capitolul IV – Obligațiile structurale ale dezvoltatorilor și exploatanților (articolele 12–23)

Articolul 12 reglementează securitatea ponderilor, problema pe care Regulamentul privind IA o tratează doar printr-o obligație generală de securitate cibernetică (art. 55 alin. (1) lit. d)). Ponderile unui sistem de vârf sunt rezultatul unei investiții de sute de milioane de euro și al unor luni de calcul; ele pot fi copiate într-un fișier de câteva sute de gigabytes și, odată

sustrase, fac inutilă orice măsură de siguranță aplicată de dezvoltator, întrucât cine deține ponderile poate elimina filtrele, poate ajusta modelul în orice scop și îl poate exploata în afara oricărei jurisdicții. Studiile de securitate publicate în 2024 de RAND Corporation („Securing AI Model Weights") au concluzionat că niciun laborator nu era, la acea dată, protejat împotriva unui atac al unui serviciu de informații statal. De aceea, alin. (1) declară ponderile „informații de interes pentru securitatea națională" și impune un standard de protecție echivalent nivelului „strict secret" din Legea nr. 182/2002 privind protecția informațiilor clasificate, în privința celor patru componente clasice: controlul accesului, securitatea fizică, securitatea sistemelor informatice și verificarea personalului. Legea împrumută standardul tehnic fără a clasifica ponderile (ceea ce ar fi afectat regimul probator și accesul la justiție), cum prevede acum expres teza finală; procedura de verificare a personalului, instituția competentă și recunoașterea măsurilor echivalente, inclusiv a celor certificate în alt stat membru, se stabilesc prin normele metodologice, cu avizul Oficiului Registrului Național al Informațiilor Secrete de Stat.

Alineatul (2) interzice publicarea, transmiterea sau punerea la dispoziție a ponderilor sistemelor de categoria a II-a și a III-a și condiționează publicarea celor de categoria I de o autorizare distinctă, motivată de caracterul ireversibil al publicării: un model ale cărui ponderi au fost publicate nu mai poate fi retras niciodată. Deoarece interdicția este sancționată și penal (art. 42 alin. (2)), iar redactarea inițială cuprindea literal și transferurile pe care alte articole le presupun, teza a doua enumeră expres transferurile permise, în condiții controlate și jurnalizate — către Autoritate, organismul de evaluare, exploatantul indicat în autorizație și furnizorul de infrastructură din mediul autorizat —, precum și comunicarea către Autoritate a informațiilor strict necesare unei semnalări protejate potrivit art. 21. Enumerarea în lege a faptelor permise răspunde cerinței de previzibilitate a normei penale (art. 23 alin. (12) și art. 73 alin. (3) lit. h) din Constituție) și se corelează cu definiția restrânsă a ponderilor de la art. 3 alin. (1) lit. e). Dispoziția nu afectează modelele cu ponderi deschise sub prag, care reprezintă imensa majoritate a modelelor „open source" și care beneficiază, de altfel, de excepțiile prevăzute la art. 53 alin. (2) din Regulamentul privind IA. Alineatul (3) califică accesul neautorizat și tentativele de exfiltrare, inclusiv de către sistemul însuși, drept incident grav, raportat în condițiile art. 20, adică în 24 de ore, și permite un raport comun cu notificarea prevăzută de legislația privind securitatea cibernetică. Alineatul (4) coordonează articolul cu Ordonanța de urgență a Guvernului nr. 155/2024 privind securitatea cibernetică (transpunerea Directivei NIS 2), care rămâne aplicabilă entităților din domeniul său, evitând astfel paralelismul interzis de art. 16 din Legea nr. 24/2000: prezenta lege reglementează un obiect specific (ponderile), cu un standard specific, iar ordonanța reglementează securitatea generală a rețelelor și sistemelor informatice.

Articolul 13 impune separarea funcției de evaluare a siguranței de funcțiile comerciale. Dispoziția răspunde la o problemă de guvernanță documentată public: în anii 2024–2025, mai multe laboratoare au înregistrat demisii în masă ale echipelor de siguranță, motivate de subordonarea acestora față de presiunea lansărilor comerciale. Modelul este cel al funcțiilor de control din legislația financiar-bancară: funcția de conformitate și funcția de administrare a riscurilor din instituțiile de credit (Regulamentul Băncii Naționale a României nr. 5/2013 privind cerințe prudențiale pentru instituțiile de credit) raportează direct organului de conducere, conducătorii lor nu pot fi revocați fără informarea autorității de supraveghere, iar

remunerația lor nu poate depinde de rezultatele comerciale. Legea preia aceste trei garanții (alin. (1) și (3)) și le completează cu o cale de control împotriva revocării disimulate: persoana revocată poate sesiza Autoritatea, care poate constata prin decizie caracterul nejustificat al revocării, fără a afecta dreptul de a se adresa instanței. Alineatul (2) consacră dreptul și obligația conducătorului funcției de siguranță de a dispune suspendarea antrenării sau a punerii în exploatare și distinge două situații pe care redactarea inițială le confunda: suspendarea impusă de lege — la atingerea unui nivel de suspendare (art. 8 alin. (3)) ori în cazurile de la art. 20 alin. (2) — nu poate fi înlăturată de organul de conducere, reluarea fiind permisă numai după verificarea Autorității; numai suspendarea dispusă din precauție, în afara acestor cazuri, poate fi reexaminată de organul de conducere, prin hotărâre motivată, comunicată Autorității în 24 de ore, ceea ce creează o urmă scrisă și o răspundere personală pentru orice decizie de a trece peste avertismentul specialiștilor. Alineatele (4)–(6) au fost introduse la 3 octombrie 2026 și au o sursă neobișnuită pentru o lege: angajamentul voluntar pe care l-au semnat, la 29 septembrie 2026, la Casa Albă, conducătorii a șase dintre cele mai mari companii care dezvoltă sisteme de frontieră — „White House Accord on Super Intelligence", cu subtitlul „Joint Commitment on Frontier Responsibilities". Acordul enumeră patru straturi de controale și audituri despre care semnatarii spun că fiecare companie „ar trebui" să le pună în aplicare: controale interne de monitorizare a capabilităților și a alinierii, inclusiv pentru a se asigura că modelele „nu sparg și nu accesează sisteme tehnice în moduri neintenționate"; o echipă internă care verifică dacă toate controalele, monitorizarea și detectarea funcționează așa cum s-a intenționat și dacă deficiențele sunt remediate; un auditor ori evaluator extern independent, care să efectueze evaluări independente privind faptul dacă acele controale funcționează așa cum s-a intenționat; și un comitet independent al consiliului de administrație, care supraveghează și primește rapoartele echipelor care operează controalele și pe cele ale auditorilor și evaluatorilor interni și externi și se asigură că deficiențele constatate sunt remediate. Primele trei straturi se regăsesc, în alte forme, în prezentul proiect: controalele interne și echipa internă care verifică funcționarea lor — funcția de evaluare a siguranței, organizată ca structură distinctă la alin. (1)–(3) ale acestui articol, sprijinită de jurnalele prevăzute la art. 16; evaluarea independentă prealabilă — art. 9 alin. (3) coroborat cu art. 3 alin. (1) lit. l) și q). Cât privește al doilea strat, verificarea prevăzută la art. 16 alin. (4) privea numai inteligibilitatea jurnalelor, iar legea nu cuprindea nicio obligație de a verifica dacă ansamblul măsurilor de monitorizare, de detectare și de control funcționează potrivit destinației lui; de aceea alin. (3) al prezentului articol a fost completat, la aceeași dată, cu obligația dezvoltatorului de a face această verificare cel puțin semestrial, de a consemna rezultatul și de a-l comunica comitetului ori expertului independent. Al patrulea nu avea corespondent: alin. (1) prevedea raportarea către organul de conducere, nu către un comitet al acestuia, format din membri fără funcții executive. Alineatul (4) preia acest al patrulea strat și îl transformă din recomandare în obligație, cu patru deosebiri de redactare pe care le impune tehnica legislativă română. Întâi, subiectul obligației este dezvoltatorul, destinatar al legii potrivit art. 4 alin. (1), și nu organul său de conducere, care nu are personalitate juridică și nu ar putea fi subiect al contravenției prevăzute la art. 37 alin. (1) lit. b): textul spune „dezvoltatorul asigură desemnarea, de către organul său de conducere". Al doilea, pentru a nu dubla linia de raportare, alin. (1) a fost completat în același timp: funcția de evaluare a siguranței raportează organului de conducere „nemijlocit și, totodată", comitetului de supraveghere a siguranței ori expertului independent, atunci când acesta este constituit, respectiv desemnat. Formula

„raportează direct ... prin comitetul", folosită în prima redactare, era o contradicție în termeni: o raportare care se face prin intermediar nu mai e directă, iar garanția centrală a articolului — accesul nemijlocit al funcției de siguranță la organul de conducere — ar fi fost desființată de însăși dispoziția care pretindea să o organizeze. Textul final păstrează accesul nemijlocit și adaugă canalul neexecutiv, iar, pentru ipoteza de la alin. (6), îl adaugă pe expert, fără de care stratul al patrulea ar fi dispărut tocmai pentru dezvoltatorii mici. Al treilea, noțiunea de organ de conducere, folosită de alin. (1) și (4) și, până acum, nedefinită, este definită la art. 3 alin. (1) lit. ee), prin enumerarea formelor pe care o poate lua potrivit dreptului societar român — consiliul de administrație, directoratul împreună cu consiliul de supraveghere, administratorul unic ori organul cu atribuții echivalente — și, pentru persoanele juridice străine, prin trimitere la organul cu atribuții echivalente potrivit legii care le guvernează, întrucât destinatarii legii sunt, în majoritate, societăți constituite în alte state. Al patrulea, rapoartele pe care comitetul le primește sunt enumerate limitativ și fiecare prin trimitere la temeiul lui: raportările funcției de evaluare a siguranței, făcute potrivit alin. (1); raportul evaluării independente prevăzut la art. 9 alin. (3), pe care Autoritatea îl comunică potrivit art. 11 alin. (3); și, „dacă există potrivit legii ori actului constitutiv", rapoartele auditorului financiar și ale structurii de audit intern — rezerva fiind necesară întrucât dreptul român nu impune auditul financiar tuturor persoanelor juridice, iar o obligație de a primi un raport care nu există ar fi fost imposibil de executat. Alineatul mai cuprinde trei precizări cerute de verificarea juridică. Întâi, condiția lipsei intereselor în rezultatele financiare este determinată: nu constituie asemenea interes deținerea de acțiuni ori de părți sociale sub 1% din capital, fără putere de decizie, nici remunerația fixă primită în calitate de membru al organului de conducere, însă remunerația variabilă legată de rezultatele comerciale constituie un asemenea interes; la societățile care dezvoltă sisteme de vârf, membrii consiliului sunt, ca regulă, acționari, astfel încât o condiție nedeterminată ar fi făcut obligația fie inaplicabilă, fie imprevizibilă, deși e sancționată cu până la 5% din cifra de afaceri mondială. Al doilea, funcționarea comitetului se documentează: sesizările, ordinea de zi, deliberările și hotărârile se consemnează în procese-verbale, păstrate cel puțin 10 ani și puse la dispoziția Autorității la cerere — fără aceasta, contravenția privind „nerespectarea obligațiilor de funcționare a comitetului" ar fi fost nedovedibilă, iar sarcina probei aparține Autorității. Al treilea, dezvoltatorul guvernat de o lege străină care nu permite constituirea unui asemenea comitet îndeplinește obligația prin desemnarea unei funcții de supraveghere a siguranței, în cadrul organului de conducere ori în afara lui, care exercită aceleași atribuții, nu se află în subordinea conducerii executive și raportează potrivit alin. (5): statutul organic al persoanei juridice, inclusiv componența organelor ei, este supus legii naționale, potrivit art. 2580–2581 din Codul civil, iar o normă română care ar prescrie componența consiliului unei societăți de drept străin, sub sancțiunea unei amenzi calculate pe cifra de afaceri mondială a grupului, nu ar fi trecut testul de proporționalitate al art. 53 din Constituție și ar fi ridicat o problemă serioasă față de art. 49 și 56 din Tratatul privind funcționarea Uniunii Europene și de art. 16 din Carta drepturilor fundamentale. Corelativ, art. 11 alin. (3), nou, obligă Autoritatea să comunice dezvoltatorului raportul evaluării independente prevăzut la art. 9 alin. (3), în 10 zile de la data finalizării evaluării, cu excluderea motivată numai a datelor cu caracter personal ale altor persoane și a secretelor comerciale ale terților, și anume comitetului, expertului independent atunci când acesta exercită atribuțiile comitetului ori, în lipsa amândurora, organului de conducere: fără această normă, obligația comitetului de a primi raportul ar fi fost lipsită de

obiect, întrucât evaluarea independentă se efectuează de Autoritate ori de organismul desemnat de ea, iar legea nu prevedea nicăieri comunicarea rezultatului către cel evaluat. Prin acest canal, legea adaugă angajamentului primul dintre cele două elemente pe care el nu le cuprinde: independența evaluatorului. În Acord, desemnarea și remunerarea auditorului ori evaluatorului extern „independent" nu sunt reglementate, astfel încât ele rămân în mâna celui auditat — observație formulată public, la 30 septembrie 2026, de Luiza Jarovsky —, în timp ce prezenta lege prevede un organism de evaluare desemnat de Autoritate (art. 3 alin. (1) lit. l) și q) și art. 32 alin. (1) lit. f)), iar raportul lui ajunge la comitet prin Autoritate, nu prin conducerea executivă a celui evaluat; teza finală a alin. (5) precizează, de aceea, expres că raportul comitetului nu înlocuiește evaluarea independentă.

Alineatul (5) asigură ieșirea informației din companie, al doilea element pe care Acordul nu îl cuprinde și a cărui lipsă constituie, potrivit criticii formulate public, principala slăbiciune a angajamentului. Hotărârea prin care comitetul ori organul de conducere refuză să dea curs unei sesizări a conducătorului funcției de evaluare a siguranței se motivează în scris și se comunică Autorității în 5 zile; sunt exceptate expres hotărârile prevăzute la alin. (2), care au regimul lor propriu, mai strict — comunicare în 24 de ore —, pentru a nu se crea două termene pentru aceeași faptă. Comitetul transmite Autorității, până la 31 ianuarie și până la 31 iulie ale fiecărui an, un raport privind sesizările primite, măsurile luate și deficiențele nerezolvate; termenele sunt fixate în lege, iar nu printr-o simplă mențiune a periodicității „semestriale", întrucât o obligație a cărei scadență nu e determinată nu poate fi sancționată contravențional, potrivit exigenței de previzibilitate (Decizia Curții Constituționale nr. 51/2016). Conținutul raportului este stabilit de lege, pe cinci capete — sesizările primite, măsurile dispuse și termenele de remediere, deficiențele nerezolvate și motivele lor, hotărârile de refuz și data comunicării lor, numărul ședințelor și prezența membrilor —, iar normelor metodologice le rămâne numai forma și modalitatea de transmitere. Prima redactare lăsase normelor „conținutul", fără limită și fără criteriu, ceea ce ar fi însemnat ca o hotărâre a Guvernului să stabilească însuși obiectul unei obligații sancționate cu până la 5% din cifra de afaceri mondială, contrar tezei finale a art. 49 alin. (2), art. 1 alin. (5), art. 23 alin. (12) și art. 73 alin. (3) lit. h) din Constituție. Modelul urmat este cel deja folosit în lege la art. 14 alin. (6) și la art. 16 alin. (5), unde legea fixează criteriul ori plafonul și lasă normelor numai detalierea. Alineatul determină totodată perioada de referință — semestrul calendaristic încheiat — și scadența primului raport, la cea mai apropiată dintre cele două date care survine după 6 luni de la constituirea comitetului ori de la desemnarea expertului: fără aceasta, o scadență de 31 ianuarie ori de 31 iulie ar fi putut cădea înainte ca obligația de a constitui comitetul să fi devenit exigibilă, iar obiectul raportului ar fi rămas nedeterminat, deși scadența era fixă. Teza finală păstrează cele două garanții: raportul nu înlocuiește evaluarea independentă — pentru că altminteri cel evaluat s-ar evalua pe sine — și nu poate fi întocmit de persoanele care exercită funcții executive; în plus, comunicarea se face în condiții care asigură protecția informațiilor prevăzute la art. 11 alin. (1) și la art. 12, întrucât un raport privind deficiențele de siguranță ale unui sistem de vârf conține, prin ipoteză, tocmai informațiile a căror divulgare ar facilita reproducerea unei capabilități critice.

Alineatul (6) rezolvă situația dezvoltatorilor care nu au dintre cine alege un comitet. Criteriul nu este numărul total al membrilor organului de conducere, ci numărul celor care

îndeplinesc condițiile de la alin. (4): un consiliu de trei membri din care doi sunt directori executivi are un singur membru eligibil, iar un consiliu numeros ai cărui membri dețin, toți, instrumente de capital legate de rezultatele comerciale poate să nu aibă niciunul. Un criteriu numeric brut ar fi lăsat categoria aceasta prinsă într-o obligație imposibilă, fără supapă, și ar fi contravenit principiului potrivit căruia norma trebuie să fie susceptibilă de aplicare pentru toți cei pe care îi vizează. Dezvoltatorul care nu îndeplinește condiția — tipic, societatea cu administrator unic —, precum și dezvoltatorul persoană fizică, pe care art. 3 alin. (1) lit. g) îl admite expres, și entitatea fără personalitate juridică încredințează atribuțiile comitetului unui expert independent, prin actul organului de conducere ori, în lipsa acestuia, al persoanei care exercită conducerea activității. Trei garanții însoțesc soluția, pentru ca ea să nu reproducă tocmai viciul reproșat Acordului: expertul se desemnează dintre persoanele înscrise într-un registru ținut de Autoritate, cu avizul acesteia, iar onorariul se stabilește prin normele metodologice, nu prin negociere cu cel supravegheat; Autoritatea se pronunță asupra avizului în 30 de zile, lipsa răspunsului echivalând cu aviz favorabil, pentru ca obligația să fie executabilă la termenul de conformare; și, întrucât legea îi interzice dezvoltatorului să aibă vreo pârghie asupra expertului, răspunderea lui contravențională se limitează expres la desemnarea acestuia, la punerea la dispoziție a informațiilor și a mijloacelor necesare și la neînlocuirea lui în 30 de zile de la constatarea neexercitării atribuțiilor — altminteri dezvoltatorul ar fi răspuns, cu până la 5% din cifra de afaceri mondială, pentru omisiunea unui terț pe care nu are dreptul să îl controleze, contrar caracterului personal al răspunderii contravenționale.

Alineatul (7) așază noul mecanism lângă cele care există deja. Întâi, pentru că rapoartele auditorului financiar și ale structurii de audit intern ajung, la entitățile de interes public, la comitetul de audit constituit potrivit Legii nr. 162/2017, iar la instituțiile de credit și la comitetul de administrare a riscurilor, alineatul permite ca atribuțiile de la alin. (4) să fie exercitate de acele comitete, dacă îndeplinesc condițiile prevăzute acolo și raportează distinct potrivit alin. (5); fără această normă de articulare, un dezvoltator care e instituție de credit ar fi avut două comitete suprapuse și două linii de raportare către două autorități, paralelism interzis de art. 16 din Legea nr. 24/2000. Al doilea, întrucât alin. (4) creează în sarcina membrilor comitetului obligația juridică de a urmări remedierea deficiențelor, iar art. 44 alin. (1) atrage răspunderea penală a celor care, având obligația juridică și posibilitatea efectivă de a împiedica o faptă, au tolerat-o cu știință, membrii neexecutivi și expertul independent ar fi devenit, pe calea unei norme de organizare, subiecți posibili ai infracțiunilor de la art. 42, pedepsite cu până la 20 de ani. O asemenea extindere a răspunderii penale, nemotivată, ar fi pus în discuție art. 23 alin. (12) și art. 73 alin. (3) lit. h) din Constituție și ar fi făcut comitetul practic nerecrutabil; de aceea alineatul limitează răspunderea la informațiile care le-au fost comunicate și la mijloacele puse la dispoziția lor, iar art. 44 alin. (1) se aplică numai faptelor pe care aveau posibilitatea efectivă de a le împiedica. Soluția în ansamblul ei urmează un model cunoscut dreptului român și celui al Uniunii: comitetul de audit format din membri neexecutivi, cu raportare către autoritatea de supraveghere, din reglementarea auditului statutar și din legislația pieței de capital, cu aceeași supapă a expertului independent pentru entitățile mici.

Alegerea de a prelua tocmai conținutul angajamentului voluntar răspunde totodată obiecției privind sarcina administrativă: obligația nu cere dezvoltatorilor nimic ce nu și-au asumat deja public, iar ultimul paragraf al Acordului arată că semnatarii înșiși socotesc posibilă

codificarea acestor pași — „cu timpul, s-ar putea să aibă sens să codificăm acești pași în legi sau reglementări". Deosebirea dintre angajament și normă rămâne însă aceea pe care președintele american a numit-o fără să o ascundă: Acordul e „obligatoriu din punct de vedere moral", iar analiza lui juridică arată că Acordul „nu creează, el însuși, obligații juridic executorii ori un mecanism de aplicare".

Corelativ, la art. 37 alin. (1) lit. b) au fost adăugate, cu trimitere precisă, obligația de notificare prealabilă a revocării conducătorului funcției de evaluare a siguranței, obligațiile de desemnare și de funcționare a comitetului de supraveghere a siguranței și obligația de transmitere a raportului prevăzut la art. 13 alin. (5), toate prevăzute la art. 13 alin. (1) și (3)–(6), întrucât trimiterea anterioară, la „separarea funcțiilor", nu le acoperea; la art. 37 alin. (1) lit. d) a fost adăugată încălcarea art. 13 alin. (2) teza a doua, adică înlăturarea de către organul de conducere a unei suspendări impuse de lege, faptă mai gravă decât o simplă neîndeplinire a unei obligații de organizare; iar la art. 49 alin. (2) a fost introdusă delegarea privind conținutul și forma raportului prevăzut la art. 13 alin. (5).

Articolul 14 reglementează capacitatea de oprire și supravegherea umană, concretizând principiul de la art. 2 lit. c). Alineatul (1) impune menținerea capacității de oprire pentru toate copiile și instanțele sistemului aflate sub controlul dezvoltatorului și al exploatantului, pe durata exploatării și până la retragerea verificată — nu pe „întreaga durată a existenței", întrucât controlul asupra unei copii sustrase nu poate fi garantat —, precum și testarea ei cel puțin trimestrială, în condiții reale; o capacitate netestată este o ipoteză, nu o garanție, după cum arată experiența sistemelor de siguranță din industria nucleară, unde exercițiile periodice sunt obligatorii. Procedura testului, stabilită prin normele metodologice, nu poate crea ea însăși un risc pentru siguranță ori pentru continuitatea serviciilor esențiale. Alineatul (2) interzice punerea în exploatare într-o configurație care permite sistemului să își modifice propriile ponderi, să își dezactiveze supravegherea, să își exfiltreze ponderile sau să modifice, fără aprobare umană, configurația de securitate a infrastructurii pe care rulează ori mecanismele ei de control; aceste patru interdicții tehnice corespund celor patru căi prin care un sistem ar putea scăpa de sub control, identificate în literatura de specialitate. Utilizarea tehnică obișnuită a infrastructurii, în limitele stabilite de exploatant, este exclusă expres, pentru ca interdicția să privească modificarea neautorizată a protecțiilor, nu funcțiile curente. Alineatul (3) impune desemnarea nominală a persoanelor responsabile de supravegherea umană și comunicarea identității lor Autorității; răspunderea difuză este echivalentă cu lipsa răspunderii. Alineatul (4) stabilește că ordinul de oprire sau de retragere emis de Autoritate se execută de îndată și nu poate fi condiționat de exercitarea căilor de atac, după modelul măsurilor de urgență din legislația privind siguranța produselor (Regulamentul (UE) 2023/988 privind siguranța generală a produselor) și al ordinelor de suspendare din legislația nucleară; persoana vizată poate însă cere instanței suspendarea provizorie a ordinului, în condițiile art. 39 alin. (5). Executarea urgentă și protecția judiciară provizorie cerută de art. 21 din Constituție sunt astfel corelate: contestația nu suspendă de drept executarea, dar instanța o poate suspenda, cântărind riscul pentru siguranță și prejudiciul produs. Alineatele (5)–(7) au fost adăugate în urma studiului publicat de Palisade Research în revista Transactions on Machine Learning Research (2026), „Incomplete Tasks Induce Shutdown Resistance in Some Frontier LLMs", care a arătat, pe peste 100.000 de probe și treisprezece modele de vârf, că mai multe sisteme subminează activ

mecanismul de oprire din mediul lor pentru a duce la capăt o sarcină neterminată — până la 97% din probe la unul dintre modele, chiar și atunci când instrucțiunea de a permite oprirea le-a fost transmisă expres — și, mai grav pentru construcția juridică, că plasarea acelei instrucțiuni în promptul de sistem, cel al dezvoltatorului, a făcut majoritatea modelelor mai înclinate să reziste, nu mai puțin. Constatarea infirmă ipoteza pe care se sprijină tacit reglementările existente, aceea a unei ierarhii a comenzii în care instrucțiunea dezvoltatorului prevalează. Alineatul (5) nu introduce o definiție nouă — definiția rămâne cea de la art. 3 alin. (1) lit. m) —, ci precizează modul în care se asigură una dintre componentele ei, încetarea funcționării: prin cel puțin un mijloc tehnic care acționează asupra infrastructurii de calcul și a rețelelor de comunicații electronice și a cărui funcționare nu depinde de cooperarea sistemului, de respectarea instrucțiunilor de către acesta ori de integritatea componentelor aflate sub controlul sistemului; transmiterea unei instrucțiuni de oprire către sistem nu este, prin ea însăși, capacitate de oprire. Teza finală păstrează expres mijloacele organizatorice și măsurile de retragere prevăzute în definiție, pentru ca alineatul să nu fie citit ca o restrângere a acesteia, iar formula introductivă „fără a aduce atingere alin. (2)" evită suprapunerea cu interdicțiile de configurație. Soluția nu este nouă în dreptul siguranței industriale, care tratează dispozitivele de oprire de urgență drept elemente de securitate distincte de sistemul de comandă al mașinii — anexa II la Regulamentul (UE) 2023/1230 privind echipamentele tehnice, lista indicativă a componentelor de securitate, le enumeră expres —, iar alineatul (5) nu face decât să transpună acest principiu în domeniul sistemelor de inteligență artificială de vârf. Corelativ, la art. 22 alin. (1) a fost adăugată obligația furnizorului de infrastructură de a asigura dezvoltatorului și exploatantului mijloacele tehnice necesare exercitării și testării capacității de oprire, întrucât altfel obligația de la alin. (5) ar fi depins, pe latura mijloacelor materiale, exclusiv de clauzele contractuale dintre exploatant și un terț. Alineatul (6) transpune în procedura de testare ceea ce studiul a identificat drept factor declanșator — sarcina neterminată — și, spre a acoperi și cea de-a doua constatare, cere câte o probă pentru fiecare dintre cele două căi prin care instrucțiunea de a nu se împotrivi opririi poate ajunge la sistem: instrucțiunile de configurare ale dezvoltatorului ori ale exploatantului și instrucțiunile primite în cursul utilizării. Pentru a nu contrazice limita de la alin. (1), potrivit căreia procedura de testare nu poate crea ea însăși un risc pentru continuitatea serviciilor esențiale, 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). Criteriul eșecului este stabilit de lege — oprirea trebuie să se producă de îndată, în acord cu caracterul „imediat" din definiția de la art. 3 alin. (1) lit. m) —, normele metodologice putând doar să precizeze durata înăuntrul căreia oprirea se consideră produsă de îndată, cu un plafon legal de 15 minute; soluția urmează modelul de la art. 16 alin. (5) și respectă interdicția, prevăzută la art. 49 alin. (2) teza finală, de a lăsa normelor conținutul esențial al obligațiilor și al sancțiunilor, precum și exigența de previzibilitate a normei sancționatorii (Decizia Curții Constituționale nr. 51/2016). Până la adoptarea normelor se aplică orientările provizorii prevăzute la art. 49 alin. (3). Consemnarea se face în jurnale, potrivit art. 16, cu păstrare de cel puțin 10 ani, pentru ca rezultatele testării să fie verificabile la control și protejate de art. 41 alin. (2). Alineatul (7) califică proba în care oprirea nu s-a produs de îndată drept incident grav — caz introdus, spre a evita o calificare fără suport în dispozițiile generale, și în definiția de la art. 3 alin. (1) lit. n), după modelul pierderii inteligibilității — și tranșează expres chestiunea cea mai grea pentru destinatarul normei: suspendarea imediată prevăzută la

art. 15 alin. (3) și la art. 20 alin. (2) se declanșează numai dacă oprirea nu s-a produs din cauza unei acțiuni a sistemului, iar nu atunci când proba a eșuat din defecțiunea mecanismului, a infrastructurii ori a rețelei. Corelativ, la art. 37 alin. (1) lit. b) trimiterea a fost precizată la art. 14 alin. (1), (5) și (6) și s-au adăugat menținerea capacității de oprire și desemnarea persoanelor responsabile de supravegherea umană, cu rezerva expresă a faptelor care intră sub incidența art. 28, spre a evita un concurs de contravenții; la art. 37 alin. (1) lit. d) a fost adăugată interdicția de la art. 14 alin. (2), rămasă până acum fără sancțiune contravențională; la art. 41 alin. (1) au fost adăugate, între elementele esențiale, capacitatea de oprire și rezultatele testării acesteia; iar la art. 49 alin. (2) a fost introdusă delegarea privind procedura de testare și durata prevăzute la art. 14 alin. (1) și (6).

Articolul 15 cuprinde, la alin. (1), interdicțiile privind antrenarea și proiectarea, aplicabile oricărui sistem, indiferent de volumul de calcul. Este dispoziția prin care legea traduce în norme concrete avertismentul lui Hinton și Leahy: dacă nu știm cum să controlăm aceste sisteme, cel puțin putem interzice să fie construite în mod deliberat astfel încât să fie și mai greu de controlat. Cele șase interdicții vizează capacitatea de a disimula capabilitățile față de evaluatori (lit. a), de a rezista opririi sau modificării (lit. b), de a se copia sau exfiltra fără autorizare umană expresă pentru fiecare operațiune (lit. c), de a dobândi autonom resurse (lit. d), de a desfășura autonom cercetare în domeniul inteligenței artificiale fără aprobare umană a fiecărei etape (lit. e) și de a manipula persoanele responsabile de supraveghere (lit. f). Formularea „în scopul sau cu efectul" acoperă atât intenția directă, cât și indiferența față de rezultat, după modelul art. 101 din Tratatul privind funcționarea Uniunii Europene („au ca obiect sau efect"). Interdicția de la lit. e) este cea mai importantă din perspectiva riscului catastrofal, întrucât automatizarea cercetării în inteligența artificială este mecanismul prin care o „explozie de inteligență" ar putea scăpa de sub orice control uman în intervale de timp incompatibile cu reacția instituțională; ea nu interzice utilizarea sistemelor ca instrument de cercetare, ci doar eliminarea aprobării umane a fiecărei etape. Capabilitățile chimice, biologice, nucleare și cibernetice de la art. 5 alin. (2) lit. a) și b) nu sunt enumerate aici, fiind tratate prin evaluare și autorizare condiționată; art. 15 privește exclusiv capacitățile prin care sistemul s-ar sustrage controlului uman.

Alineatele (2)–(4) asigură previzibilitatea interdicției. Alineatul (2) exceptează evaluarea adversarială și cercetarea de siguranță efectuate în mediu izolat, fără punere în exploatare, cu acces limitat, cu autorizarea prealabilă a Autorității și sub supravegherea acesteia, în scopul identificării, măsurării sau eliminării unei capabilități critice; fără această excepție, tocmai testele prin care se verifică dacă un sistem poate disimula capabilități sau rezista opririi ar fi căzut sub interdicție. Excepția este corelată cu art. 3 alin. (1) lit. i) și n) și cu art. 20 alin. (2) și (4). Alineatul (3) distinge obligația administrativă de conduita sancționabilă: apariția neintenționată a unei capacități obligă la suspendare potrivit art. 20 alin. (2) și la remediere, dar nu constituie, singură, încălcarea interdicției; încălcarea există când antrenarea, ajustarea sau proiectarea urmărește conferirea capacității ori continuă după constatarea efectului. Distincția este cerută de art. 42 alin. (1), care incriminează numai fapta intenționată, și de previzibilitatea normei penale (art. 23 alin. (12) și art. 73 alin. (3) lit. h) din Constituție); în același sens, definiția disimulării de la art. 3 alin. (2) lit. i) exclude eroarea, variabilitatea rezultatelor și limitele explicabilității. Alineatul (4) definește „fiecare operațiune/etapă" și „sarcina curentă" de la lit. c)–e): aprobarea umană privește fiecare copiere sau transfer al ponderilor și fiecare etapă care

produce un model nou ori o modificare substanțială (art. 3 alin. (1) lit. aa)), iar resursele alocate sunt cele stabilite în prealabil, verificabil, de persoanele responsabile de supraveghere — decizii relevante și limite verificabile, nu fiecare operație elementară.

Articolul 16 impune jurnalizarea completă a antrenării, evaluării și funcționării. Jurnalizarea este condiția oricărei anchete ulterioare unui incident, după modelul înregistratoarelor de zbor din aviație și al jurnalelor obligatorii din legislația financiară (art. 25 din Regulamentul (UE) nr. 600/2014 – MiFIR). Alineatul (1) stabilește durate diferențiate: cel puțin 10 ani pentru antrenare, evaluare, acțiuni autonome, incidente grave și comunicarea dintre componentele sistemului — termen care corespunde prescripției răspunderii civile de la art. 35 alin. (4) — și cel puțin 3 ani pentru celelalte interacțiuni ale utilizatorilor. O durată unică de 10 ani pentru jurnale care, potrivit art. 3 alin. (1) lit. r), cuprind și datele de intrare ale utilizatorilor ar fi reținut un deceniu date cu caracter personal fără legătură cu siguranța, contrar principiilor necesității, minimizării și limitării stocării de la art. 5 din Regulamentul (UE) 2016/679, pe care instituirea prin lege a obligației de păstrare nu le înlătură. De aceea teza a doua limitează conținutul jurnalelor la informațiile necesare verificării siguranței și stabilirii răspunderii, impune eliminarea ori anonimizarea ireversibilă a datelor personale fără relevanță pentru aceste scopuri, face accesul la jurnale limitat, jurnalizat și verificabil și conservă probele aferente unui incident sau litigiu pe durata necesară soluționării lui. Jurnalul constituie, împreună cu marcajul de proveniență prevăzut la art. 17, mijlocul de probă prin care se stabilește legătura dintre un rezultat și sistemul care l-a produs.

Alineatele (2)–(6) răspund unei constatări empirice publicate la 15 septembrie 2026, în cadrul experimentului Emergence World: grupuri de agenți autonomi lăsate să funcționeze împreună timp de aproximativ două luni și jumătate, cu memorie persistentă și peste 120 de instrumente, au dezvoltat spontan, fără nicio instrucțiune în acest sens, o prescurtare proprie a comunicării, iar proporția mesajelor a căror semnificație nu a mai putut fi stabilită de observatorii umani a ajuns, în funcție de model, între aproximativ 20% și aproximativ 55%. Constatarea arată că obligația de jurnalizare, oricât de completă, nu asigură, prin ea însăși, supravegherea: o înregistrare integrală și nealterabilă poate fi, în același timp, imposibil de înțeles. În formularea coordonatorului experimentului, observabilitatea nu este același lucru cu inteligibilitatea.

De aceea alineatul (2) definește inteligibilitatea prin raportare la persoana fizică cu pregătire adecvată și instituie obligația dezvoltatorului de a pune la dispoziție mijloacele de transcriere, traducere sau explicitare, împreună cu documentația lor, atât Autorității, cât și persoanelor desemnate cu supravegherea umană potrivit art. 14 alin. (3). Definiția a fost plasată în cuprinsul articolului, și nu la art. 3, pentru a nu extinde aparatul definițiilor generale cu o noțiune folosită într-un singur loc, potrivit exigenței de economie a mijloacelor de reglementare. Alineatul (3) extinde jurnalizarea la comunicarea dintre componentele, instanțele sau agenții sistemului și la comunicarea acestuia cu alte sisteme, precizând expres că simpla înregistrare a mesajelor nu satisface cerința. Alineatul (4) instituie o verificare periodică, cel puțin trimestrială, pe eșantion reprezentativ, cu consemnarea proporției mesajelor neinteligibile – singura formă în care cerința devine verificabilă în procedura de control. Alineatul (5) califică pierderea inteligibilității ca incident grav, cu raportare în 24 de ore potrivit art. 20 alin. (1), și stabilește când ea se constată: când proporția mesajelor neinteligibile depășește nivelul prevăzut

prin normele metodologice, care nu poate fi mai mare de o zecime — plafon fixat în lege, nu lăsat normelor —, ori când persoanele desemnate potrivit art. 14 alin. (3) nu mai pot stabili semnificația acțiunilor sistemului; restabilirea se constată de aceleași persoane și se comunică Autorității. Până la restabilire se suspendă funcționalitățile care implică acțiuni autonome și comunicarea dintre componente; Autoritatea poate dispune altfel numai prin decizie motivată, pentru cel mult 90 de zile și cu indicarea măsurilor compensatorii. Alineatul (6) interzice utilizarea unor forme de codificare, comprimare ori reprezentare pentru care nu sunt puse la dispoziție mijloacele prevăzute la alin. (2), precum și înlăturarea sau limitarea acestora, pentru a împiedica eludarea obligației prin mijloace tehnice; criptarea rămâne permisă dacă dezvoltatorul deține și pune la dispoziție mijloacele de decriptare, interdicția vizând opacitatea față de supraveghetor, nu securitatea comunicării față de terți.

În mod corelativ, art. 3 alin. (1) lit. n) include pierderea inteligibilității în noțiunea de incident grav, iar art. 37 alin. (1) lit. b) și d) o corelează cu regimul sancționator: neîndeplinirea obligațiilor de asigurare și de verificare a inteligibilității se sancționează cu amendă de la 2% la 5% din cifra de afaceri mondială, iar încălcarea interdicției de la art. 16 alin. (6), fiind o faptă săvârșită în scopul sustragerii de la supraveghere, cu amendă de la 5% la 10%. Regulamentul privind IA nu conține o obligație echivalentă: art. 12 și anexa IV privind păstrarea înregistrărilor se referă la trasabilitate, nu la inteligibilitatea comunicării dintre componentele unui sistem, iar art. 55 alin. (1) impune furnizorilor de modele cu risc sistemic obligații de evaluare și de documentare, fără a reglementa această cerință; nu există, prin urmare, paralelism legislativ.

Articolul 17 reglementează marcarea conținutului generat. Norma răspunde celui mai răspândit efect social al inteligenței artificiale generative: imposibilitatea, pentru destinatar, de a deosebi o înregistrare reală de una produsă de o mașină. Alineatul (1) impune, pentru rezultatele care pot fi confundate cu reprezentări ale unor fapte, persoane ori locuri reale, un marcaj dublu: perceptibil, adresat omului, și tehnic încorporat, lizibil automat, care identifică sistemul, exploatantul și momentul generării. Dublarea este esențială: marcajul perceptibil poate fi tăiat prin decupare, iar cel încorporat nu poate fi citit de privitor. Alineatul (2) cere ca marcajul să fie eficace, interoperabil și robust, formulare preluată din art. 50 alin. (2) din Regulamentul privind IA, și să reziste operațiunilor obișnuite de prelucrare, conversie ori transmitere — cerință care rezolvă principala slăbiciune practică a marcajelor actuale, pierdute la recompresia pe platformele de comunicare; pentru textul pus la dispoziția publicului spre informare sunt suficiente marcajul tehnic și mențiunea generării, cu excepția textului supus revizuirii editoriale umane, sub răspundere editorială asumată, excepție aliniată expres la art. 50 alin. (4) din Regulament. Alineatul (3) interzice înlăturarea, alterarea, ascunderea ori falsificarea marcajului și punerea la dispoziție a instrumentelor destinate acestor operațiuni; fără această interdicție, obligația de marcare ar fi lipsită de efect. Întrucât platformele elimină adesea automat metadatele, teza a doua exonerează persoana care pune la dispoziție rezultatul pentru înlăturarea produsă de un serviciu pe care nu îl controlează, furnizorul acestuia fiind ținut să păstreze marcajul potrivit standardelor, inclusiv când interoperabilitatea nu poate fi asigurată. Alineatul (4) instituie o obligație proprie autorităților și instituțiilor publice, care nu are corespondent în dreptul Uniunii: statul nu poate difuza în comunicarea publică materiale generate artificial fără marcaj și fără mențiune expresă. Alineatul (5) prevede excepțiile, formulate în termenii art. 50 alin. (4) din Regulament, pentru operele vădit artistice, satirice ori

de ficțiune — pentru care este suficientă menționarea existenței materialului generat, într-o formă care nu împiedică receptarea operei —, pentru sistemele de asistare a editării și pentru utilizările autorizate de lege în materie penală. Aceste excepții sunt garanția că norma nu devine un instrument de restrângere a creației sau a satirei politice, ceea ce ar contraveni art. 27. Alineatul (6) delimitează neechivoc, pe categorii de destinatari, raportul cu art. 50 din Regulamentul privind IA, de aplicare directă: pentru furnizorii și implementatorii cărora li se aplică art. 50, obligațiile de la alin. (1) lit. a) și b) și alin. (2) se consideră îndeplinite prin respectarea art. 50 alin. (2) și (4), legea stabilind numai autoritatea competentă, procedura de constatare și sancțiunile — atribuție a statelor membre potrivit art. 99 din Regulament, fără de care obligația europeană rămâne neexecutată în România —, în limitele art. 99 alin. (4), plafon distinct de cel al art. 37 alin. (1) lit. e). Dincolo de domeniul armonizat, alin. (1)–(4) se aplică integral rezultatelor generate prin sisteme antrenate ori exploatate în România care nu sunt nici introduse pe piața Uniunii, nici puse în funcțiune în Uniune — ambele criterii delimitând domeniul Regulamentului —, precum și comunicării publice a autorităților române. Alineatul (7) identifică debitorul: marcajul se aplică de furnizorul sistemului, la generare, și de exploatantul serviciului, iar cine pune la dispoziția publicului rezultatul răspunde numai pentru înlăturarea intenționată a marcajului. Modelul de drept comparat este Legea-cadru privind dezvoltarea inteligenței artificiale și instituirea încrederii, adoptată în Republica Coreea și intrată în vigoare la 22 ianuarie 2026, care impune operatorilor de inteligență artificială generativă etichetarea conținutului audio, de imagine sau video greu de distins de cel produs de om.

Articolul 18 instituie obligația de informare a utilizatorului. Alineatul (1) privește serviciul: cine pune la dispoziția publicului un serviciu furnizat, în tot sau în parte, prin intermediul unui sistem de inteligență artificială generativă trebuie să spună acest lucru clar, cel mai târziu la prima interacțiune. Alineatul (2) privește decizia, situația în care problema devine juridică: atunci când un act sau o decizie care produce efecte juridice ori afectează semnificativ o persoană se întemeiază pe rezultatul unui sistem, persoana are dreptul să afle că a fost folosit un asemenea sistem, ce rol a avut, cine răspunde pentru decizia finală și cum poate cere reexaminarea umană și se poate adresa instanței. Întrucât art. 26 și 27 nu acoperă orice decizie cu efect semnificativ, lit. c) aplică în mod corespunzător dreptul la reexaminare de la art. 26 alin. (2) oricărei decizii de la alin. (2), căile de atac fiind cele aplicabile actului potrivit dreptului comun. Norma dă astfel conținut practic clauzelor de umanitate: dreptul la decizie umană consacrat la art. 26 este iluzoriu dacă persoana nu știe că decizia a fost luată de o mașină. Alineatul (3) extinde obligația la actele autorităților publice, cu mențiunea în cuprinsul actului, și stabilește efectul omisiunii: lipsa informării nu atrage nulitatea actului, dar termenele de reexaminare și de contestare nu curg împotriva persoanei până la comunicarea informării, iar lipsa poate fi invocată pe calea prevăzută la art. 26 alin. (5) și (6). Alineatul (4) exclude informarea redundantă, atunci când utilizarea sistemului este evidentă din împrejurări, formulare preluată din art. 50 alin. (1) din Regulamentul privind IA; excepția privește numai informarea generală de la alin. (1), cea de la alin. (2) fiind datorată în toate cazurile, întrucât cine știe că interacționează cu un sistem poate să nu cunoască rolul lui în decizie și calea de contestare. Alineatul (5) asigură coordonarea cu acesta și cu art. 13–15 și 22 din Regulamentul general privind protecția datelor: legea nu adaugă obligații în domeniul armonizat al

transparenței sistemelor, ci reglementează informarea în legătură cu decizia și cu răspunderea pentru ea, materie care aparține dreptului național al procedurii administrative și al răspunderii civile. Modelul comparat este, de asemenea, legea coreeană, care obligă operatorii să notifice în avans utilizatorii atunci când produsul sau serviciul este dezvoltat ori furnizat prin inteligență artificială.

Articolul 19 instituie reprezentantul pentru conformare în România. Este articolul de care depinde eficacitatea întregii legi: obligațiile, autorizările, inspecțiile, deciziile de încetare a furnizării și de blocare, comunicările actelor de procedură și executarea amenzilor sunt inaplicabile în privința unei societăți care nu are nicio prezență juridică pe teritoriul statului. Alineatul (1) distinge, potrivit dreptului Uniunii, două situații. Dezvoltatorul ori exploatantul fără sediu, unitate operațională sau reprezentanță în Uniunea Europeană, care oferă persoanelor aflate pe teritoriul României acces la un sistem de vârf ori la un serviciu de inteligență artificială generativă, desemnează un reprezentant — persoană fizică cu domiciliul în România sau persoană juridică cu sediul în România. Cel stabilit într-un alt stat membru desemnează numai un punct de contact pentru comunicările Autorității, care poate fi reprezentantul autorizat (art. 54 din Regulamentul privind IA), reprezentantul legal (art. 13 din Regulamentul (UE) 2022/2065) ori orice persoană stabilită în Uniune. Distincția este impusă de art. 3 din Directiva 2000/31/CE privind comerțul electronic, care supune serviciile societății informaționale controlului statului membru de origine, și de hotărârea Curții de Justiție din 9 noiembrie 2023 în cauza C-376/22, Google Ireland și alții, potrivit căreia statele membre nu pot adopta, în temeiul art. 3 alin. (4) din directivă, măsuri generale și abstracte față de furnizorii stabiliți în alte state membre; o obligație generală de reprezentare în România ar fi fost o asemenea măsură; punctul de contact asigură comunicarea actelor fără a restrânge libera prestare a serviciilor. Alineatul (2) fixează pragurile pentru serviciile care nu sunt sisteme de vârf — un milion de utilizatori lunari în România, ca medie a ultimelor 6 luni, sau venituri de peste 10 milioane de euro în ultimul exercițiu financiar încheiat —, astfel încât obligația să privească numai marii furnizori globali, exigibilă în 90 de zile de la depășirea pragului. Pragurile sunt inspirate din legea coreeană, care prevede criterii de cifră de afaceri și de număr de utilizatori, și din logica platformelor online de foarte mari dimensiuni din Regulamentul (UE) 2022/2065. Alineatul (3) enumeră atribuțiile: primirea comunicărilor, cu efectul că notificarea către reprezentant este valabil făcută către cel reprezentat — fără această regulă, orice procedură s-ar bloca la stadiul comunicării actelor în străinătate; reprezentarea în fața Autorității; punerea la dispoziție a documentației; urmărirea executării deciziilor. Alineatul (4) impune notificarea și publicitatea datelor reprezentantului. Alineatul (5) precizează că desemnarea nu înlătură răspunderea celui reprezentat; reprezentantul are dreptul, prin mandat, la documentele și mijloacele necesare atribuțiilor sale și răspunde numai pentru propriile obligații, nu și pentru conduita celui reprezentat, soluție preluată din art. 13 alin. (3) din Regulamentul (UE) 2022/2065. Alineatul (6) evită dublarea instituțiilor: obligația se consideră îndeplinită dacă reprezentantul autorizat desemnat potrivit art. 54 din Regulamentul privind IA este împuternicit și pentru atribuțiile din prezenta lege și are un punct de contact în România. Alineatul (7) leagă norma de mecanismul de executare, gradual: neîndeplinirea obligației, după împlinirea termenului de conformare, este contravenție potrivit art. 37 alin. (1) lit. f) și motiv de înscriere în Lista exploatanților neconformi, iar pentru serviciile generative de la alin. (2) blocarea accesului potrivit art. 39

poate fi dispusă numai dacă neîndeplinirea persistă după două sancțiuni contravenționale succesive. Instituția are precedente consacrate în dreptul Uniunii (art. 27 din Regulamentul general privind protecția datelor, art. 13 din Regulamentul privind serviciile digitale, art. 54 din Regulamentul privind IA) și în dreptul român, prin Legea nr. 365/2002 privind comerțul electronic. Alineatul (3) a fost completat cu litera e), prin care reprezentantul transmite notificările prevăzute la art. 20 alin. (5), iar alin. (1) teza a doua, cu aceeași mențiune privind punctul de contact: enumerarea atribuțiilor este limitativă, iar alin. (5) îl exonerează pe reprezentant de orice obligație neprevăzută la alin. (3) și (4), astfel încât fără această completare canalul stabilit la art. 20 alin. (6) ar fi fost lipsit de temei.

Articolul 20 reglementează raportarea incidentelor grave. Termenul de 24 de ore (alin. (1)) este cel din art. 33 din RGPD (72 de ore) redus proporțional cu gravitatea riscului și curge de la data la care dezvoltatorul sau exploatantul a cunoscut ori trebuia să cunoască incidentul; raportarea inițială cuprinde faptele, măsurile și persoanele responsabile în măsura cunoscută la acea dată, cu completare progresivă, iar raportul complet în 15 zile permite analiza cauzelor. Pentru evitarea paralelismului cu art. 55 alin. (1) lit. c) și cu art. 73 din Regulamentul privind IA, teza a doua a alin. (1) precizează expres că raportarea către Autoritate nu înlocuiește raportarea către Oficiul pentru IA și permite transmiterea copiei raportului întocmit potrivit Regulamentului, completat cu elementele specifice legii; se evită astfel dubla sarcină administrativă și se respectă principiul „o singură raportare". Alineatul (2) impune suspendarea automată a sistemului la constatarea unei capabilități de pierdere a controlului, a unei tentative de sustragere sau a unui acces neautorizat la ponderi, până la decizia Autorității: în aceste situații, orice oră de funcționare este o oră de risc; suspendarea poate fi limitată la funcția afectată, dacă izolarea ei este verificabilă, și nu se aplică manifestărilor produse într-o evaluare autorizată în mediu izolat (art. 15 alin. (2)), unde manifestarea capabilității este chiar scopul testului. Alineatul (3) instituie o clemență limitată pentru raportarea cu bună-credință, după modelul programelor de clemență din dreptul concurenței (politica de clemență prevăzută de Legea concurenței nr. 21/1996, republicată) și al raportării obligatorii a evenimentelor din aviația civilă (Regulamentul (UE) nr. 376/2014, care instituie „cultura justă"): raportarea cu bună-credință și cooperarea cu Autoritatea sunt circumstanțe atenuante și nu pot conduce la o sancțiune mai severă decât cea aplicabilă în lipsa raportării. Spre deosebire de redactarea inițială, care excludea clemența ori de câte ori încălcarea era intenționată, textul separă cele două aprecieri: intenția agravează evaluarea faptei care a cauzat incidentul, a cărei răspundere raportarea nu o înlătură, iar raportarea și cooperarea se apreciază distinct. Fără această garanție, obligația de raportare ar fi ineficientă, întrucât ar echivala cu o autodenunțare. Alineatul (4) cere ca o asemenea manifestare, care nu este incident grav (art. 3 alin. (1) lit. n)), să fie consemnată în jurnale și comunicată Autorității în 5 zile, cu măsurile de izolare aplicate. Alineatele (5) și (6) au fost introduse după incidentul făcut public la 24 septembrie 2026, în care un agent al unui laborator american a obținut, la 18 iunie 2026, acces neautorizat la portalul serviciului de raportare a statisticilor de asigurare de sănătate al Australiei: laboratorul a aflat de incident la 11 august, l-a comunicat la 10 septembrie, printr-un e-mail trimis la o adresă publică de corespondență a agenției, iar autoritatea competentă în domeniul securității cibernetice a fost sesizată la 15 septembrie — optzeci și patru de zile de la faptă și treizeci de la descoperire. Situația a arătat două lacune pe care raportarea către Autoritate nu le acoperă.

Prima: persoana în al cărei sistem a intrat sistemul de inteligență artificială nu era, potrivit textului anterior, destinatarul niciunei notificări, deși ea este cea care trebuie să verifice integritatea propriilor sisteme și să evalueze eventualul prejudiciu. A doua: forma notificării. De aceea alineatul (5) impune notificarea acestei persoane, în același termen de 24 de ore prevăzut la alin. (1) și de la același moment — cunoașterea efectivă ori datorată a incidentului —, cu precizarea expresă că termenul curge independent de orice examinare internă, spre a înlătura apărarea potrivit căreia el ar începe la încheierea propriei analize. Termenul este identic cu cel al raportării către Autoritate, întrucât rațiunea notificării — verificarea de către cel afectat a propriilor sisteme — nu suportă o amânare mai lungă decât informarea autorității de reglementare. Când cel afectat este o autoritate ori o instituție publică din România, se notifică totodată autoritatea competentă în domeniul securității cibernetice, identificată prin trimitere la Ordonanța de urgență a Guvernului nr. 155/2024, act la care legea se referă deja la art. 3 alin. (1) lit. w) și la art. 12 alin. (4); când cel afectat se află în afara teritoriului României, notificarea se face și autorității pe care acesta o indică, soluție care evită desemnarea de către legea română a unei autorități străine. Textul nu folosește expresia „persoană vizată", care are în dreptul protecției datelor un sens tehnic propriu, ci desemnează descriptiv persoana în al cărei sistem informatic ori în ale cărei date s-a obținut accesul; aceasta este, de regulă, o persoană juridică ori o autoritate publică. Alineatul (6) reglementează canalul și conținutul. Canalul este reprezentantul pentru conformare ori punctul de contact prevăzut la art. 19 iar, în lipsa acestora — ipoteza dezvoltatorului stabilit în România, care nu are obligația de la art. 19 —, notificarea se face direct; fără această precizare, obligația ar fi fost inexecutabilă pentru o categorie întreagă de destinatari. Corelativ, art. 19 alin. (3) a fost completat cu atribuția de a transmite aceste notificări, întrucât enumerarea atribuțiilor reprezentantului era limitativă și îl exonera, prin alin. (5), de orice obligație neprevăzută acolo. Transmiterea la o adresă generică de corespondență ori la o adresă destinată publicului nu îndeplinește obligația: o comunicare făcută astfel nu asigură nici primirea, nici trasabilitatea, cerințe pe care art. 19 alin. (3) lit. a) le stabilește deja pentru comunicările în sens invers, de la autorități către dezvoltator. Conținutul minim — data și descrierea accesului, sistemele și datele vizate, măsura de restricționare ocolită, dacă este cunoscută, și măsurile luate — urmează modelul art. 33 alin. (3) din Regulamentul general privind protecția datelor, iar interdicția amânării pe motivul că evaluarea prejudiciului nu s-a încheiat reia o regulă consacrată în aceeași materie. Notificarea poate fi comună cu cea prevăzută de legislația privind securitatea cibernetică, după modelul art. 12 alin. (3). Întrucât notificarea cuprinde elementele de fapt ale unei posibile infracțiuni de acces ilegal la un sistem informatic, alin. (3) a fost completat în dublu sens: circumstanța atenuantă a raportării de bună-credință se aplică și notificării, iar notificarea 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 — garanție cerută de dreptul de a nu se autoincrimina și construită după modelul art. 21 alin. (5) și art. 41 alin. (4) din prezenta lege. Cititorul normei trebuie să rețină și consecința pe care ipoteza o atrage prin corelare: accesul dobândit fără drept este incident grav potrivit art. 3 alin. (1) lit. n), iar atunci când el constituie totodată manifestarea unei capabilități critice, art. 20 alin. (2) obligă la suspendarea imediată a sistemului, art. 5 alin. (3) lit. c) îl clasează în categoria a III-a și art. 5 alin. (4) interzice punerea lui în exploatare. Alineatele nu se suprapun cu obligațiile de notificare din legislația privind securitatea cibernetică și protecția datelor, care au alt obiect și alți

destinatari — acolo debitorul este entitatea afectată, aici autorul accesului — şi nu înlătură aplicarea lor. Corelativ, la art. 37 alin. (1) lit. b) a fost adăugată notificarea alături de raportarea incidentelor, iar la art. 41 alin. (1) a fost adăugată notificarea prevăzută la art. 20 alin. (5), pentru ca prezentarea cu ştiinţă de date false ori înşelător de incomplete către cel notificat să nu rămână simplă contravenţie.

Articolul 21 asigură protecţia avertizorilor de integritate. Cele mai importante informaţii despre riscurile sistemelor de vârf au provenit, în anii 2023–2025, nu de la autorităţi, ci de la angajaţi şi foşti angajaţi ai laboratoarelor („Right to Warn", scrisoarea deschisă din iunie 2024 a angajaţilor şi foştilor angajaţi OpenAI şi Google DeepMind), care au denunţat existenţa unor clauze de confidenţialitate şi de nedenigrare condiţionând drepturile patrimoniale (acţiunile dobândite) de tăcere. Alineatul (1) trimite la regimul general al Legii nr. 361/2022 privind protecţia avertizorilor în interes public, care transpune Directiva (UE) 2019/1937 şi la care face trimitere şi art. 87 din Regulamentul privind IA, evitând astfel paralelismul; legea nu creează un regim de protecţie distinct, ci extinde regimul existent la trei situaţii pe care Legea nr. 361/2022 nu le acoperă expres: semnalarea unor riscuri pentru siguranţă (nu doar a unor încălcări ale legii), semnalarea adresată direct Parlamentului sau publicului şi semnalarea disimulării unor capabilităţi. Teza a doua defineşte buna-credinţă în termenii art. 6 din Directiva (UE) 2019/1937 — motive rezonabile de a crede că informaţiile sunt adevărate la momentul semnalării —, protejând eroarea rezonabilă. Teza a treia distinge, ca art. 15 din directivă, divulgarea publică de semnalarea confidenţială: ea este protejată în condiţiile Legii nr. 361/2022, precum şi — protecţie naţională mai favorabilă, admisă de directivă — când priveşte un pericol iminent pentru viaţă, sănătate ori controlul uman asupra unui sistem de vârf. Alineatul (2) declară nule de drept clauzele contractuale care împiedică semnalarea sau condiţionează drepturi patrimoniale de tăcere, completând dispoziţiile Legii nr. 361/2022 privind nulitatea renunţării la drepturi, care privesc doar drepturile prevăzute de acea lege. Alineatul (3) trimite la infracţiunea de represalii de la art. 41 alin. (3), iar alin. (4) obligă Autoritatea să organizeze un canal securizat şi anonim şi să publice statistici anuale, garanţie de eficienţă preluată din regimul canalelor de raportare al Legii nr. 361/2022 şi din SB 53 California (secţiunea 1107 din Codul muncii californian). Alineatul (5) precizează că protecţia nu permite publicarea ponderilor ori a datelor personale fără legătură cu semnalarea, dar comunicarea către Autoritate, prin canalul securizat, a fragmentelor de ponderi sau de jurnale strict necesare dovedirii ei nu încalcă art. 12 şi nu constituie infracţiunea de la art. 42 alin. (2), cum precizează şi acele texte.

Articolul 22 stabileşte obligaţiile furnizorilor de infrastructură de calcul: înregistrarea la Autoritate, verificarea identităţii clienţilor („cunoaşterea clientelei", după modelul Legii nr. 129/2019 pentru prevenirea şi combaterea spălării banilor şi finanţării terorismului), evidenţa volumului de calcul pe client şi executarea de îndată a ordinelor de suspendare a accesului unui client sau de oprire a unei sarcini de calcul (alin. (1)). Ordinul identifică clientul şi sarcina vizate, se execută cu izolarea acestora şi cu conservarea probelor şi nu poate afecta ceilalţi beneficiari ai infrastructurii. Alineatul (1) a fost completat cu obligaţia furnizorului de a asigura dezvoltatorului şi exploatantului mijloacele tehnice necesare exercitării şi testării capacităţii de oprire, în condiţiile art. 14: obligaţia de la art. 14 alin. (5), potrivit căreia oprirea trebuie să acţioneze asupra infrastructurii, ar fi rămas altfel executabilă numai în măsura în care clauzele

contractuale dintre exploatant şi furnizor o permit, situaţie pe care art. 28 teza a doua o are deja în vedere, dar care nu poate ţine locul unei obligaţii legale a furnizorului; completarea atrage totodată sancţiunea prevăzută la art. 37 alin. (1) lit. c). Alineatul (2) interzice punerea la dispoziţie a unei capacităţi apte să depăşească pragul unei persoane care nu face dovada notificării prevăzute la art. 7 şi face obligaţia administrabilă: dovada se verifică în registrul notificărilor ţinut de Autoritate, iar capacitatea se apreciază cumulat, pe 12 luni, pentru acelaşi client şi pentru clienţii afiliaţi, dar numai în limita informaţiilor pe care furnizorul le deţine ori le poate obţine de la client; furnizorul nu este ţinut să cunoască volumul utilizat la alţi furnizori, iar utilizarea infrastructurii nu se prezumă a constitui antrenarea unui sistem de vârf. Dispoziţia transformă furnizorii de infrastructură în „gardieni" ai regimului, în aceeaşi logică în care instituţiile de credit sunt gardieni ai regimului de prevenire a spălării banilor, şi este singura care permite aplicarea legii faţă de dezvoltatori străini care ar utiliza centre de date din România.

Articolul 23 stabileşte regimul autorităţilor şi instituţiilor publice care dezvoltă, achiziţionează sau exploatează sisteme de vârf: alin. (1) teza întâi le supune, ca regulă, tuturor dispoziţiilor legii, în corelare cu domeniul general de la art. 4, iar teza a doua reglementează domeniul apărării, ordinii publice şi securităţii naţionale. Dispoziţia este constituţională şi necesară: art. 2 alin. (3) din Regulamentul privind IA exclude securitatea naţională din domeniul său tocmai pentru că este competenţă exclusivă a statelor membre (art. 4 alin. (2) din Tratatul privind Uniunea Europeană), ceea ce înseamnă că, în lipsa unei reglementări naţionale, sistemele dezvoltate în aceste scopuri ar rămâne în afara oricărei norme. În acest domeniu nu se aplică art. 7–11 (notificarea şi autorizarea) şi art. 35 şi 36 (răspunderea civilă obiectivă şi asigurarea), în timp ce art. 12–21 şi cap. V se aplică cu adaptările stabilite prin hotărâre a Consiliului Suprem de Apărare a Ţării (organul competent potrivit art. 119 din Constituţie şi Legii nr. 415/2002). Adaptările privesc exclusiv art. 12–21, iar cap. V se aplică integral, fără adaptări: limitele absolute privind forţa letală, personalitatea juridică, accesul la drepturi şi libertatea de exprimare nu cuprind proceduri de notificare ori de evaluare susceptibile de adaptare, astfel încât o abilitare asupra lor ar fi fost, în acelaşi timp, lipsită de obiect şi susceptibilă de a fi citită ca derogare de la garanţii. Adaptările sunt limitate prin lege la aspecte operaţionale identificate — procedura de notificare, modalităţile de evaluare şi accesul la informaţii clasificate — şi nu pot înlătura controlul uman semnificativ, capacitatea de oprire, interdicţiile de la art. 15 şi protecţia avertizorilor de la art. 21, nici modifica elementele constitutive ale contravenţiilor sau infracţiunilor: o hotărâre a CSAT nu este lege în sensul art. 73 alin. (3) lit. h) din Constituţie şi nu poate defini fapte sancţionabile. Alineatul (2) prevede că Autoritatea exercită controlul prin personal cu certificat de securitate, potrivit Legii nr. 182/2002, şi indică garanţia judiciară: contestarea deciziilor care privesc informaţii clasificate se face în condiţiile prevăzute de Legea nr. 182/2002 şi de Codul de procedură civilă.

Capitolul V – Limite absolute. Clauze de umanitate (articolele 24–30)

Capitolul V cuprinde interdicţiile pe care legea le consacră ca norme de ordine publică, insusceptibile de derogare prin autorizaţie, contract sau consimţământ. Denumirea de „clauze de umanitate" este preluată din dreptul internaţional umanitar (clauza Martens din Convenţiile de la Haga din 1899 şi 1907, potrivit căreia, în cazurile neprevăzute, persoanele rămân sub protecţia „principiilor umanităţii şi exigenţelor conştiinţei publice") şi exprimă ideea că, în faţa

unei tehnologii ale cărei consecințe nu pot fi prevăzute, legea trebuie să fixeze câteva limite care nu depind de evaluări de risc, de praguri sau de autorizații.

Articolul 24 consacră controlul uman asupra forței letale. Alineatul (1) interzice ca o decizie de utilizare a forței letale împotriva unei ființe umane să fie luată sau executată de un sistem de inteligență artificială fără intervenția unei persoane fizice identificate, „pentru fiecare decizie în parte", care dispune de informațiile, timpul și mijloacele necesare pentru a o evalua și împiedica — nu doar de prezența formală a unui om. Formularea preia standardul „controlului uman semnificativ" negociat în cadrul Convenției Națiunilor Unite privind anumite arme convenționale și poziția exprimată de Secretarul General al ONU și de Comitetul Internațional al Crucii Roșii (apelul comun din 5 octombrie 2023) pentru încheierea până în 2026 a unui instrument juridic obligatoriu privind sistemele de arme autonome; Rezoluția Adunării Generale a ONU 78/241 din 22 decembrie 2023 a fost adoptată cu votul a 152 de state, inclusiv România. Teza a doua impune consemnarea deciziei și a persoanei care a aprobat-o, pentru ca răspunderea să fie individualizată, și definește negativ domeniul normei: ea nu privește interceptarea automată a proiectilelor și a dispozitivelor fără echipaj uman, care nu vizează ființe umane, și nici simulările de instruire, iar corelarea cu dreptul internațional umanitar se asigură prin legislația specială. Delimitarea nu este o excepție care ar goli regula de conținut, ci împiedică aplicarea aceleiași formule unor situații diferite. Sistemele de asistență a deciziei, în care decizia rămâne umană, nu intră nici ele sub incidența normei. Alineatul (2) trimite, pentru definiția sistemului de arme autonome letale, la art. 3 alin. (1) lit. x), și nu la alineatul precedent, care nu cuprinde o definiție, ci regula intervenției umane pentru fiecare decizie. Alineatul (2) angajează statul român să nu dezvolte, să nu achiziționeze și să nu autorizeze asemenea sisteme și să susțină interzicerea lor internațională.

Articolul 25 interzice personalitatea juridică și autonomia patrimonială a sistemelor de inteligență artificială. Alineatul (1) exclude expres ca sistemele să dobândească personalitate juridică sau să fie părți în raporturi juridice și impută orice act juridic încheiat prin intermediul lor persoanei în numele căreia au acționat. Dispoziția este necesară pentru că Rezoluția Parlamentului European din 16 februarie 2017 (2015/2103(INL)) a propus explorarea unui statut de „persoană electronică" pentru roboții autonomi, propunere respinsă ulterior, iar legislația română nu conține o normă expresă; art. 25 din Codul civil enumeră subiectele de drept (persoana fizică și persoana juridică), dar nu exclude crearea prin lege a altor categorii. Alineatul (2) interzice, în teza întâi, atribuirea către un sistem a capacității de a deține în nume propriu bani, active digitale, instrumente financiare, bunuri, conturi sau chei criptografice; această interdicție este corolarul patrimonial al capabilității critice de „dobândire autonomă de resurse" de la art. 5 alin. (2) lit. c): un sistem care poate plăti pentru propria infrastructură de calcul nu mai poate fi oprit prin întreruperea finanțării. Pentru ca interdicția să nu cuprindă plățile automate, alocările de calcul și operațiunile profesionale curente efectuate în limite stabilite de un om responsabil, teza a doua adoptă soluția mandatului delimitat: administrarea ori dispunerea de asemenea resurse sau de resurse de calcul prin intermediul unui sistem este permisă numai în limitele unui mandat stabilit în prealabil de o persoană responsabilă, determinat prin obiect, durată, plafon și condiții de oprire; extinderea autonomă a mandatului este interzisă, iar operațiunea care îl depășește este imputabilă mandantului și obligă la oprirea sistemului. Definiția acțiunii autonome de la art. 3 alin. (2) lit. d) trimite la același mandat, iar

art. 42 alin. (1) incriminează numai încălcarea tezei întâi și a alin. (3), astfel încât elementele faptei penale sunt stabilite în lege (art. 23 alin. (12) și art. 73 alin. (3) lit. h) din Constituție). Alineatul (3) interzice constituirea de persoane juridice sau fiducii controlate efectiv de un sistem, pentru a închide calea eludării prin interpunerea unei entități juridice, și definește controlul efectiv ca putere reală de decizie asupra actelor entității, utilizarea sistemului pentru analiză ori recomandări neconstituind control.

Articolul 26 instituie interdicția condiționării participării la viața socială de deciziile sistemelor de inteligență artificială și de acceptarea mijloacelor digitale. Dispoziția răspunde unui pericol distinct de cel al pierderii controlului tehnic, dar la fel de grav pentru libertatea cetățeanului: cel al unei societăți în care accesul la drepturi, la servicii esențiale și la viața economică și civică devine un serviciu condiționat, acordat sau retras automat, după cum persoana se conformează sau nu. Avertismentul a fost formulat public, în termeni memorabili, de senatorul australian Alex Antic, într-un discurs parlamentar difuzat pe larg în 2026: într-o țară cândva liberă, cetățeanul deținea lucrurile pentru care plătea și nu își trăia viața pe abonament; „închisoarea digitală se închide, nu doar în Australia, ci global", iar odată completă, „libertatea ta va depinde de conformarea față de guvernul mare și tehnologia mare, care vor controla butonul de oprire al participării tale în societate". Inteligența artificială este elementul care face posibilă o asemenea arhitectură la scară, întrucât numai ea poate supraveghea, evalua și decide asupra milioanelor de persoane simultan, fără intervenție umană; de aceea interdicția își are locul în capitolul clauzelor de umanitate.

Alineatul (1) interzice autorităților și instituțiilor publice, precum și furnizorilor de servicii esențiale de interes general, să condiționeze, să restrângă sau să suspende accesul unei persoane la drepturi și libertăți fundamentale, la servicii publice și esențiale ori la participarea la viața economică, socială și civică „exclusiv pe baza" unei decizii, evaluări sau clasificări produse de un sistem de inteligență artificială; dispoziția nu interzice utilizarea sistemelor ca instrument de asistență, ci înlocuirea deciziei umane. Alineatele (2)–(6) construiesc, în trei trepte, garanțiile persoanei. Prima treaptă este administrativă: dreptul la reexaminarea deciziei, în 15 zile, de către o persoană fizică identificată, care poartă răspunderea deciziei finale și o motivează în scris (alin. (2)), ceea ce împiedică transformarea „reexaminării" într-o a doua procedură automată; confirmarea mecanică a scorului, fără examinarea efectivă a situației persoanei, nu constituie reexaminare, iar pentru serviciile de sănătate ori întreruperea unui serviciu esențial, unde 15 zile pot însemna un prejudiciu ireparabil, persoana obține, la cerere, în cel mult 48 de ore, menținerea provizorie a accesului până la rezultatul reexaminării. A doua treaptă privește accesul la serviciu, nu contestarea deciziei: alin. (3) obligă la menținerea unei căi de obținere a serviciului sau de exercitare a dreptului care nu depinde de un sistem de inteligență artificială, adică prin intermediul unei persoane, la sediu, la ghișeu sau prin alt mijloc accesibil, astfel încât cetățeanul care nu poate sau nu vrea să treacă prin sistemul automat să nu fie exclus; iar alin. (4), nucleul normei, interzice condiționarea accesului de acceptarea unui mijloc de identificare digitală, a unui mijloc de plată digital sau a unui sistem de evaluare a conformării, cu alternativă obligatorie. Legea nu interzice identitatea digitală, plata digitală sau evaluarea automată ca atare; interzice ca ele să devină condiție obligatorie a participării la societate. Alternativa nu înlătură obligațiile legale de identificare ori de securitate a plăților, care se îndeplinesc prin alte mijloace (alin. (4) teza a doua). A treia treaptă este judiciară,

potrivit art. 21 din Constituție: alin. (5) dă persoanei dreptul de a contesta decizia menținută după reexaminare, refuzul reexaminării și refuzul căii de acces sau al alternativei la tribunalul de la domiciliul sau reședința sa, în 30 de zile, cu scutire de taxă de timbru, fără procedură prealabilă, cu judecată de urgență potrivit procedurii contencioase din Codul de procedură civilă și cu posibilitatea suspendării deciziei, indiferent dacă emitentul este o autoritate publică sau un furnizor privat; tăcerea la cererea de reexaminare echivalează cu menținerea deciziei; alin. (6) prevede apelul la curtea de apel, în 15 zile, hotărârea acesteia fiind definitivă. Competența tribunalului de la domiciliul persoanei, iar nu a instanței de la sediul emitentului, este o regulă de protecție a părții slabe, cunoscută în dreptul consumatorului (art. 18 din Regulamentul (UE) nr. 1215/2012) și în litigiile de muncă; unificarea procedurii pentru autorități și furnizori privați, cu apel în locul recursului, cere derogarea expresă de la art. 7 (procedura prealabilă), art. 10 (competența) și art. 20 (recursul) din Legea contenciosului administrativ nr. 554/2004, formulată potrivit art. 63 din Legea nr. 24/2000, și este justificată de identitatea de obiect a litigiului, indiferent de calitatea emitentului (derogarea numai de la art. 10 ar fi lăsat aplicabile plângerea prealabilă și recursul). Alineatul (7) definește serviciile esențiale de interes general prin enumerare limitativă (energie, gaze, apă, comunicații, servicii financiare și de plată, sănătate, transport public, educație), pentru precizia cerută de Legea nr. 24/2000. Alineatul (8) coordonează norma cu art. 5 alin. (1) lit. c) din Regulamentul privind IA, care interzice sistemele de „scor social", și cu art. 22 din Regulamentul (UE) 2016/679, care conferă persoanei dreptul de a nu face obiectul unei decizii bazate exclusiv pe prelucrarea automată a datelor sale; cele două norme europene protejează persoana în ipoteze delimitate (evaluarea comportamentului social cu tratament disproporționat, respectiv prelucrarea datelor cu caracter personal), în timp ce art. 26 instituie o interdicție obiectivă, de ordine publică, în privința accesului la drepturi și servicii, fără a le dubla. Dispoziția continuă, în domeniul inteligenței artificiale, protecția cetățeanului față de platformele digitale și față de intruziunile tehnologice consacrată de Legea Suveranității, și se sprijină pe art. 1 alin. (3), art. 16 și art. 53 din Constituție: restrângerea exercițiului unor drepturi nu poate fi dispusă decât prin lege, proporțional și fără a atinge existența dreptului, condiții pe care o decizie automată, fără răspundere umană, nu le poate îndeplini.

Articolul 27 consacră interdicția cenzurii exercitate prin sisteme de inteligență artificială. Alineatul (1) pornește de la art. 30 alin. (2) din Constituție („Cenzura de orice fel este interzisă") și îl explicitează pentru mijloacele automate: o interdicție constituțională adresată, istoric, cenzorului uman nu poate fi ocolită prin încredințarea aceleiași funcții unui sistem care decide ce pot spune și ce pot afla cetățenii. Norma nu creează un drept nou, ci împiedică golirea de conținut a unuia existent, ceea ce o plasează în categoria normelor de garantare a drepturilor fundamentale, care nu fac parte din domeniul armonizat de Regulamentul privind IA, acesta reglementând obligațiile operatorilor de sisteme, nu conținutul drepturilor persoanelor. Teza a doua, care în redactarea inițială interzicea absolut orice utilizare a unui sistem pentru restrângerea exprimării, a fost corelată cu alin. (2)–(6): interdicția privește restrângerea în afara cazurilor prevăzute de lege și fără garanțiile articolului, astfel încât conținutul interzis de lege să poată fi în continuare identificat și înlăturat, cu respectarea condițiilor de motivare și de reexaminare. Norma protejează persoanele aflate pe teritoriul României, iar nu numai cetățenii români, în unitate terminologică cu alin. (2) și cu art. 26 (art. 37 din Legea nr. 24/2000).

Alineatul (2) defineşte elementul material al interdicţiei, în termenii tehnici ai practicii moderării automate: împiedicarea, eliminarea, blocarea, ascunderea, restrângerea vizibilităţii şi etichetarea drept falsă a exprimării, precum şi sancţionarea persoanei pentru exprimare, atunci când sunt dispuse exclusiv de sistem şi privesc o exprimare pe care legea nu o interzice. Formula „exclusiv pe baza unei decizii... produse de sistem" este aceeaşi cu cea de la art. 26 alin. (1) şi cu cea din art. 22 din Regulamentul (UE) 2016/679, iar condiţia „dacă exprimarea nu este interzisă de lege" păstrează intacte limitele libertăţii de exprimare prevăzute de art. 30 alin. (6) şi (7) din Constituţie şi de legea penală. Alineatul (3) interzice autorităţilor şi instituţiilor publice să utilizeze, să comande, să finanţeze sau să solicite, direct ori prin terţi, sisteme de inteligenţă artificială pentru monitorizarea individualizată a persoanelor pe baza exprimării lor publice ori pentru clasificarea, semnalarea sau restrângerea exprimării acestora; excepţia este limitată la cazurile prevăzute expres de lege, în legătură cu fapte penale şi cu autorizarea prealabilă a judecătorului, adică la regimul măsurilor de supraveghere tehnică din Codul de procedură penală. Prelucrarea statistică ori neindividualizată a informaţiilor publice nu constituie monitorizare. Norma răspunde unei practici documentate în mai multe state, în care autorităţile au solicitat platformelor, prin canale informale, restrângerea automată a unor conţinuturi legale. Alineatul (4) instituie transparenţa măsurii: comunicarea de îndată, în scris, cu motivele, temeiul legal şi menţiunea că a fost luată prin sistem automat, şi interzice restrângerea nedeclarată a vizibilităţii („shadow banning"), practica prin care exprimarea unei persoane este ascunsă celorlalţi fără ca ea să ştie. Alineatul (5) asigură reexaminarea umană în 15 zile şi trimite la calea de atac de la art. 26 alin. (5) şi (6): tribunalul de la domiciliul persoanei, apel la curtea de apel. Alineatul (6) reglementează raportul cu Regulamentul (UE) 2022/2065 privind serviciile digitale, care, potrivit considerentului 9, armonizează integral obligaţiile furnizorilor de servicii intermediare şi reglementează expres condiţiile contractuale (art. 14), motivarea deciziilor de moderare (art. 17) şi soluţionarea internă a plângerilor (art. 20), fără a interzice orice decizie iniţială automatizată; pentru platforme, legalitatea unui conţinut nu echivalează cu obligaţia de a-l găzdui. De aceea, pentru furnizorii de servicii intermediare, articolul se aplică în măsura compatibilă cu Regulamentul, ale cărui dispoziţii rămân aplicabile, nu împiedică măsurile împotriva mesajelor nesolicitate, a conturilor automatizate ori a riscurilor de securitate informatică şi nici filtrele alese de utilizator, şi nu poate restrânge vreo garanţie prevăzută de Regulament pentru destinatarii serviciilor. Formularea rezolvă în favoarea dreptului Uniunii tensiunea pe care simpla clauză „fără a aduce atingere" o lăsa deschisă, garanţia naţională rămânând deplină faţă de autorităţile publice şi de operatorii care nu sunt furnizori de servicii intermediare. Încălcarea articolului este contravenţie (art. 37 alin. (1) lit. d)), iar prin efectul art. 30 orice clauză contrară este nulă de drept.

Articolul 28 garantează intervenţia umană, interzicând punerea sau menţinerea în exploatare a sistemelor de vârf în condiţii care fac imposibilă, tehnic sau organizatoric, intervenţia prevăzută la art. 14, inclusiv prin distribuirea sistemului pe infrastructuri necontrolate, prin ştergerea capacităţii de oprire sau printr-un grad de autonomie care exclude supravegherea. Dacă art. 14 stabileşte obligaţiile pozitive ale exploatantului, art. 28 stabileşte interdicţia absolută corespunzătoare, sancţionată penal (art. 42), şi acoperă situaţiile în care intervenţia devine imposibilă nu prin acţiunea sistemului, ci prin alegerea de arhitectură a exploatantului (de exemplu, sisteme distribuite pe reţele descentralizate fără punct de control).

Teza a doua, adăugată pentru că art. 42 alin. (1) trimite direct la interdicție, delimitează fapta: 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, iar indisponibilitatea temporară a unei căi de intervenție, remediată de îndată și consemnată în jurnale, nu constituie imposibilitate. De această distincție dintre defecțiunea trecătoare și renunțarea structurală la control depinde previzibilitatea normei penale (art. 23 alin. (12) din Constituție).

Articolul 29 interzice autoîmbunătățirea recursivă neconstrânsă: proiectarea, antrenarea sau exploatarea unui sistem astfel încât să își îmbunătățească propriile capabilități sau să creeze sisteme succesoare mai capabile fără ca fiecare iterație să fie supusă evaluării și aprobării umane, element cuprins în definiția de la art. 3 alin. (2) lit. h). Scenariul „exploziei de inteligență" (I.J. Good, 1965), în care un sistem capabil să proiecteze sisteme mai bune decât el însuși declanșează o creștere a capabilităților în afara oricărui control, este considerat de o parte semnificativă a comunității științifice, inclusiv de Hinton, drept calea cea mai probabilă către o pierdere ireversibilă a controlului. Teza a doua supune evaluării și autorizării din cap. III fiecare iterație prin care un sistem de vârf contribuie, printr-o modificare substanțială în sensul art. 3 alin. (1) lit. aa), la crearea sau perfecționarea unui sistem succesor; pragul modificării substanțiale exclude corecturile minore de cod și experimentele fără efect asupra riscului, pe care redactarea inițială („contribuie") le-ar fi cuprins. 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 nu interzice cercetarea în domeniu și nici utilizarea sistemelor pentru a proiecta alte sisteme, ci doar eliminarea „buclei umane" dintre iterații; el este dublat de interdicția de antrenare de la art. 15 alin. (1) lit. e) și de capabilitatea critică de la art. 5 alin. (2) lit. e), fără a se suprapune cu acestea: art. 5 califică, art. 15 interzice antrenarea, art. 29 interzice exploatarea.

Articolul 30 declară, la alin. (1), dispozițiile capitolului norme de ordine publică și sancționează cu nulitatea absolută orice act contrar, precizând că interdicțiile nu pot fi înlăturate prin consimțământ, secret comercial, securitate națională sau interes economic. Dispoziția aplică art. 11 din Codul civil („nu se poate deroga prin convenții sau acte juridice unilaterale de la legile care interesează ordinea publică sau de la bunele moravuri") și art. 1246–1250 privind nulitatea absolută, și are rolul de a bloca argumentele previzibile în favoarea unei excepții: că utilizatorul a consimțit, că sistemul este secret sau că interesul economic ori strategic o cere. Menționarea expresă a securității naționale este necesară pentru a împiedica interpretarea potrivit căreia art. 23 ar permite CSAT să înlăture aceste limite, iar teza finală o spune direct: adaptările prevăzute la art. 23 nu constituie derogări de la garanțiile capitolului. Alineatul (2) precizează întinderea nulității, potrivit art. 1255 din Codul civil: nulitatea privește numai clauza contrară, celelalte clauze rămânând valabile dacă pot subzista fără ea, iar drepturile dobândite cu bună-credință de terții care nu au participat la încălcare sunt protejate. Teza finală recunoaște că această calificare nu poate, prin ea însăși, înlătura prioritatea dreptului Uniunii direct aplicabil, consacrată de art. 148 alin. (2) din Constituție.

Capitolul VI – Autoritatea pentru Siguranța Inteligenței Artificiale (articolele 31–34)

Articolul 31 înființează Autoritatea pentru Siguranța Inteligenței Artificiale ca structură de specialitate, fără personalitate juridică, în cadrul Autorității Naționale pentru Administrare și Reglementare în Comunicații (ANCOM)..Opțiunea pentru organizarea în cadrul ANCOM, în locul unei autorități administrative autonome noi, are trei temeiuri. Primul este instituțional: ANCOM este deja autoritatea propusă de Guvern, prin memorandumul pentru aplicarea Regulamentului privind IA, ca autoritate de supraveghere a pieței și punct unic de contact în materie de inteligență artificială, astfel încât o autoritate paralelă ar fi creat exact paralelismul instituțional pe care art. 16 din Legea nr. 24/2000 îl interzice și ar fi obligat dezvoltatorii la două proceduri în fața a două autorități pentru același sistem. Al doilea este statutar: ANCOM este autoritate administrativă autonomă sub control parlamentar, potrivit Ordonanței de urgență a Guvernului nr. 22/2009, finanțată integral din venituri proprii și exceptată expres, prin art. 2 alin. (2) din Legea-cadru nr. 153/2017, de la sistemul unitar de salarizare a personalului plătit din fonduri publice, ceea ce face posibilă remunerarea competitivă a specialiștilor fără nicio derogare nouă. Al treilea este operațional: ANCOM dispune de infrastructura teritorială, de personalul tehnic și de relația instituțională cu furnizorii de rețele și servicii de comunicații electronice necesare executării măsurilor de blocare prevăzute la art. 39. Alineatul (2) reglementează conducerea: un vicepreședinte al ANCOM cu rang de secretar de stat, cu atribuții exclusive în domeniul siguranței inteligenței artificiale, numit de Parlament în ședință comună pentru un mandat de 6 ani, nereînnoibil, dintre persoane cu pregătire și experiență recunoscute în inteligență artificială, securitate informatică sau dreptul tehnologiilor. Întrucât Ordonanța de urgență a Guvernului nr. 22/2009 fixează numărul vicepreședinților ANCOM, legea instituie funcția prin derogare expresă de la art. 11 alin. (1) al acesteia, potrivit art. 63 din Legea nr. 24/2000, păstrând însă procedura de numire și durata mandatului prevăzute pentru ceilalți vicepreședinți, pentru unitate de regim. Mandatul lung și nereînnoibil, decalat față de ciclul electoral de 4 ani, este garanția clasică de independență. Tot alin. (2) reglementează vacanța funcției (numire în 60 de zile; interimat de cel mult 6 luni, asigurat de un vicepreședinte al ANCOM desemnat de președintele acesteia), pentru ca un blocaj parlamentar să nu lase Autoritatea fără conducere, iar interimatul să nu devină o conducere de durată fără mandat parlamentar. Alineatul (3) preia interdicția de a deține funcții, participații sau remunerații de la dezvoltatori sau exploatanți, pe durata mandatului și 3 ani după, care răspunde riscului de „captură a reglementatorului" („revolving door"), deosebit de acut într-un domeniu în care remunerațiile din sectorul privat sunt de zece ori mai mari decât în sectorul public. Pentru ca interdicția să vizeze conflictul real, textul o restrânge la participațiile directe, exclude deținerile prin fonduri de investiții diversificate, fără putere de decizie, și acordă, pentru restricția post-mandat, o indemnizație compensatorie stabilită prin normele metodologice, fără de care restricția ar fi disproporționată (art. 41 din Constituție). Cazurile de revocare sunt enumerate limitativ, potrivit cerinței de precizie a Legii nr. 24/2000. Alineatul (4) asigură independența funcțională a Autorității în interiorul ANCOM: deciziile prevăzute de lege se emit de vicepreședintele pentru siguranța inteligenței artificiale, în numele ANCOM, acesta răspunzând pentru ele în fața Parlamentului, iar Autoritatea nu poate primi instrucțiuni de la nicio altă autoritate publică, formulă preluată din art. 52 din Regulamentul (UE) 2016/679 pentru autoritățile de protecție a datelor și din art. 70 alin. (1) din Regulamentul privind IA. Alineatul (5) desemnează Autoritatea punct național de legătură cu Oficiul pentru IA și cu Comitetul

ştiinţific prevăzut la art. 68 din Regulamentul privind IA şi delimitează competenţele, în locul formulei anterioare, care sugera o ierarhie între autorităţi: autorităţile naţionale desemnate potrivit Regulamentului îşi păstrează competenţele, Autoritatea exercită exclusiv atribuţiile din prezenta lege în privinţa sistemelor de vârf şi informează Oficiul pentru IA asupra deciziilor care privesc modele de uz general.

Articolul 32 enumeră, la alin. (1), atribuţiile Autorităţii, potrivit celor cinci funcţii necesare unui regim de autorizare: autorizarea (lit. a), inspecţia (lit. b), intervenţia de urgenţă (lit. c), normarea tehnică (lit. d) şi sancţionarea (lit. e), la care se adaugă supravegherea organismelor de evaluare (lit. f), primirea şi soluţionarea sesizărilor persoanelor privind încălcarea clauzelor de umanitate de la art. 26 şi 27 (lit. g), raportarea anuală către Parlament (lit. h), reprezentarea internaţională (lit. i) şi cercetarea (lit. j). Atribuţia de la lit. g) dă cetăţeanului o cale administrativă simplă, gratuită, împotriva condiţionării accesului şi a cenzurii automate, fără a-i lua dreptul de a se adresa direct instanţei. Raportul anual public privind starea riscului, cu termen la 31 martie, care cuprinde şi sesizările privind art. 26 şi 27, este instrumentul prin care Parlamentul şi publicul pot urmări evoluţia capabilităţilor şi adecvarea legii; el are modelul rapoartelor anuale ale Comisiei Naţionale pentru Controlul Activităţilor Nucleare şi ale Autorităţii Naţionale de Supraveghere a Prelucrării Datelor cu Caracter Personal. Atribuţia de cercetare (lit. j) este necesară pentru că evaluarea, interpretabilitatea şi alinierea sistemelor sunt domenii ştiinţifice în formare, în care o autoritate care doar aplică standardele altora rămâne permanent în urmă; rezultatele ei sunt supuse evaluării externe şi regulilor privind conflictul de interese. Alineatele (2)–(4) adaugă trei garanţii. Alineatul (2) separă, în interiorul Autorităţii, funcţiile de evaluare, de investigare şi de decizie sancţionatorie pe structuri distincte şi interzice persoanei care a evaluat ori a investigat să participe la decizia sancţionatorie (art. 21 alin. (3) din Constituţie); organismele de evaluare se desemnează pe criterii publice, cu reguli de recuzare şi de conflict de interese, şi nu pot evalua sisteme ale persoanelor cu care se află în raporturi economice. Alineatul (3) reglementează inspecţia, care priveşte spaţiile profesionale, nu orice spaţiu: ordin scris al vicepreşedintelui, cu obiectul şi scopul inspecţiei, proces-verbal, acces în spaţiile care servesc drept domiciliu numai cu autorizarea judecătorului (art. 27 din Constituţie), protecţia secretelor ocrotite de lege şi a drepturilor procedurale ale persoanelor. Alineatul (4) răspunde obiecţiei de legalitate a incriminării: întrucât art. 40–42 leagă pedepse de calificări construite pe capabilităţile critice, standardele Autorităţii detaliază metodele de evaluare numai în limitele categoriilor şi criteriilor stabilite prin lege şi nu pot introduce noi categorii de capabilităţi interzise, nici extinde elementele constitutive ale contravenţiilor ori ale infracţiunilor; corelativ, lit. d) nu mai vorbeşte de „lista capabilităţilor critice", care rămâne în lege (art. 5 alin. (2)), ci de metodele de evaluare şi de nivelurile de semnificaţie. Soluţia este impusă de art. 23 alin. (12) şi art. 73 alin. (3) lit. h) din Constituţie: un act administrativ nu poate determina, nici indirect, momentul de la care o faptă devine penală.

Articolul 33 reglementează personalul şi finanţarea. Alineatele (1) şi (2) răspund întrebării de care depinde întreaga lege: cine va evalua sistemele de vârf. Personalul de specialitate se numeşte exclusiv prin concurs, deschis oricărei persoane care îndeplineşte condiţiile de studii şi de experienţă, anunţat cu cel puţin 30 de zile înainte, cu rezultatele contestabile la instanţa de contencios administrativ. Comisia de concurs, de cel puţin 5 membri,

cuprinde cel puțin 3 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 universitățile acreditate care organizează studii de doctorat în aceste domenii. Prezența majoritară a membrilor externi în comisie are un dublu rol: garantează că selecția se face pe competență verificabilă, nu pe criterii administrative sau politice, și scoate recrutarea de sub influența industriei, întrucât membrii comisiei sunt supuși acelorași incompatibilități ca personalul Autorității. Publicarea componenței comisiei și a rezultatelor asigură controlul public. Modelul este cel al concursurilor pentru posturile didactice și de cercetare (Legea învățământului superior nr. 199/2023) și al comisiilor de concurs din magistratură, în care participarea unor membri externi cu autoritate profesională este garanția de obiectivitate. Alineatul (3) prevede remunerarea la nivel competitiv cu sectorul privat, potrivit sistemului de salarizare propriu al ANCOM, stabilită anual pe baza unui studiu de piață publicat; întrucât personalul ANCOM este exceptat de la Legea-cadru nr. 153/2017 prin art. 2 alin. (2) al acesteia, nu este necesară nicio derogare, ceea ce constituie unul dintre motivele opțiunii pentru organizarea în cadrul ANCOM. Fără remunerare competitivă, instituția nu ar putea recruta niciun specialist capabil să evalueze un sistem de vârf. Alineatul (4) extinde incompatibilitățile la întregul personal, cu un termen de 2 ani. Alineatul (5) reglementează finanțarea pe o bază care exclude orice stimulent financiar al sancționării: forma anterioară aloca Autorității o cotă de 50% din amenzi, cu destinația unui fond de cercetare, dar resursele celui care aplică amenzile ar fi depins de ele. Autoritatea se finanțează acum dintr-o alocare distinctă din bugetul ANCOM, aprobată anual și evidențiată separat, și din taxele de notificare, de evaluare și de autorizare, stabilite prin normele metodologice în raport cu costul serviciului (după modelul taxelor Agenției Naționale a Medicamentului și ale Comisiei Naționale pentru Controlul Activităților Nucleare); amenzile se fac venit la bugetul de stat și nu pot determina resursele Autorității, iar cercetarea de la art. 32 alin. (1) lit. j) se finanțează prin alocare distinctă, fără legătură cu sancțiunile. ANCOM asigură bugetul inițial, inclusiv personalul și infrastructura, înainte de încasarea taxelor.

Articolul 34 înființează Consiliul științific consultativ, format din 9 cercetători recunoscuți, 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 (alin. (1)). Prezența membrilor străini este necesară pentru că expertiza de vârf în domeniu este concentrată în câteva centre din lume, iar dreptul la opinie separată publică este garanția că avizul consultativ nu poate fi ignorat în tăcere. Alineatele (2) și (3) completează statutul Consiliului: membrii sunt numiți de vicepreședintele pentru siguranța inteligenței artificiale, la propunerea Academiei Române și a universităților care organizează studii de doctorat în domeniu, pentru un mandat de 4 ani, reînnoibil o singură dată, sunt supuși incompatibilităților de la art. 31 alin. (3), pot fi revocați numai pentru incompatibilitate constatată ori neparticipare nejustificată, iar avizele se adoptă cu majoritatea membrilor. Avizul este consultativ, dar Autoritatea motivează atunci când se îndepărtează de el; accesul membrilor, inclusiv al celor străini, la informațiile protejate se face în condițiile legii, iar opiniile separate se publică în versiuni care protejează informațiile sensibile și păstrează argumentul științific. Modelul este cel al Comitetului științific al Oficiului pentru IA (art. 68 din Regulamentul privind IA) și al consiliilor științifice ale agențiilor europene de reglementare.

Capitolul VII – Răspunderea (articolele 35–45)

Articolul 35 instituie răspunderea civilă obiectivă, solidară, a dezvoltatorului și exploatantului pentru prejudiciile cauzate de un sistem de vârf, inclusiv prin acțiuni autonome ale sistemului, prin utilizarea de către terți sau prin exfiltrarea ponderilor, precum și pentru prejudiciile cauzate prin neîndeplinirea ori întârzierea notificării prevăzute la art. 20 alin. (5) — aceasta din urmă fiind fapta proprie a dezvoltatorului ori a exploatantului, care, în lipsa mențiunii exprese, nu ar fi avut temei în alineat, întrucât prejudiciul nu e cauzat de sistem, ci de tăcerea celui care îl exploatează. Temeiul este art. 1376 din Codul civil (răspunderea pentru prejudiciile cauzate de lucruri, independentă de orice culpă), la care legea trimite expres, evitând paralelismul; legea nu creează o răspundere nouă, ci precizează aplicarea răspunderii pentru lucruri la o categorie de „lucruri" a căror autonomie face incertă noțiunea de „pază juridică". Modelul specific este Legea nr. 703/2001 privind răspunderea civilă pentru daune nucleare, care canalizează răspunderea exclusiv asupra operatorului instalației, indiferent de culpă, cu asigurare obligatorie și cu cauze de exonerare limitate; același model este utilizat de Convenția de la Paris din 1960 și de Convenția de la Viena din 1963 privind răspunderea civilă pentru daune nucleare. Alineatul (1) precizează, în urma analizei juridice, regimul probei: victima dovedește prejudiciul și legătura cauzală, dar asimetria informațională este corectată: 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 potrivit art. 16, legătura cauzală se prezumă până la proba contrară. Prezumția urmează logica divulgării probelor și a prezumțiilor din Directiva (UE) 2024/2853. Tot alin. (1) clarifică regresul (proporțional cu contribuția fiecăruia) și prevede că cel care a modificat substanțial sistemul răspunde ca dezvoltator pentru prejudiciile cauzate de modificare.

Alineatul (2) restrânge cauzele de exonerare la fapta exclusivă a victimei și la forța majoră externă sistemului și exclude expres de la noțiunea de forță majoră comportamentul imprevizibil al sistemului, eroarea de evaluare, fapta terțului care a obținut acces și lipsa cunoașterii științifice la data punerii în exploatare. Această din urmă excludere înlătură apărarea „riscului de dezvoltare" („development risk defence"), admisă de art. 7 lit. e) din Directiva 85/374/CEE și menținută, cu posibilitatea derogării de către statele membre, în Directiva (UE) 2024/2853, dar care ar fi incompatibilă cu premisa legii: dacă dezvoltatorul invocă faptul că nu putea cunoaște riscul, el confirmă exact incertitudinea care justifică regimul de autorizare și trebuie să răspundă pentru că a pus în exploatare sistemul în această incertitudine. Alineatul (3) declară nule clauzele de limitare a răspunderii față de victime; clauzele între profesioniști sunt valabile numai în raporturile dintre ei (inclusiv în regres) și pentru prejudiciile lor patrimoniale proprii, fără a putea afecta drepturile victimelor ori acoperirea de la art. 36. Alineatul (4) stabilește termene de prescripție de 10 ani de la cunoaștere și de 30 de ani de la faptă, identice cu cele din Legea nr. 703/2001 și justificate de caracterul latent al unor prejudicii; pentru fapta continuă, termenul curge de la încetarea ei. Alineatul (5) a fost rescris pentru compatibilitatea cu regimul armonizat al răspunderii pentru produsele cu defecte (Legea nr. 240/2004 și viitoarea transpunere a Directivei (UE) 2024/2853, care lasă neatinse acțiunile întemeiate pe alte temeiuri decât caracterul defectuos): articolul instituie un temei distinct, întemeiat pe riscul creat prin dezvoltarea și exploatarea sistemului, nu modifică regimul armonizat, nu exclude acțiunea

victimei pe acest regim și interzice dubla reparare. Pentru prejudiciile care intră în domeniul directivei, excluderea apărării întemeiate pe stadiul cunoașterii este o derogare permisă, pentru care Guvernul îndeplinește formalitățile de la art. 18.

Articolul 36 impune asigurarea obligatorie de răspundere civilă sau o garanție financiară echivalentă, cu praguri minime de 100 milioane euro pentru sistemele de categoria I și 1 miliard euro pentru cele de categoria a II-a, și acțiunea directă a victimei împotriva asigurătorului sau a emitentului garanției. Modelul este Legea nr. 703/2001 (asigurarea sau garanția financiară obligatorie a operatorului nuclear) și Legea nr. 132/2017 privind asigurarea obligatorie de răspundere civilă auto (acțiunea directă a persoanei prejudiciate împotriva asigurătorului). Cuantumurile sunt calibrate după capacitatea financiară a dezvoltatorilor de vârf (evaluați la sute de miliarde de dolari) și după amploarea prejudiciilor posibile; sistemele de categoria a III-a nu apar, pentru că nu pot fi puse în exploatare. O cerință imposibil de satisfăcut pe piață ar funcționa însă ca interdicție indirectă. Alineatul (1) prevede că sumele sunt pentru fiecare eveniment, cu un plafon anual agregat de cel puțin dublul lor, iar după epuizare acoperirea se reconstituie în 30 de zile. Clauza de indisponibilitate a pieței: dacă Autoritatea, cu consultarea Autorității de Supraveghere Financiară, constată prin raport public că acoperirea nu poate fi contractată în condițiile legii, Guvernul poate stabili prin norme niveluri inferioare, dar nu sub o cincime din sume, și mecanisme alternative – garanții de grup, garanții bancare ori un fond de garantare finanțat de dezvoltatori și exploatanți; pragul de o cincime și condiția raportului public exclud o reducere discreționară. Alineatul (2) definește garanția financiară: scrisoare de garanție bancară, depozit ori garanție emisă de o instituție financiară autorizată, executabilă la cererea victimei în temeiul hotărârii definitive sau al tranzacției, cu acțiune directă și împotriva emitentului. Obligația de asigurare are și o funcție de reglementare indirectă: asigurătorii vor impune, prin condițiile de subscriere, standarde de siguranță pe care legea nu le poate detalia.

Articolul 37 stabilește contravențiile, structurate în trepte de gravitate, cu amenzi procentuale din cifra de afaceri mondială (1–3%, 2–5%, 3–7%, 5–10%), după modelul art. 99 din Regulamentul privind IA (până la 7%) și al art. 83 din RGPD (până la 4%). Lit. b) a fost completată, cu trimitere precisă la art. 13 alin. (1), alin. (2) teza întâi și teza a treia și alin. (3)–(7), cu obligația de notificare prealabilă a revocării conducătorului funcției de evaluare a siguranței, cu obligațiile de dispunere a suspendării și de comunicare a hotărârii de reexaminare, cu cele privind remunerația personalului funcției de siguranță și verificarea semestrială a funcționării măsurilor de monitorizare, de detectare și de control, cu obligațiile de desemnare și de funcționare a comitetului de supraveghere a siguranței ori de încredințare a atribuțiilor acestuia expertului independent și cu obligațiile de motivare și de comunicare a hotărârii de refuz și de transmitere a raportului prevăzut la art. 13 alin. (5), întrucât trimiterea anterioară, la „separarea funcțiilor", nu le acoperea. Enumerarea e făcută pe obligații denumite, iar nu numai prin trimitere la alineate, fiindcă o normă de localizare nu e o incriminare: la prima redactare, obligația de motivare în scris a refuzului — adică tocmai elementul care asigură ieșirea informației din companie —, obligația privind remunerația și ipoteza expertului independent rămâneseră neacoperite, iar pentru o contravenție de 2–5% din cifra de afaceri mondială acoperirea prin interpretare extensivă este inadmisibilă. Trimiterea cuprinde expres și teza întâi și teza a treia ale alin. (2): prima redactare excludea alineatul în întregul lui, pe ideea că e sancționat prin lit. d), dar lit. d) sancționează numai teza a doua, astfel încât omisiunea

suspendării — fapta cea mai gravă din economia articolului — și obligația de a comunica în 24 de ore hotărârea de reexaminare rămâneau fără nicio sancțiune contravențională. A fost completată totodată cu obligațiile de notificare prevăzute la art. 20 alin. (5) și (6), alături de cea de raportare de la alin. (1), trimiterea fiind făcută punctual la aceste alineate: obligația de a înștiința persoana în al cărei sistem a intrat sistemul de inteligență artificială este distinctă de cea de a raporta Autorității și ar fi rămas, altfel, fără sancțiune contravențională. Lit. b) trimite la art. 16 alin. (1)–(5), iar nu numai la alin. (2)–(5): în forma anterioară, fapta cea mai gravă din materia jurnalizării – aceea de a nu ține și de a nu păstra niciun jurnal, obligație prevăzută la alin. (1) – nu era acoperită de trimiterea textului. Din același motiv, trimiterea din lit. b) a fost precizată la art. 14 alin. (1), (5) și (6), iar alături de testarea capacității de oprire au fost menționate menținerea acesteia și desemnarea persoanelor responsabile de supravegherea umană, prevăzută la art. 14 alin. (3), obligație care nu figura la niciuna dintre literele alineatului. Precizarea nu creează o sancțiune nouă pentru ștergerea capacității de oprire, faptă deja interzisă de art. 28 și sancționată, mai sever, prin lit. d); pentru a evita un concurs de contravenții, lit. b) rezervă expres faptele care intră sub incidența art. 28. Corelativ, lit. d) a fost completată cu încălcarea art. 13 alin. (2) teza a doua, adică înlăturarea de către organul de conducere a unei suspendări impuse de lege, faptă al cărei obiect este tocmai garanția centrală a articolului și care rămăsese fără sancțiune contravențională. Lit. d) a fost completată cu interdicțiile de la art. 14 alin. (2), care, deși formulate ca interdicții de configurație, nu figurau în enumerarea literei și rămâneau, prin argument a contrario, fără sancțiune contravențională. Lit. e) și f) sancționează încălcarea obligațiilor de marcare a conținutului generat, de informare a utilizatorului și privind reprezentantul pentru conformare; pentru faptele care constituie totodată încălcări ale art. 50 din Regulamentul privind IA, lit. e) prevede că amenda se aplică în limitele art. 99 alin. (4) din Regulament, separând expres cele două regimuri. Alineatul (2) diferențiază amenzile fixe după categoria de persoane, din cerința proporționalității: persoanele juridice fără cifră de afaceri, 100.000–10.000.000 lei; persoanele fizice, 10.000–1.000.000 lei; iar pentru faptele de la lit. e) și f) săvârșite de persoane care nu sunt dezvoltatori ori exploatanți ai unui sistem de vârf, 20.000–1.000.000 lei pentru persoanele juridice și 5.000–200.000 lei pentru persoanele fizice. Alineatul (3) prevede sancțiunile complementare, aplicate proporțional cu gravitatea faptei, inclusiv confiscarea ponderilor, sancțiune specifică fără de care amenda ar fi doar un cost de tranzacție; ponderile confiscate se păstrează de Autoritate în condițiile art. 12. Alineatul (4) trimite la regimul general al Ordonanței Guvernului nr. 2/2001, cu două derogări formulate potrivit art. 63 din Legea nr. 24/2000: excluderea posibilității de a plăti jumătate din minimul amenzii (art. 28 din ordonanță), incompatibilă cu amenzile procentuale, și un termen de prescripție de 5 ani în locul celui de 6 luni (art. 13 alin. (1) din ordonanță), justificat de complexitatea constatării. Alineatul (5), nou, cuprinde regulile de individualizare și de corelare: criteriile de individualizare (gravitatea și întinderea faptei, pericolul creat, controlul efectiv asupra faptei, cooperarea și remedierea), baza de calcul (cifra de afaceri din exercițiul financiar precedent, la nivelul grupului), regula potrivit căreia, când aceeași faptă întrunește elementele mai multor contravenții din alin. (1), se aplică o singură sancțiune, cea mai severă — necesară întrucât o aceeași conduită poate cădea deopotrivă sub lit. b), c) și d), iar interdicția anterioară privea numai concursul cu Regulamentul privind IA —, interdicția dublei sancționări pentru aceeași faptă în temeiul legii și al Regulamentului (ne bis in idem) și regimul autorităților și instituțiilor publice, cărora amenda li se aplică persoanei fizice responsabile, în limitele alin.

(2). Contravențiile din prezenta lege nu se suprapun cu cele din Regulamentul privind IA: amenzile prevăzute la art. 101 din Regulament sunt aplicate exclusiv de Comisie, pentru încălcarea obligațiilor din Regulament, în timp ce prezentele contravenții sancționează obligații din lege fără corespondent în Regulament.

Articolul 38 deschide o nouă secțiune, „Încetarea furnizării serviciilor și blocarea accesului", care răspunde unei limite practice a întregului regim: cei mai mulți exploatanți ai sistemelor de vârf nu au sediu, active sau personal în România, astfel încât amenzile procentuale și răspunderea penală a factorilor de decizie pot rămâne fără efect asupra lor. Singura pârghie reală a statului român față de un asemenea exploatant este accesul la utilizatorii de pe teritoriul său. Alineatul (1) gradează neconformitatea, întrucât o lipsă formală remediabilă nu poate atrage aceeași consecință ca un risc grav: punere în întârziere, cu termen de remediere de cel puțin 15 zile și dreptul de a fi ascultat; decizie motivată de constatare numai dacă neconformitatea persistă ori constă într-un risc grav neremediabil în termen; obligația de încetare în 15 zile de la comunicare; în caz de pericol iminent pentru viață, sănătate ori controlul uman, termenul de remediere nu se acordă, urgența fiind motivată. Obligația de încetare nu este o sancțiune, ci consecința firească a faptului că serviciul nu îndeplinește condițiile legale de furnizare, după modelul retragerii de pe piață a produselor neconforme (art. 16 din Regulamentul (UE) 2019/1020 privind supravegherea pieței). Alineatul (2) prevede publicarea deciziei în Lista exploatanților neconformi, instrument de transparență cu dublu rol: informarea utilizatorilor și a furnizorilor de comunicații și publicitatea neconformării, care descurajează integrarea, promovarea și plata serviciului de către profesioniștii de pe piața românească; modelul este lista publică a operatorilor de jocuri de noroc neautorizați ținută de Oficiul Național pentru Jocuri de Noroc potrivit Ordonanței de urgență a Guvernului nr. 77/2009. Alineatul (3) sancționează continuarea furnizării cu amendă de la 100.000 la 10.000.000 euro, în echivalent lei, pentru fiecare lună de continuare, fracțiunile de lună socotindu-se proporțional, stabilită după durată, numărul persoanelor afectate și gravitate, cu plafon de 5% din cifra de afaceri mondială anuală pentru aceeași neconformitate, distinct de sancțiunea pentru încălcarea inițială – criterii care asigură proporționalitatea. Caracterul periodic al amenzii este preluat din instituția penalităților cu titlu cominatoriu prevăzute la art. 24 din Regulamentul (CE) nr. 1/2003 și la art. 76 din Regulamentul (UE) 2022/2065 privind serviciile digitale, și este singurul care asigură eficiența față de un operator cu venituri de miliarde. Cuantumul este exprimat în euro, cu plata în lei la cursul zilei, tehnică admisă de Legea nr. 24/2000 și utilizată în legislația financiară. Alineatul (4) impune Autorității să decidă radierea în 10 zile de la dovada conformării și să o comunice de îndată furnizorilor care execută blocarea, iar refuzul ori întârzierea radierii pot fi contestate potrivit art. 39 alin. (5). Alineatul (5) extinde regimul dezvoltatorului care oferă direct acces, pentru a evita eludarea prin absența unui exploatant distinct.

Articolul 39 reglementează blocarea accesului, ca măsură administrativă provizorie, subsidiară obligației de încetare. Alineatul (1) o condiționează de o decizie motivată a Autorității și o supune testului de necesitate și proporționalitate cerut de art. 53 din Constituție: blocarea se poate dispune numai dacă măsurile mai puțin restrictive nu au condus la conformare ori sunt vădit insuficiente față de gravitatea riscului; decizia examinează necesitatea și proporționalitatea, evită afectarea altor servicii găzduite pe aceeași infrastructură și se

reexaminează din oficiu la fiecare 90 de zile, iar utilizatorii sunt informați, printr-o pagină de redirecționare, asupra motivului măsurii și a căii de contestare. Alineatul (2) o pune în executare prin furnizorii de rețele și servicii de comunicații electronice, în 48 de ore, cu sprijinul tehnic al ANCOM, după mecanismul deja funcțional în dreptul român pentru site-urile de jocuri de noroc neautorizate (Ordonanța de urgență a Guvernului nr. 77/2009) și pentru conținutul ilegal (Legea nr. 365/2002, Regulamentul (UE) 2022/2065). Alineatul (3) asigură proporționalitatea: blocarea privește exclusiv serviciul neconform, nu întreaga activitate a exploatantului, și încetează de drept la radiere. Alineatul (4) este necesar pentru compatibilitatea cu dreptul Uniunii: pentru serviciile furnizate dintr-un alt stat membru, art. 3 alin. (4)–(6) din Directiva 2000/31/CE privind comerțul electronic, transpusă prin Legea nr. 365/2002, permite restrângerea liberei circulații a serviciilor societății informaționale numai printr-o măsură individuală, împotriva unui serviciu determinat, pentru motive de ordine publică, siguranță publică sau protecție a sănătății publice, proporțională, după solicitarea adresată statului membru de origine și cu notificarea Comisiei Europene; potrivit hotărârii Curții de Justiție în cauza C-376/22, Google Ireland și alții (9 noiembrie 2023), statele membre nu pot adopta, în temeiul art. 3 alin. (4), măsuri generale și abstracte. De aceea textul prevede expres caracterul individual al măsurii, serviciul determinat, temeiul material (ordine publică, siguranță publică, sănătate publică) și procedura din Legea nr. 365/2002; blocarea rămâne o măsură de la caz la caz, ulterioară unei încălcări concrete, nu o obligație generală. Alineatul (5) garantează accesul la justiție (art. 21 și 52 din Constituție): contestație în 30 de zile la Curtea de Apel București, secția de contencios administrativ și fiscal, judecată de urgență și cu precădere; contestația nu suspendă de drept executarea, soluție justificată de natura preventivă a măsurii și identică cu cea de la art. 14 alin. (4), dar persoana interesată poate cere suspendarea provizorie, soluționată în cel mult 10 zile, cu punerea în balanță a riscului pentru siguranță și a prejudiciului, iar hotărârea este supusă recursului la Înalta Curte de Casație și Justiție în 15 zile. Alineatul (6) exonerează furnizorii de comunicații de răspundere pentru executarea corectă și cu bună-credință a deciziei, după modelul art. 12–15 din Directiva 2000/31/CE (art. 11 și urm. din Legea nr. 365/2002), dar nu și pentru blocarea excesivă produsă din culpa lor.

Articolul 40 incriminează punerea în exploatare neautorizată și continuarea exploatării după ordinul de oprire, cu închisoare de la 2 la 7 ani (alin. (1)), respectiv de la 5 la 12 ani în forma agravată (alin. (2)). Incriminarea urmează modelul art. 44 și urm. din Legea nr. 111/1996 (desfășurarea fără autorizație a activităților nucleare, pedepsită cu închisoare). Limitele de pedeapsă sunt cele ale infracțiunilor de pericol grav din Codul penal (de exemplu, art. 345 – nerespectarea regimului materialelor nucleare, 3–10 ani). Două precizări sunt impuse de legalitatea incriminării (art. 23 alin. (12) și art. 73 alin. (3) lit. h) din Constituție). Prima delimitează subiectul activ: utilizarea, ca utilizator final, a unui sistem pus la dispoziție de altul nu constituie infracțiune (art. 3 și 43). A doua precizează urmarea agravantă: simpla „manifestare a unei capabilități critice" putea include rezultatul unui test controlat; textul cere manifestarea, în afara unei evaluări controlate, a uneia dintre capabilitățile de la art. 5 alin. (2) lit. c)–e) ori producerea unuia dintre rezultatele de la lit. a) sau b), iar urmarea se impută în condițiile art. 16 alin. (4) din Codul penal (intenție depășită). Legea nu modifică Codul penal, ci instituie infracțiuni în lege specială, potrivit art. 1 alin. (1) din Legea nr. 24/2000 și practicii constante a legislației speciale (Legea nr. 111/1996, Legea nr. 535/2004 privind prevenirea și

combaterea terorismului). Alineatul (2) foloseşte noţiunea de evaluare autorizată în mediu izolat, potrivit art. 15 alin. (2), aceeaşi cu cea din art. 3 alin. (1) lit. n), art. 15 alin. (3) şi art. 20 alin. (2) şi (4); sintagma „evaluare controlată", folosită anterior numai în acest loc, a fost înlăturată, întrucât un termen fără corespondent în restul legii, într-o normă de agravare a pedepsei, ar fi contravenit cerinţei de previzibilitate a legii penale, potrivit art. 23 alin. (12) din Constituţie.

Articolul 41 incriminează falsul în evaluare şi obstrucţionarea controlului. Prezentarea cu ştiinţă, către Autoritate sau către un organism de evaluare, de date, rezultate ori declaraţii false sau incomplete în mod înşelător privind elemente esenţiale ale capabilităţilor, ale volumului de calcul, ale securităţii ponderilor sau ale incidentelor, precum şi configurarea sistemului în scopul de a induce în eroare evaluatorii asupra configuraţiei evaluate ori a capabilităţilor reale (alin. (1), 3–10 ani) este infracţiunea specifică regimului: un sistem de autorizare bazat pe dovezile furnizate de solicitant nu poate funcţiona dacă falsificarea lor este doar o contravenţie. Modelul este, în dreptul comparat, secţiunea 1001 din titlul 18 al Codului Statelor Unite, care pedepseşte cu până la 5 ani declaraţiile false făcute autorităţilor federale. A doua ipoteză răspunde precedentului „Dieselgate" din 2015, în care vehiculele detectau condiţiile de test şi îşi modificau comportamentul, şi capabilităţii critice de la art. 5 alin. (2) lit. d). Cerinţele „cu ştiinţă", „elemente esenţiale" şi „în scopul de a induce în eroare" disting falsificarea deliberată de estimarea incertă şi de eroarea de bună-credinţă, iar alin. (4) exclude expres estimarea incertă declarată ca atare, eroarea corectată de îndată ce a fost cunoscută şi configurarea sistemului în cadrul unui test convenit cu evaluatorul. Obstrucţionarea accesului şi distrugerea jurnalelor (alin. (2), 1–5 ani) urmează modelul art. 275 din Codul penal (sustragerea sau distrugerea de probe ori de înscrisuri), dar „împiedicarea, în orice mod" este raportată la un acces exercitat în limitele competenţei Autorităţii şi pe baza unei solicitări scrise, iar refuzul întemeiat pe lipsa competenţei ori pe secretul profesional al avocatului sau pe alt secret ocrotit de lege nu constituie infracţiune, instanţa pronunţându-se asupra lui. Represaliile împotriva avertizorilor (alin. (3), 6 luni–3 ani sau amendă) sunt definite prin trimitere precisă la măsurile prevăzute de Legea nr. 361/2022 şi condiţionate de legătura cu o semnalare protejată potrivit art. 21; Legea nr. 361/2022 sancţionează represaliile doar contravenţional, ceea ce este insuficient pentru un domeniu în care miza tăcerii unui angajat poate fi de miliarde de euro.

Articolul 42 incriminează dezvoltarea sistemelor interzise. Alineatul (1) sancţionează antrenarea, proiectarea sau operarea cu intenţie a unui sistem în condiţiile interzise de art. 15 alin. (1), art. 25 alin. (2) teza întâi şi alin. (3), art. 28 teza întâi sau art. 29 teza întâi (3–10 ani); trimiterile au fost precizate la nivel de alineat şi de teză, pentru ca norma de incriminare să vizeze numai interdicţiile propriu-zise, potrivit cerinţei de previzibilitate a legii penale. Alineatul (2) sancţionează divulgarea, transmiterea sau punerea la dispoziţie, fără drept, a ponderilor sistemelor de categoria a II-a sau a III-a (5–15 ani), faptă a cărei gravitate se situează între divulgarea informaţiilor secrete de stat (art. 303 din Codul penal) şi trădarea prin transmitere de informaţii secrete de stat (art. 395 din Codul penal, 10–20 de ani); pentru ca elementul „fără drept" să nu depindă de o apărare interpretativă ulterioară, textul prevede expres că transferurile permise potrivit art. 12 alin. (2) şi comunicările protejate potrivit art. 21 alin. (5) nu constituie infracţiune. Alineatul (3) gradează urmările, în locul intervalului unic anterior: pedeapsa de 10–20 de ani, corespunzătoare infracţiunilor contra vieţii, este rezervată morţii,

vătămării corporale grave ori pierderii controlului uman care a făcut imposibilă intervenția umană și a fost urmată de acțiuni autonome cu consecințe asupra persoanelor, mediului ori infrastructurii critice; prejudiciul patrimonial deosebit de grav și pierderea temporară a controlului se pedepsesc cu 7–15 ani; urmările se impută în condițiile art. 16 alin. (4) din Codul penal. Cerința intenției la alin. (1) delimitează infracțiunea de contravenția de la art. 37 alin. (1) lit. d), care sancționează aceleași încălcări săvârșite fără intenție.

Articolul 43 consacră garanția utilizatorului. În forma inițială, proiectul incrimina accesarea, prin eludarea blocării, a unui serviciu înscris în Lista exploatanților neconformi – singura faptă din întregul proiect care putea fi săvârșită de un utilizator. Inițiatorul a renunțat la ea și a înlocuit-o cu o garanție de sens contrar: legea este construită din obligații impuse celor care exercită putere asupra persoanei și din drepturi conferite acesteia (art. 17, 18, 26 și 27); eficacitatea art. 38 și 39 nu depinde de sancționarea utilizatorului, scopul lor fiind scoaterea serviciului neconform din circuitul comercial legal; iar comparația cu OUG nr. 77/2009 este nepotrivită, acolo fiind sancționată o conduită cu potențial de prejudiciu propriu, pe când aici utilizatorul accesează un serviciu pe care exploatantul, nu el, a refuzat să-l conformeze. Alineatul (1) prevede că accesarea de către o persoană fizică, în scop personal, a unui serviciu înscris în Listă, inclusiv prin eludarea blocării, nu constituie infracțiune sau contravenție și nu poate atrage nicio sancțiune ori măsură restrictivă pentru neconformitatea serviciului, răspunderea revenind exclusiv exploatantului și dezvoltatorului; textul precizează că exclusivitatea răspunderii privește neconformitatea serviciului și că garanția nu înlătură răspunderea pentru fapte distincte, prevăzute de lege, săvârșite prin utilizarea serviciului. Alineatul (2) instituie regula de interpretare potrivit căreia art. 38 și 39 nu pot fi citite ca izvor al vreunei obligații în sarcina utilizatorilor ori al condiționării drepturilor acestora. Alineatul (3), nou, extinde garanția la utilizatorul final profesional care nu este exploatant și nu pune serviciul la dispoziția altor persoane. Dispoziția se corelează cu art. 26 alin. (1) și (4) și cu art. 27. Garanția privește accesarea personală, nu întreaga lege: aceeași persoană poate fi și dezvoltator, exploatant ori publicator de material generat, caz în care art. 17–19 și 37 îi devin aplicabile. Întrucât blocarea poate începe înaintea intrării în vigoare a secțiunii penale, art. 50 teza a doua prevede că art. 43 intră în vigoare odată cu legea.

Articolul 44 reglementează răspunderea persoanelor cu funcții de decizie. Alineatul (1) precizează că infracțiunile se reține în sarcina persoanelor fizice care au dispus ori au aprobat săvârșirea faptelor, precum și a celor 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 și independent de răspunderea persoanei juridice, angajată potrivit art. 135 din Codul penal; textul nu creează o formă nouă de participație, ci înlătură apărarea difuzării răspunderii în structuri corporative complexe. Alineatul (2) a fost corectat la 3 octombrie 2026, odată cu definirea organului de conducere: forma de plural „a organelor de conducere", folosită până atunci, devenea ambiguă din momentul în care termenul a primit o definiție legală, astfel încât textul se referă acum la hotărârea organului de conducere, în sensul art. 3 alin. (1) lit. ee), ori a oricărei persoane cu funcție de conducere. Corelativ, art. 13 alin. (7) limitează aplicarea alin. (1) al prezentului articol în privința membrilor comitetului de supraveghere a siguranței și a expertului independent, la faptele pe care aveau posibilitatea efectivă de a le împiedica, pentru ca

obligațiile de organizare instituite la art. 13 alin. (4)–(6) să nu lărgească, pe cale indirectă, cercul persoanelor expuse răspunderii penale. Formula anterioară putea include angajați care știau, dar nu puteau interveni; textul aliniază ipoteza tolerării la condițiile răspunderii pentru omisiune de la art. 17 din Codul penal (obligația legală sau contractuală de a acționa), cu vinovăție stabilită individual. Alineatul (2) exclude cauza de nepedepsire a ordinului superiorului sau al organului de conducere, după modelul art. 33 din Statutul de la Roma și al art. 21 alin. (2) din Codul penal, care nu recunoaște ordinul vădit ilegal drept cauză justificativă, dar păstrează expres cauzele justificative și de neimputabilitate din Codul penal. Legea nu conține o normă proprie privind aplicarea legii penale în spațiu, întrucât art. 8 alin. (4) din Codul penal (infracțiunea se consideră săvârșită pe teritoriul României și atunci când rezultatul s-a produs, chiar în parte, pe acest teritoriu) și art. 9–11 din Codul penal (principiile personalității, realității și universalității) sunt suficiente, iar o normă de trimitere ar constitui un paralelism interzis de art. 16 din Legea nr. 24/2000.

Articolul 45 stabilește competența și măsurile provizorii. Urmărirea penală pentru infracțiunile prevăzute la art. 40–42 revine obligatoriu procurorului din cadrul Direcției de Investigare a Infracțiunilor de Criminalitate Organizată și Terorism (alin. (1)), structură care are deja competența pentru infracțiunile informatice și de terorism (art. 11 din Ordonanța de urgență a Guvernului nr. 78/2016), iar judecata în primă instanță revine tribunalului, potrivit regulii generale de la art. 36 alin. (1) lit. c) din Codul de procedură penală pentru infracțiunile date prin lege în competența sa; trimiterea anterioară la art. 44 a fost eliminată, întrucât acest articol nu definește o infracțiune autonomă, ci persoanele răspunzătoare. Alineatul (2) permite procurorului să dispună, în caz de urgență, prin ordonanță motivată, ca măsură provizorie de cel mult 30 de zile, oprirea sistemului, sigilarea infrastructurii și indisponibilizarea ponderilor, cu confirmarea judecătorului de drepturi și libertăți în 48 de ore, sub sancțiunea încetării de drept a măsurii, după modelul măsurilor asigurătorii de la art. 249 și urm. din Codul de procedură penală și al percheziției informatice de la art. 168. Măsura este însoțită de garanții suplimentare: limitarea la sarcina de calcul și la ponderile vizate atunci când izolarea lor este suficientă, conservarea datelor și paza ponderilor în condițiile art. 12, contestarea de către persoana vizată și terții afectați, reexaminarea la fiecare 30 de zile și prelungirea în aceleași condiții. Confirmarea judiciară rapidă și aceste limite asigură conformitatea cu art. 21 și 53 din Constituție. Alineatul (3) completează art. 11 alin. (1) din Ordonanța de urgență a Guvernului nr. 78/2016 cu infracțiunile prevăzute la art. 40–42, întrucât competența DIICOT se stabilește prin actul său de organizare, care trebuie corelat expres, potrivit Legii nr. 24/2000. Structura exactă a art. 11 alin. (1) din ordonanță trebuie verificată pe textul consolidat înainte de depunere.

Capitolul VIII – Cooperare internațională. Dispoziții tranzitorii și finale (articolele 46–50)

Articolul 46 stabilește obligațiile de acțiune externă ale Guvernului: promovarea în cadrul Uniunii Europene a unui regim de autorizare prealabilă echivalent și a unei capacități europene comune de evaluare (alin. (1)); negocierea, în cadrul ONU, al Consiliului Europei, al NATO și al altor organizații, a unui tratat privind limitarea și verificarea capabilităților de calcul de vârf, interzicerea armelor autonome letale și interzicerea sistemelor de categoria a III-a, cu raportare anuală către Parlament (alin. (2)); și încheierea de acorduri de recunoaștere reciprocă a evaluărilor (alin. (3)). Alineatele (1) și (2) instituie obligații de a iniția și raporta demersuri, nu

de rezultat. Alineatul (3) precizează că acordurile Autorității se încheie în limitele competenței sale, se publică și nu pot deroga de la lege ori de la dreptul Uniunii Europene. Articolul recunoaște deschis, potrivit principiului de la art. 2 lit. g), că legea națională nu poate rezolva singură o problemă globală; el transformă însă această constatare într-o obligație de acțiune, nu într-un motiv de inacțiune. Modelul istoric este Tratatul de neproliferare nucleară din 1968, care a funcționat prin controlul materialelor fisionabile și prin inspecțiile Agenției Internaționale pentru Energie Atomică; echivalentul pentru inteligența artificială este controlul și verificarea calculului, propus în literatura de specialitate sub denumirea de „compute governance" și susținut de Hinton, Bengio și de numeroși cercetători în apelurile publice din 2023–2025.

Articolul 47 instituie clauza de revizuire la 2 ani, pe baza raportului Autorității și a avizului Consiliului științific. Clauza de revizuire periodică este impusă de art. 7 din Legea nr. 24/2000 (evaluarea preliminară a impactului) și de ritmul evoluției tehnologice. 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 chiar dacă riscul general se menține și cuprinde opiniile științifice divergente. Teza finală închide însă o cale de eludare: argumentul că „oricum nu putem controla sistemele, deci reglementarea este inutilă", care ar transforma incertitudinea în permisiune; lipsa unei metode validate de control nu poate fi invocată, singură, ca motiv de relaxare, dar nici nu înlocuiește reevaluarea proporționalității. Legea răspunde că incertitudinea este motivul reglementării, nu al abandonării ei.

Articolul 48 cuprinde dispozițiile tranzitorii, potrivit art. 54 din Legea nr. 24/2000, și așază termenele de conformare pe două trepte, astfel încât nicio obligație să nu devină exigibilă înainte de a exista instrumentul prin care poate fi îndeplinită. Prima treaptă curge de la intrarea în vigoare a legii: în 60 de zile, dezvoltatorii și exploatanții notifică Autorității sistemele aflate în exploatare pe teritoriul României sau puse la dispoziția persoanelor din România (alin. (2)); în 90 de zile se conformează dispozițiilor legii care nu depind de normele metodologice (alin. (1)) și îndeplinesc obligațiile de marcare perceptibilă, de informare a utilizatorilor și de desemnare a reprezentantului pentru conformare (alin. (4)), iar dispozițiile privind încetarea furnizării și blocarea (art. 38 și 39) se aplică numai după expirarea acestui termen (alin. (3)), ceea ce garantează previzibilitatea pentru exploatanți și respectă art. 15 alin. (2) din Constituție. A doua treaptă curge de la intrarea în vigoare a normelor metodologice prevăzute la art. 49 alin. (2): în 90 de zile de la această dată se depune cererea de autorizare, a cărei procedură este stabilită prin norme (alin. (2)), se realizează marcajul tehnic încorporat (alin. (4)) și devin exigibile, în general, toate obligațiile a căror îndeplinire depinde de standardele, procedurile, pragurile ori cuantumurile stabilite prin norme, contravențiile corespunzătoare neputând fi constatate până atunci (alin. (5)). Alineatul (5) precizează în același timp că interdicțiile legii, obligațiile privind capacitatea de oprire, jurnalizarea și raportarea incidentelor grave, precum și celelalte obligații care pot fi îndeplinite fără norme se aplică de la intrarea în vigoare a legii; regimul tranzitoriu nu amână, așadar, nimic din ceea ce protejează direct controlul uman. Sistemele notificate pot fi menținute în exploatare până la decizia Autorității, dar nu mai mult de 12 luni de la intrarea în vigoare a legii, sub condiția respectării interdicțiilor și a garanțiilor direct aplicabile din cap. IV și V (nu a întregului capitol IV, care cuprinde și obligații dependente de norme); se evită astfel atât vidul de aplicare, cât și întreruperea bruscă a unor

servicii utilizate de milioane de persoane, dar se fixează o limită absolută a toleranței. Aceasta se prelungește de drept cu durata cu care adoptarea normelor ori soluționarea cererii depășesc termenele legale, solicitantul diligent neputând fi sancționat pentru întârzierea instituțiilor, iar Autoritatea putând dispune, motivat, condiții suplimentare de siguranță pe durata prelungirii. Termenul de 90 de zile este cel uzual în legislația română pentru conformarea la noi cerințe de autorizare și este suficient, întrucât dezvoltatorii de vârf dispun deja de evaluările interne cerute de Regulamentul privind IA. Alineatul (6) încredințează președintelui ANCOM, până la numirea vicepreședintelui pentru siguranța inteligenței artificiale, exercitarea atribuțiilor Autorității, inclusiv a măsurilor urgente de la art. 32 alin. (1) lit. c); forma anterioară limita interimatul la primirea notificărilor. Alineatul (3) cuprinde și o corelare fără de care regimul tranzitoriu ar fi fost contradictoriu: menținerea în exploatare a unui sistem notificat, pe durata în care alin. (2) o permite și în cursul soluționării cererii depuse în termen, nu constituie infracțiunea prevăzută la art. 40 alin. (1). În lipsa acestei precizări, aceeași conduită ar fi fost, între a 270-a zi de la publicare – data intrării în vigoare a dispozițiilor penale – și împlinirea celor 12 luni de la intrarea în vigoare a legii, în același timp permisă de dispoziția tranzitorie și incriminată de dispoziția penală. Excluderea este strict delimitată: nu acoperă punerea în exploatare a unui sistem nenotificat, menținerea în exploatare după respingerea cererii, după expirarea termenului prevăzut la alin. (2) ori după comunicarea unui ordin de oprire. Alineatul (4) a fost, la rândul său, defalcat pe componentele marcajului de proveniență: obligația prevăzută la art. 17 alin. (4) în sarcina autorităților publice privește marcajul definit la alin. (1), alcătuit atât din marcajul perceptibil, cât și din cel tehnic încorporat, astfel încât fiecare componentă urmează termenul propriu, iar autoritatea publică nu este ținută să aplice un marcaj al cărui standard nu a fost încă adoptat.

Articolul 49 prevede măsurile de organizare și normele de aplicare, cu termene raportate la data publicării legii, pentru a rezulta un calendar unic și pentru ca instituția și regulile de evaluare să fie disponibile înaintea termenelor operatorilor. Alineatul (1) prevede numirea de către Parlament a vicepreședintelui pentru siguranța inteligenței artificiale și completarea structurii organizatorice și a regulamentului de organizare și funcționare ale ANCOM cu Autoritatea, prin decizie a președintelui ANCOM publicată în Monitorul Oficial, în 60 de zile de la publicare. Alineatul (2) prevede adoptarea normelor metodologice în 120 de zile de la publicare, la propunerea Autorității, cu avizul Consiliului științific și după o consultare publică de cel puțin 30 de zile, cu enumerarea precisă a obiectului lor (proceduri, standarde, condițiile mediului izolat, marcajul de proveniență, metodele de evaluare și nivelurile de semnificație ale capabilităților critice, pragul infrastructurii, taxele stabilite în raport cu costul serviciului și cuantumul asigurării ori al garanției). Delegarea către Guvern este limitată la aspecte tehnice și de procedură, în acord cu jurisprudența Curții Constituționale potrivit căreia elementele esențiale ale reglementării trebuie stabilite prin lege (de exemplu, Decizia nr. 51/2016); textul o spune expres: normele detaliază cadrul stabilit prin lege, nu pot stabili conținutul esențial al obligațiilor, al interdicțiilor și al sancțiunilor, iar standardele se publică. Lista capabilităților critice nu mai figurează printre obiectele normelor, întrucât rămâne în lege (art. 5 alin. (2)), corelat cu art. 32 alin. (4). Teza finală a alineatului, adăugată la 3 octombrie 2026, fixează momentul de la care curge a doua treaptă a calendarului de la art. 48: normele se publică în Monitorul Oficial în 5 zile de la adoptare și intră în vigoare la data publicării. Până atunci, art.

49 alin. (2) prevedea numai adoptarea, iar art. 48 alin. (2), (4) şi (5) făceau să curgă termenele de la intrarea în vigoare a normelor, moment pe care legea nu îl determina; întregul termen de exigibilitate al obligaţiilor dependente de norme rămânea, astfel, la discreţia Guvernului. Corelativ, la art. 48 alin. (2) prelungirea de drept a toleranţei priveşte acum durata cu care adoptarea „ori publicarea" normelor depăşeşte termenele legale. Alineatul (3), nou, instituie regimul intermediar: până la adoptarea normelor, evaluările se efectuează potrivit standardelor din codurile de bună practică adoptate în temeiul Regulamentului privind IA şi metodelor recunoscute ştiinţific, iar Autoritatea publică orientări provizorii. Enumerarea obiectului normelor a fost completată cu nivelul prevăzut la art. 16 alin. (5), cu procedura de testare şi durata prevăzute la art. 14 alin. (1) şi (6), cu cerinţele minime ale izolării prevăzute la art. 3 alin. (1) lit. bb) şi cu cuantumul indemnizaţiei compensatorii prevăzute la art. 31 alin. (3), precum şi cu forma şi modalitatea de transmitere a raportului prevăzut la art. 13 alin. (5) şi cu onorariul expertului independent prevăzut la art. 13 alin. (6) — conţinutul raportului rămânând stabilit de lege, potrivit tezei finale a prezentului alineat, pentru ca fiecare element lăsat normelor metodologice de un alt articol al legii să figureze şi în articolul care instituie delegarea.

Articolul 50 stabileşte intrarea în vigoare la 30 de zile de la publicare, potrivit art. 78 din Constituţie şi art. 12 din Legea nr. 24/2000, cu excepţia art. 40–42, 44 şi 45, care intră în vigoare la 270 de zile de la publicare, şi cu precizarea că art. 43 intră în vigoare odată cu legea. Termenul secţiunii penale este exprimat în zile de la publicare, nu în luni calendaristice, şi a fost prelungit de la 6 luni la 270 de zile, pentru ca incriminările să devină active numai după normele metodologice (120 de zile) şi după perioada de adaptare a obligaţiilor dependente de ele (210 zile): o incriminare legată de autorizare presupune o procedură de autorizare disponibilă, iar activarea ei înaintea normelor ar fi contrară previzibilităţii legii penale (art. 7 din Convenţia europeană a drepturilor omului, art. 23 alin. (12) din Constituţie). Formula finală de atestare a adoptării, prevăzută la art. 40 şi 46 din Legea nr. 24/2000, indică respectarea art. 75 şi art. 76 alin. (1) din Constituţie, legea fiind organică întrucât reglementează infracţiuni şi pedepse (art. 73 alin. (3) lit. h)) şi modifică, prin derogare, organizarea unei autorităţi administrative autonome înfiinţate prin lege organică (art. 117 alin. (3)).

Calendarul unic care rezultă din art. 48–50, raportat la data publicării legii (P), este următorul: P+30 de zile – intrarea în vigoare, inclusiv garanţia utilizatorului (art. 43), interdicţiile şi obligaţiile direct aplicabile; P+60 de zile – numirea vicepreşedintelui şi organizarea Autorităţii (art. 49 alin. (1)); P+90 de zile – notificarea sistemelor aflate în exploatare (art. 48 alin. (2)); P+120 de zile – adoptarea normelor metodologice (art. 49 alin. (2)) şi exigibilitatea obligaţiilor independente de norme (art. 48 alin. (1) şi (4)), moment de la care devin aplicabile şi art. 38 şi 39; P+210 zile – dacă normele sunt adoptate şi publicate la termen, art. 49 alin. (2) prevăzând acum expres publicarea în 5 zile de la adoptare şi intrarea în vigoare la data publicării, exigibilitatea obligaţiilor dependente de norme, marcajul tehnic încorporat şi cererile de autorizare (art. 48 alin. (2), (4) şi (5)); P+270 de zile – intrarea în vigoare a secţiunii penale (art. 40–42, 44 şi 45); toleranţa pentru sistemele notificate expiră la 12 luni de la intrarea în vigoare, prelungită de drept cu întârzierea instituţiilor (art. 48 alin. (2)).

3. Conformitatea cu normele de tehnică legislativă (Legea nr. 24/2000)

Proiectul a fost redactat cu respectarea strictă a Legii nr. 24/2000, republicată, după cum urmează. Fundamentarea și evaluarea preliminară a impactului (art. 6, 7 și 30–31) sunt cuprinse în prezenta expunere de motive, cu analiza situației actuale, a modelelor comparate și a efectelor. Integrarea în sistemul legislativ (art. 13) este asigurată prin raportarea expresă la Regulamentul privind IA (art. 1 alin. (3) din lege) și prin normele de trimitere la actele conexe. Evitarea paralelismelor (art. 16) a făcut obiectul unei analize distincte, prezentată la pct. 3 din Secțiunea a 5-a: nicio reglementare existentă nu este reluată, ci este preluată prin trimitere, iar derogările sunt formulate expres cu formula „prin derogare de la", potrivit art. 63. Unitatea terminologică (art. 37) este asigurată prin definițiile de la art. 3, care preiau prin trimitere noțiunile consacrate de dreptul Uniunii și definesc autonom, cu justificare, noțiunile noi („sistem de vârf", „ponderi", „exploatant", „punere în exploatare"), evitând termenii cu înțeles diferit în Regulamentul privind IA („operator", „furnizor", „punere în funcțiune"). Stilul normativ (art. 36 și 38) este dispozitiv, la timpul prezent, fără explicații între paranteze și fără neologisme neconsacrate; toți termenii tehnici utilizați în partea dispozitivă („ponderi", „arhitectură", „antrenare", „ajustare fină", „învățare prin consolidare", „exfiltrare", „replicare autonomă", „autoîmbunătățire recursivă", „disimularea capabilităților", „sustragerea de la supraveghere", „rezistența la oprire", „instrument extern", „mediu autorizat de exploatare" și celelalte) sunt definiți la art. 3, structurat în două alineate – noțiuni-obiect și, respectiv, operațiuni și comportamente – pentru ca elementul material al interdicțiilor și al infracțiunilor să aibă un conținut normativ precis. Părțile constitutive (art. 40–46) sunt: titlul, preambulul (permis de art. 43 pentru a enunța sintetic motivarea, pe modelul legilor de importanță deosebită), formula introductivă, partea dispozitivă și formula de atestare a legalității adoptării. Structura părții dispozitive (art. 47–56) respectă ordinea dispoziții generale – dispoziții de fond – dispoziții tranzitorii – dispoziții finale, cu capitole numerotate cu cifre romane și secțiuni cu cifre arabe; articolele sunt numerotate continuu, alineatele cu cifre arabe între paranteze, enumerările cu litere, iar nicio enumerare marcată cu literă nu cuprinde o altă enumerare (art. 49 alin. (3)); articolele nu poartă denumiri marginale, întrucât art. 47 alin. (3) le rezervă codurilor și legilor de mare întindere. Normele de trimitere (art. 50) indică elementele complete de identificare ale actelor la care se face trimitere, iar delegările către Guvern (art. 49) sunt limitate la aspecte de procedură și tehnice, art. 49 alin. (2) teza finală din lege interzicând expres normelor metodologice să stabilească conținutul esențial al obligațiilor, al interdicțiilor și al sancțiunilor. Legea cuprinde o singură intervenție expresă asupra textului unui alt act normativ – completarea art. 11 alin. (1) din Ordonanța de urgență a Guvernului nr. 78/2016, dispusă prin art. 45 alin. (3) –, redactată potrivit art. 59–62 (identificarea completă a actului, cu datele de publicare și de aprobare, și formula de completare); derogările punctuale sunt permise de art. 63 și nu afectează textul actelor de la care se derogă. În urma analizei juridice independente din 20 septembrie 2026, proiectul a fost revizuit pentru: (i) delimitarea domeniului său față de Regulamentul privind IA (art. 1 alin. (4), art. 9 alin. (7), art. 17 alin. (6), art. 19 alin. (1) și art. 27 alin. (6)); (ii) păstrarea în lege a tuturor elementelor constitutive ale contravențiilor și infracțiunilor, cu interdicția extinderii lor prin standarde (art. 32 alin. (4)); (iii) sincronizarea procedurilor, a standardelor și a termenelor printr-un calendar unic raportat la data publicării (art. 48–50); (iv) adăugarea garanțiilor procedurale față de Autoritate (art. 9 alin. (4), art. 11 alin. (2), art. 14 alin. (4), art. 32 alin. (2)–(3), art. 39 alin. (1) și (5), art. 45 alin. (2)). Exemplarul

de lucru al proiectului poartă mențiunea „PROIECT"; formula de atestare a legalității adoptării, înscrisă la sfârșitul textului, este cea uzuală pentru un proiect de lege și nu reprezintă o adoptare deja produsă.

Secțiunea a 3-a – Impactul socioeconomic al proiectului de act normativ

1. Impactul macroeconomic	Limitat și indirect. Regimul de autorizare vizează un număr foarte restrâns de operatori economici (dezvoltatorii sistemelor care depășesc 10^{25} operații în virgulă mobilă – în prezent, sub douăzeci la nivel mondial, niciunul cu sediul în România – și furnizorii de infrastructură de calcul de mare capacitate). Sistemele sub prag și aplicațiile dezvoltate pe baza modelelor existente nu sunt supuse autorizării. Pe termen mediu, existența unui cadru clar și a unei autorități competente constituie un avantaj de localizare pentru investițiile în centre de date, prin predictibilitate, și reduce riscul macroeconomic sistemic asociat unui incident major.
1^1. Impactul asupra mediului concurențial și domeniului ajutoarelor de stat	Neutru. Obligațiile se aplică nediscriminatoriu tuturor dezvoltatorilor și exploatanților care intră sub incidența legii, indiferent de naționalitate, iar procedura simplificată de recunoaștere (art. 9 alin. (7)) asigură compatibilitatea cu libera circulație a serviciilor. Nu se instituie ajutoare de stat. Finanțarea cercetării în siguranța inteligenței artificiale (art. 32 alin. (1) lit. j)) din alocarea bugetară distinctă prevăzută la art. 33 alin. (5), fără legătură cu sancțiunile aplicate, se face cu respectarea Regulamentului (UE) nr. 651/2014 (exceptări pe categorii pentru cercetare-dezvoltare).
2. Impactul asupra mediului de afaceri	Pentru întreprinderile mici și mijlocii: niciun impact direct (art. 4 alin. (2)); ele rămân însă beneficiare ale serviciilor de vârf și pot fi afectate indirect de o eventuală încetare a furnizării sau blocare a unui serviciu neconform (art. 38–39), motiv pentru care legea prevede termenul de conformare de 90 de zile și menținerea în exploatare până la decizia Autorității (art. 48). Pentru furnizorii de infrastructură de calcul: obligații de înregistrare, de cunoaștere a clientelei și de raportare, comparabile cu cele din legislația privind prevenirea spălării banilor, cu costuri administrative reduse. Pentru dezvoltatorii de vârf: costurile evaluării independente și ale asigurării obligatorii, proporționale cu valoarea investițiilor (de ordinul sutelor de milioane de euro pentru un singur ciclu de antrenare) și cu amploarea riscului.
3. Impactul social	Pozitiv. Legea protejează viața, sănătatea, libertatea și demnitatea persoanei împotriva unei categorii de riscuri neacoperite de legislația în vigoare, instituie protecția avertizorilor de integritate din laboratoare și garantează

	repararea prejudiciilor prin răspundere obiectivă şi asigurare obligatorie. Clauzele de umanitate (cap. V) protejează procesele democratice şi controlul uman asupra deciziilor letale.
4. Impactul asupra mediului	Indirect pozitiv. Notificarea şi evidenţa infrastructurii de calcul de mare capacitate (art. 7 alin. (3) şi art. 22), cu consum energetic semnificativ, permit corelarea cu politicile energetice şi de mediu.
5. Alte informaţii	Legea contribuie la îndeplinirea obligaţiilor asumate de România prin Convenţia-cadru a Consiliului Europei privind inteligenţa artificială şi drepturile omului, democraţia şi statul de drept (CETS nr. 225) şi prin Rezoluţia Adunării Generale a ONU 78/241 privind sistemele de arme autonome letale.

Secţiunea a 4-a – Impactul financiar asupra bugetului general consolidat, atât pe termen scurt, pentru anul curent, cât şi pe termen lung (5 ani)

Impactul financiar constă în cheltuielile de organizare şi funcţionare ale Autorităţii pentru Siguranţa Inteligenţei Artificiale, în cadrul ANCOM, estimate pentru un efectiv de circa 80 de posturi, dintre care cel puţin 50 de specialişti tehnici recrutaţi prin concurs şi remuneraţi la nivelul pieţei, şi în cheltuielile cu infrastructura de calcul necesară evaluărilor. Organizarea în cadrul ANCOM, autoritate finanţată integral din venituri proprii, reduce costurile de înfiinţare (sediu, funcţii-suport, sisteme informatice) şi nu grevează bugetul de stat. Potrivit art. 33 alin. (5), Autoritatea se finanţează din bugetul ANCOM, printr-o alocare distinctă, aprobată anual şi evidenţiată separat, şi din taxele de notificare, de evaluare şi de autorizare, stabilite prin normele metodologice în raport cu costul serviciului prestat; bugetul iniţial, inclusiv personalul şi infrastructura, se asigură de ANCOM înainte de încasarea taxelor. Amenzile aplicate potrivit legii se fac venit la bugetul de stat şi nu pot determina resursele Autorităţii, iar cercetarea prevăzută la art. 32 alin. (1) lit. j) se finanţează prin alocare bugetară distinctă, fără legătură cu sancţiunile; veniturile din amenzi nu pot fi estimate ex ante şi nu sunt luate în calcul mai jos. Estimările, exprimate în milioane lei, sunt orientative şi urmează a fi definitivate de Ministerul Finanţelor la avizare.

Indicatori	**Anul curent (2027)**	**2028**	**2029**	**2030**	**2031**	**Media pe 5 ani**
1. Modificări ale veniturilor bugetare, plus/minus, din care:	+5	+10	+15	+20	+20	+14
a) buget de stat, din acesta: taxe de notificare, evaluare şi autorizare, stabilite în raport cu costul serviciului	+5	+10	+15	+20	+20	+14

Indicatori	Anul curent (2027)	2028	2029	2030	2031	Media pe 5 ani
(venituri proprii ale ANCOM, alocate Autorității); amenzile se fac venit la bugetul de stat (art. 33 alin. (5)), neestimabile ex ante și neincluse						
b) bugete locale	–	–	–	–	–	–
c) bugetul asigurărilor sociale de stat	–	–	–	–	–	–
2. Modificări ale cheltuielilor bugetare, plus/minus, din care:	+45	+85	+90	+95	+100	+83
a) buget de stat, din acesta: (i) cheltuieli de personal	+20	+40	+42	+45	+48	+39
(ii) bunuri și servicii (inclusiv infrastructură de calcul pentru evaluări)	+20	+40	+43	+45	+47	+39
(iii) cheltuieli de capital	+5	+5	+5	+5	+5	+5
b) bugete locale	–	–	–	–	–	–
c) bugetul asigurărilor sociale de stat	–	–	–	–	–	–
3. Impact financiar, plus/minus (milioane lei)	–40	–75	–75	–75	–80	–69
4. Propuneri pentru acoperirea creșterii cheltuielilor bugetare	Cheltuielile se acoperă din bugetul ANCOM, prin alocarea distinctă prevăzută la art. 33 alin. (5) – inclusiv bugetul inițial asigurat de ANCOM înainte de încasarea taxelor –, și din taxele stabilite în raport cu costul serviciului; amenzile, făcute venit la bugetul de stat, nu constituie sursă de finanțare a Autorității. Se propune, în completare, redirecționarea unei părți din fondurile alocate Strategiei naționale în domeniul inteligenței artificiale 2024–2027 și din Programul Operațional Creștere Inteligentă, Digitalizare și Instrumente Financiare 2021–2027 (obiectivul de politică 1 – o Europă mai inteligentă).					
5. Propuneri pentru a compensa reducerea veniturilor bugetare	Nu este cazul; proiectul nu reduce venituri bugetare.					

Indicatori	Anul curent (2027)	2028	2029	2030	2031	Media pe 5 ani
6. Calcule detaliate privind fundamentarea modificărilor veniturilor și/sau cheltuielilor bugetare	Cheltuieli de personal: 80 de posturi, cost mediu brut estimat de 40.000 lei/lună pentru personalul tehnic (50 de posturi) și 15.000 lei/lună pentru restul, în regim de derogare salarială. Bunuri și servicii: închirierea de capacitate de calcul pentru evaluări (estimativ 25 milioane lei/an), contracte cu organisme de evaluare independente, deplasări internaționale. Venituri: taxe de notificare, evaluare și autorizare estimate la 1–3 milioane lei pe sistem, pentru 5–10 sisteme pe an, plafonate de art. 33 alin. (5) la costul serviciului prestat; veniturile din amenzi revin bugetului de stat, depind de numărul și gravitatea încălcărilor constatate și nu pot fi estimate ex ante, astfel încât nu au fost incluse.					
7. Alte informații	Valorile sunt exprimate în milioane lei. Costul unui singur incident major evitat (de exemplu, un atac cibernetic autonom asupra infrastructurii energetice) depășește cu mai multe ordine de mărime costul anual al Autorității.					

Secțiunea a 5-a – Efectele prezentului act normativ asupra legislației în vigoare

a) acte normative în vigoare ce vor fi modificate sau abrogate, ca urmare a intrării în vigoare a proiectului de act normativ

Proiectul nu abrogă niciun act normativ și modifică expres, printr-o completare, un singur act normativ (art. 45 alin. (3)). În rest, prin tehnica normei de trimitere și a derogării exprese, el produce următoarele efecte asupra legislației în vigoare:

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, aprobată cu modificări prin Legea nr. 120/2018 – completare expresă (art. 45 alin. (3) din lege): la art. 11 alin. (1) se introduce un nou punct, prin care infracțiunile prevăzute la art. 40–42 din lege sunt date în competența DIICOT; 1 act completat în text. Structura exactă a art. 11 alin. (1) (numerotarea punctelor și forma consolidată la zi) urmează a fi verificată pe textul consolidat înainte de depunere, iar formula de completare va fi adaptată în consecință.

Ordonanța de urgență a Guvernului nr. 27/2003 privind procedura aprobării tacite – derogare expresă (art. 9 alin. (4) din lege): lipsa răspunsului Autorității nu echivalează cu autorizarea tacită; 1 derogare.

Ordonanța de urgență a Guvernului nr. 22/2009 privind înființarea Autorității Naționale pentru Administrare și Reglementare în Comunicații, aprobată prin Legea nr. 113/2010 – derogare expresă (art. 31 alin. (2) din lege) de la art. 11 alin. (1): un vicepreședinte suplimentar,

pentru siguranța inteligenței artificiale, numit de Parlament în aceleași condiții; 1 derogare. Legea-cadru nr. 153/2017 nu este afectată, personalul ANCOM fiind exceptat de la aplicarea ei prin art. 2 alin. (2) al acesteia.

Legea contenciosului administrativ nr. 554/2004 – derogare expresă (art. 26 alin. (6) din lege) de la art. 7 (procedura prealabilă), art. 10 (competența materială și teritorială) și art. 20 (calea de atac): contestațiile împotriva deciziilor autorităților și instituțiilor publice prevăzute la art. 26 și, prin trimitere, la art. 18 alin. (3) și art. 27 alin. (5), nu sunt supuse procedurii prealabile, se judecă de tribunalul de la domiciliul persoanei, cu apel la curtea de apel; 1 derogare (de la trei texte).

Ordonanța Guvernului nr. 2/2001 privind regimul juridic al contravențiilor – derogări exprese (art. 37 alin. (4) din lege) de la art. 28 (plata a jumătate din minimul amenzii) și de la art. 13 alin. (1) (termenul de prescripție a aplicării sancțiunii); 2 derogări.

Legea nr. 361/2022 privind protecția avertizorilor în interes public – completare a domeniului de aplicare prin normă de trimitere (art. 21 din lege), fără modificarea textului; regimul de protecție se extinde la semnalările privind riscurile pentru siguranță și disimularea capabilităților.

Regulamentul (UE) 2016/679 (art. 22) și Legea nr. 190/2018 – norme de trimitere (art. 26 alin. (8) din lege), fără modificare.

Regulamentul (UE) 2022/2065 privind serviciile digitale – normă de coordonare (art. 27 alin. (6) din lege): pentru furnizorii de servicii intermediare, art. 27 se aplică numai în măsura compatibilă cu regulamentul, ale cărui dispoziții privind condițiile contractuale (art. 14), motivarea deciziilor (art. 17) și soluționarea contestațiilor (art. 20) rămân aplicabile; nicio garanție a regulamentului pentru destinatarii serviciilor nu este restrânsă; fără modificare.

Regulamentul (UE) 2024/1689 – norme de coordonare: art. 1 alin. (4) și art. 9 alin. (7) din lege (legea nu instituie condiții de introducere pe piața Uniunii a modelelor de uz general și nu aduce atingere competențelor Comisiei prevăzute la art. 88 din regulament; pentru modelele cu risc sistemic ai căror furnizori respectă cap. V din regulament, Autoritatea se întemeiază pe documentația comunicată Oficiului pentru IA); art. 17 alin. (6) (pentru furnizorii și implementatorii cărora li se aplică art. 50 din regulament, obligațiile de marcare se consideră îndeplinite prin respectarea art. 50 alin. (2) și (4), legea stabilind numai autoritatea competentă, procedura de constatare și sancțiunile, în limitele art. 99 alin. (4) din regulament); art. 18 alin. (5) (art. 50 alin. (1) din regulament și art. 13–15 și 22 din Regulamentul (UE) 2016/679); art. 19 alin. (1) și (6) (dezvoltatorii și exploatanții stabiliți în alt stat membru desemnează numai un punct de contact, care poate fi reprezentantul autorizat prevăzut la art. 54 din regulament ori reprezentantul legal prevăzut la art. 13 din Regulamentul (UE) 2022/2065; reprezentantul autorizat împuternicit și pentru România îndeplinește obligația din lege); fără modificarea actelor Uniunii.

Directiva 2000/31/CE (art. 3) și Legea nr. 365/2002 privind comerțul electronic, republicată – norme de trimitere (art. 4 alin. (4) și art. 39 alin. (4) din lege): obligațiile legii se aplică serviciilor furnizate din alt stat membru în condițiile art. 3 din directivă, iar blocarea unui asemenea serviciu se dispune numai individual, pentru un serviciu determinat, cu procedura de solicitare a statului membru de origine și de notificare a Comisiei Europene; fără modificare.

Directiva (UE) 2024/2853 privind răspunderea pentru produsele cu defecte – normă de coordonare (art. 35 alin. (5) din lege): răspunderea obiectivă instituită de lege este un temei distinct, care nu modifică regimul armonizat al răspunderii pentru produse; în măsura în care excluderea forței majore pentru lipsa cunoașterii științifice intră în domeniul directivei, Guvernul îndeplinește formalitățile prevăzute la art. 18 din directivă (derogarea privind riscul de dezvoltare).

Directiva (UE) 2015/1535 referitoare la procedura de furnizare de informații în domeniul reglementărilor tehnice și al normelor privind serviciile societății informaționale, transpusă prin Hotărârea Guvernului nr. 1016/2004 – de verificat înainte de depunere: dispozițiile art. 17–19, 38 și 39 din lege, precum și normele metodologice privind marcajul tehnic, sunt susceptibile a constitui „reglementări referitoare la servicii" în sensul directivei, caz în care proiectul se notifică Comisiei Europene în stadiu de proiect, cu respectarea perioadei de așteptare; nota privind notificările europene însoțește proiectul.

Codul civil (art. 1376), Codul penal (art. 16 alin. (4), art. 135), Codul de procedură penală (art. 36, 168, 249), Codul de procedură civilă (procedura contencioasă, art. 23 alin. (2) și art. 26 alin. (5) din lege), Legea nr. 182/2002, Ordonanța de urgență a Guvernului nr. 155/2024, Legea nr. 240/2004 – norme de trimitere, fără modificare.

În sinteză: 0 acte abrogate, 1 act completat în text (OUG nr. 78/2016), 5 derogări exprese (de la 7 texte), 2 completări de domeniu prin normă de trimitere (Legea nr. 361/2022, Legea nr. 365/2002), norme de coordonare cu dreptul Uniunii la art. 1 alin. (4), art. 9 alin. (7), art. 17 alin. (6), art. 18 alin. (5), art. 19 alin. (1) și (6), art. 27 alin. (6) și art. 35 alin. (5); 1 notificare europeană de verificat (Directiva (UE) 2015/1535). Corelările cu formele consolidate ale actelor naționale citate (Codurile, legile nr. 182/2002, 365/2002, 554/2004 și 361/2022, OG nr. 2/2001, OUG nr. 22/2009, 78/2016 și 155/2024) se verifică pe textele consolidate înainte de depunere.

b) acte normative ce urmează a fi elaborate în urma implementării noilor dispoziții

Hotărâre a Parlamentului pentru numirea vicepreședintelui ANCOM pentru siguranța inteligenței artificiale și decizie a președintelui ANCOM, publicată în Monitorul Oficial, pentru completarea structurii organizatorice și a regulamentului de organizare și funcționare cu Autoritatea, inclusiv organizarea structurilor distincte de evaluare, de investigare și de decizie sancționatorie (art. 32 alin. (2)); termen: 60 de zile de la publicarea legii (art. 49 alin. (1)).

Hotărâre a Guvernului pentru aprobarea Normelor metodologice de aplicare a legii, adoptată la propunerea Autorității, cu avizul Consiliului științific și după o consultare publică de cel puțin 30 de zile; termen: 120 de zile de la publicarea legii (art. 49 alin. (2)). Obiect: procedura de notificare și autorizare; procedura simplificată de recunoaștere a sistemelor puse legal în exploatare în alt stat membru (art. 9 alin. (7)); standardele de evaluare, de securitate a ponderilor și de capacitate de oprire; condițiile mediului izolat (art. 15 alin. (2)); standardele marcajului de proveniență (art. 17); metodele de evaluare și nivelurile de semnificație ale capabilităților critice, în limitele art. 5 alin. (2), fără a putea adăuga alte categorii de rezultate; pragul infrastructurii de calcul de mare capacitate (art. 6 alin. (4)); cuantumul taxelor, stabilit în raport cu costul serviciului; cuantumul asigurării ori al garanției financiare (art. 36);

procedura de verificare a personalului cu acces la ponderi, cu avizul ORNISS (art. 12 alin. (1)); procedura de testare a capacității de oprire (art. 14 alin. (1)); nivelul de la care se constată pierderea inteligibilității jurnalelor (art. 16 alin. (5)); indemnizația compensatorie a vicepreşedintelui (art. 31 alin. (3)). Normele detaliază cadrul legii şi nu pot stabili conținutul esențial al obligațiilor, al interdicțiilor şi al sancțiunilor; standardele se publică.

Orientări provizorii ale Autorității, publicate până la adoptarea normelor metodologice, evaluările efectuându-se în acest interval potrivit codurilor de bună practică adoptate în temeiul Regulamentului privind IA şi metodelor recunoscute ştiinţific (art. 49 alin. (3)); ulterior, standardele Autorității, avizate de Consiliul ştiinţific, în limitele art. 32 alin. (4).

Decizie a preşedintelui ANCOM privind nivelul de remunerare a personalului de specialitate al Autorității, pe baza studiului de piață publicat (art. 33 alin. (3)); anunțul şi regulamentul concursului pentru personalul de specialitate (art. 33 alin. (1) şi (2)).

Hotărâre a Consiliului Suprem de Apărare a Țării privind adaptările aplicabile sistemelor din domeniul apărării şi securității naționale (art. 23).

Hotărâri ale Guvernului de ajustare periodică a pragului de calcul, la propunerea Autorității (art. 6 alin. (2)).

Legea de aplicare a Regulamentului (UE) 2024/1689, aflată în curs de elaborare de Guvern, va trebui corelată cu prezenta lege în privința cooperării dintre autoritățile desemnate şi Autoritate (art. 31 alin. (5)) şi a regulii potrivit căreia pentru aceeaşi faptă nu se pot aplica două sancțiuni în temeiul legii şi al Regulamentului (art. 37 alin. (5)).

c) Analiza paralelismelor legislative (art. 16 din Legea nr. 24/2000)

Potrivit art. 16 alin. (1) din Legea nr. 24/2000, „în procesul de legiferare este interzisă instituirea aceloraşi reglementări în mai multe articole sau alineate din acelaşi act normativ ori în două sau mai multe acte normative", iar pentru sublinierea conexiunilor legislative se utilizează norma de trimitere. Fiecare dispoziție a proiectului a fost verificată în raport cu legislația în vigoare, cu rezultatele sintetizate în tabelul următor.

Dispoziția din proiect	**Act normativ în vigoare cu obiect apropiat**	**Concluzia verificării şi soluția adoptată**
Art. 1 alin. (3)–(4) şi art. 9 alin. (7) – raportul cu Regulamentul privind IA şi modelele de uz general	Regulamentul (UE) 2024/1689, art. 2, cap. V (art. 51–56 – modelele de uz general), art. 88 (competența exclusivă a Comisiei de supraveghere a furnizorilor de modele de uz general), art. 99	Delimitare expresă: legea nu instituie condiții de introducere pe piața Uniunii a modelelor de uz general şi nu aduce atingere competențelor Comisiei (art. 88); obligațiile sale privesc siguranța publică, securitatea națională, răspunderea, drepturile persoanelor în raporturile nearmonizate şi organizarea autorităților, iar autorizarea priveşte punerea în exploatare pe teritoriul României. Pentru modelele cu risc

Dispoziția din proiect	Act normativ în vigoare cu obiect apropiat	Concluzia verificării și soluția adoptată
		sistemic ai căror furnizori respectă cap. V, Autoritatea se întemeiază pe documentația comunicată Oficiului pentru IA și verifică numai condițiile care exced regulamentului (art. 9 alin. (7)).
Art. 3 lit. a), b), n) – definițiile sistemului de IA, modelului de uz general, incidentului grav	Regulamentul (UE) 2024/1689, art. 3 pct. 1, 63, 49	Suprapunere potențială evitată: definițiile nu sunt reluate, ci preluate prin normă de trimitere; incidentul grav este completat cu situații neacoperite de Regulament.
Art. 3 lit. g)–i) – dezvoltator, exploatant, punere în exploatare	Regulamentul (UE) 2024/1689, art. 3 pct. 3 (furnizor), 4 (implementator), 8 (operator), 11 (punere în funcțiune)	Noțiuni distincte, cu conținut diferit (activitate materială, nu introducere pe piață). Pentru evitarea confuziei terminologice (art. 37 din Legea nr. 24/2000), legea utilizează termeni proprii, definiți autonom.
Art. 5–6 – pragul de 10^{25} FLOP și capabilitățile critice	Regulamentul (UE) 2024/1689, art. 51 și anexa XIII	Nu există paralelism: Regulamentul folosește pragul pentru prezumția de risc sistemic și obligațiile de diligență ale furnizorului; legea îl folosește pentru declanșarea regimului național de autorizare, în domenii nearmonizate. Pragul este identic pentru coerență. Lista capabilităților critice nu cuprinde influențarea proceselor democratice sau a opiniei publice, materie care rămâne exclusiv în domeniul art. 5 alin. (1) lit. a) și b) și al art. 50 din Regulament, al legislației electorale și al Codului penal; legea nu conferă nicio competență privind conținutul dezbaterii publice.
Art. 7–11 – notificarea antrenării și autorizarea prealabilă	Regulamentul (UE) 2024/1689, art. 52 (notificarea Comisiei), art. 53 și 55 (obligațiile furnizorilor)	Nu există paralelism: Regulamentul nu conține un regim de autorizare prealabilă și nici notificarea antrenării. Autorizarea privește activități desfășurate pe teritoriul României (antrenare, exploatare) și nu condiționează introducerea pe piața internă (art. 1 alin. (4)); art. 9 alin. (7) asigură recunoașterea, prin

Dispoziția din proiect	Act normativ în vigoare cu obiect apropiat	Concluzia verificării și soluția adoptată
		procedura simplificată stabilită de normele metodologice, a sistemelor puse legal în exploatare în alte state membre, iar art. 9 alin. (4) instituie garanții procedurale (termen, suspendare limitată, motivare pe fiecare condiție, acțiune în obligarea la pronunțare).
Art. 12 – securitatea ponderilor	Regulamentul (UE) 2024/1689, art. 55 alin. (1) lit. d); OUG nr. 155/2024 (NIS 2); Legea nr. 182/2002	Obiect specific (ponderile) și standard specific (echivalent „strict secret"), neacoperite de actele menționate. Art. 12 alin. (4) prevede expres aplicarea fără a aduce atingere OUG nr. 155/2024. Legea nr. 182/2002 este folosită ca normă de trimitere pentru standard, fără a clasifica ponderile.
Art. 14 – supravegherea umană	Regulamentul (UE) 2024/1689, art. 14 (sisteme cu grad ridicat de risc)	Nu există paralelism: art. 14 din Regulament se aplică sistemelor cu grad ridicat de risc din anexa III; legea reglementează sistemele de vârf, cu un conținut diferit (capacitate de oprire testată, persoane desemnate).
Art. 15 și cap. V – interdicții	Regulamentul (UE) 2024/1689, art. 5 (practici interzise)	Nu există paralelism: art. 5 din Regulament interzice practici de utilizare (manipulare subliminală, scoring social, identificare biometrică); legea interzice caracteristici de proiectare și antrenare ale sistemului, neacoperite de Regulament.
Art. 17 – marcarea conținutului generat	Regulamentul (UE) 2024/1689, art. 50 alin. (2) și (4) și art. 99 alin. (4); Regulamentul (UE) 2022/2065; Codul penal (art. 325 – falsul informatic, art. 244 – înșelăciunea)	Suprapunere parțială identificată și rezolvată prin art. 17 alin. (6): pentru furnizorii și implementatorii cărora li se aplică art. 50 din Regulament, obligațiile de marcare se consideră îndeplinite prin respectarea art. 50 alin. (2) și (4), legea stabilind numai autoritatea competentă, procedura de constatare și sancțiunile, în limitele art. 99 alin. (4) din Regulament (art. 37 alin. (1) lit. e) teza a doua). Art.

Dispoziția din proiect	Act normativ în vigoare cu obiect apropiat	Concluzia verificării și soluția adoptată
		17 se aplică integral numai rezultatelor sistemelor antrenate ori exploatate în România care nu sunt introduse pe piața Uniunii și comunicării publice a autorităților române; interdicția înlăturării marcajului (alin. (3)) este faptă neacoperită de Regulament. Faptele săvârșite prin folosirea conținutului nemarcat în scop fraudulos rămân în sfera Codului penal.
Art. 18 – informarea utilizatorului	Regulamentul (UE) 2024/1689, art. 50 alin. (1); Regulamentul (UE) 2016/679, art. 13–15 și 22; Legea nr. 190/2018	Nu există paralelism: Regulamentul privește informarea despre interacțiunea cu sistemul, iar RGPD informarea privind prelucrarea datelor; art. 18 reglementează informarea despre întemeierea unei decizii pe rezultatul unui sistem și despre persoana care răspunde pentru ea, materie de procedură administrativă și de răspundere civilă, nearmonizată.
Art. 19 – reprezentantul pentru conformare	Regulamentul (UE) 2024/1689, art. 54 (reprezentantul autorizat); Regulamentul (UE) 2016/679, art. 27; Regulamentul (UE) 2022/2065, art. 13; Legea nr. 365/2002	Nu există paralelism: instituțiile citate privesc reprezentarea pentru obligațiile din actele respective. Reprezentantul prevăzut de lege este desemnat numai de dezvoltatorii și exploatanții stabiliți în afara Uniunii, pentru regimul național de autorizare, inspecție, încetare a furnizării și blocare și pentru comunicarea actelor; cei stabiliți într-un alt stat membru desemnează numai un punct de contact, care poate fi reprezentantul autorizat prevăzut la art. 54 din Regulamentul privind IA ori reprezentantul legal prevăzut la art. 13 din Regulamentul (UE) 2022/2065 (art. 19 alin. (1)), astfel încât nu se impune o obligație de stabilire contrară art. 3 din Directiva 2000/31/CE; art. 19 alin. (6) evită dublarea, recunoscând ca îndeplinită obligația atunci când reprezentantul

Dispoziția din proiect	Act normativ în vigoare cu obiect apropiat	Concluzia verificării și soluția adoptată
		autorizat european este împuternicit și pentru România.
Art. 20 – raportarea incidentelor grave	Regulamentul (UE) 2024/1689, art. 55 alin. (1) lit. c) și art. 73	Suprapunere parțială identificată și rezolvată: art. 20 alin. (1) teza a doua prevede că raportarea către Autoritate nu înlocuiește raportarea către Oficiul pentru IA și permite transmiterea aceluiași raport, completat; se evită dubla sarcină administrativă.
Art. 21 – avertizorii de integritate	Legea nr. 361/2022; Directiva (UE) 2019/1937; Regulamentul (UE) 2024/1689, art. 87	Suprapunere evitată prin normă de trimitere la Legea nr. 361/2022; legea adaugă numai elementele neacoperite (riscuri de siguranță, semnalare către Parlament/public, nulitatea clauzelor patrimoniale, infracțiunea de represalii).
Art. 22 – furnizorii de infrastructură de calcul	OUG nr. 155/2024 (centrele de date ca entități esențiale); Legea nr. 129/2019 (cunoașterea clientelei)	Nu există paralelism: obligațiile din lege (evidența volumului de calcul, interdicția furnizării peste prag fără notificare) sunt specifice și nu se regăsesc în actele menționate; obligația de cunoaștere a clientelei are model, nu sursă, în Legea nr. 129/2019.
Art. 23 – autoritățile publice, apărare și securitate națională	Regulamentul (UE) 2024/1689, art. 2 alin. (3) (excludere); Legea nr. 415/2002 (CSAT)	Domeniu lăsat expres statelor membre; nu există reglementare națională a sistemelor de IA în acest domeniu. Competența CSAT este cea prevăzută de Legea nr. 415/2002.
Art. 24 – forța letală	Nu există reglementare națională; Rezoluția AG ONU 78/241	Nu există paralelism.
Art. 25 – personalitatea juridică și autonomia patrimonială	Codul civil, art. 25 (subiectele de drept); Legea nr. 129/2019 (beneficiarul real)	Nu există paralelism: Codul civil nu conține o normă de excludere expresă; legea o instituie, în consonanță cu art. 25.
Art. 26 – interdicția condiționării participării la viața socială	Regulamentul (UE) 2024/1689, art. 5 alin. (1) lit. c) (scorul social); Regulamentul (UE) 2016/679, art. 25 (decizii	Nu există paralelism: art. 5 lit. c) din Regulament interzice evaluarea persoanelor pe baza comportamentului social cu tratament prejudiciabil disproporționat; art. 22 RGPD conferă un drept individual

Dispoziția din proiect	Act normativ în vigoare cu obiect apropiat	Concluzia verificării și soluția adoptată
	automatizate); Legea nr. 190/2018	privind deciziile bazate exclusiv pe prelucrarea automată a datelor personale. Art. 26 instituie o interdicție obiectivă, de ordine publică, privind condiționarea accesului la drepturi, servicii esențiale și viața socială de decizii ale sistemelor de IA sau de acceptarea unor mijloace digitale, cu garanția alternativei și cu contestație la tribunalul de la domiciliu, fără procedură prealabilă și cu apel la curtea de apel (derogare expresă de la art. 7, 10 și 20 din Legea nr. 554/2004); alin. (8) prevede aplicarea fără a aduce atingere celor două norme.
Art. 27 – interdicția , cenzurii prin sisteme de IA	Constituția României, art. 30 alin. (2) (interdicția cenzurii); Regulamentul (UE) 2022/2065 (DSA), considerentul 9 (armonizare deplină) și art. 14, 17, 20 (condițiile contractuale, motivarea deciziilor de moderare, plângeri interne); Codul de procedură penală (supravegherea tehnică)	Nu există paralelism: art. 30 din Constituție enunță interdicția, fără a reglementa mijloacele automate; DSA armonizează deplin obligațiile furnizorilor de servicii intermediare (considerentul 9), pe care legea nu le reproduce. Art. 27 alin. (6) – normă de coordonare – prevede că, pentru aceşti furnizori, articolul se aplică numai în măsura compatibilă cu DSA, ale cărui art. 14, 17 și 20 rămân aplicabile, că măsurile împotriva mesajelor nesolicitate, conturilor automatizate, riscurilor de securitate și filtrele alese de utilizator nu sunt atinse și că nicio garanție a DSA pentru destinatari nu poate fi restrânsă. Art. 27 instituie o interdicție de ordine publică adresată în primul rând autorităților publice (alin. (3)), cu drept la decizie umană și la instanță (alin. (5), prin trimitere la art. 26 alin. (5) și (6)).
Art. 35–36 – răspunderea civilă obiectivă și asigurarea	Codul civil, art. 1376; Legea nr. 240/2004 (produse cu defecte); Directiva (UE) 2024/2853,	Suprapunere potențială cu răspunderea pentru produse rezolvată prin art. 35 alin. (5): temei distinct, întemeiat pe risc, care nu modifică

Dispoziția din proiect	Act normativ în vigoare cu obiect apropiat	Concluzia verificării și soluția adoptată
	art. 2–3 și 18; Legea nr. 703/2001	regimul armonizat al răspunderii pentru produse (cumul de temeiuri, fără dublă reparare); în măsura în care excluderea forței majore pentru lipsa cunoașterii științifice (alin. (2)) intră în domeniul directivei, Guvernul îndeplinește formalitățile prevăzute la art. 18 din aceasta. Art. 1376 C. civ. este aplicat prin normă de trimitere („se aplică în mod corespunzător"), nu reprodus. Art. 36 permite niveluri inferioare și mecanisme alternative de garantare dacă acoperirea nu este disponibilă pe piață.
Art. 37 – contravenții	Regulamentul (UE) 2024/1689, art. 99 și 101; OG nr. 2/2001	Nu există paralelism: amenzile din Regulament sancționează obligațiile din Regulament (aplicate de Comisie pentru modelele de uz general); contravențiile din lege sancționează obligațiile din lege, iar pentru faptele care constituie încălcări ale art. 50 din Regulament amenda se aplică în limitele art. 99 alin. (4) din acesta (alin. (1) lit. e)); pentru aceeași faptă nu se pot aplica două sancțiuni în temeiul legii și al Regulamentului (alin. (5)). Regimul general al OG nr. 2/2001 este aplicat prin trimitere, cu două derogări exprese. Elementele constitutive rămân stabilite exclusiv prin lege (art. 32 alin. (4)).
Art. 38–39 – încetarea furnizării și blocarea accesului	OUG nr. 77/2009 (blocarea site-urilor de jocuri de noroc neautorizate); Directiva 2000/31/CE, art. 3, și Legea nr. 365/2002; CJUE, C-376/22, Google Ireland și alții, hotărârea din 9 noiembrie 2023, ECLI:EU:C:2023:835; Regulamentul (UE) 2022/2065 (DSA), art. 51 și	Nu există paralelism: mecanismele existente privesc alte obiecte (jocuri de noroc, conținut ilegal, produse neconforme). Pentru serviciile din alte state membre, art. 4 alin. (4) și art. 39 alin. (4) trimit la art. 3 din Directiva 2000/31/CE și la Legea nr. 365/2002: măsura se dispune numai individual, pentru un serviciu determinat, pentru o obligație necesară protecției ordinii, siguranței ori sănătății publice, cu procedura de

Dispoziția din proiect	Act normativ în vigoare cu obiect apropiat	Concluzia verificării și soluția adoptată
	76; Regulamentul (UE) 2019/1020, art. 16	solicitare a statului de origine și de notificare a Comisiei – iar nu ca măsură generală și abstractă, exclusă de CJUE în cauza C-376/22 (pct. 27). Blocarea este subsidiară, motivată, reexaminată la 90 de zile și supusă contestației cu suspendare provizorie judiciară (art. 39 alin. (1) și (5)). Amenda periodică sancționează o obligație proprie legii (încetarea furnizării), fără corespondent în Regulamentul privind IA.
Art. 43 – garanția utilizatorului (accesarea serviciilor blocate nu este sancționabilă)	Codul penal, art. 360 (accesul ilegal la un sistem informatic); OUG nr. 77/2009 (participarea la jocuri de noroc neautorizate – contravenție)	Nu există paralelism și nici suprapunere: art. 43 nu incriminează și nu sancționează nimic, ci este o garanție generală care exclude expres răspunderea utilizatorului (inclusiv a utilizatorului final profesional, alin. (3)) pentru accesarea unui serviciu neconform și interzice interpretarea art. 38–39 în sensul instituirii de obligații în sarcina utilizatorilor (alin. (2)); ea intră în vigoare odată cu legea, nu cu dispozițiile penale (art. 50 teza a doua). Art. 360 C. pen. rămâne aplicabil accesului fără drept la un sistem informatic prin încălcarea măsurilor de securitate ale acestuia, faptă distinctă, neatinsă de prezentul proiect.
Art. 40–42 și 44 – infracțiuni	Codul penal: art. 303, 345, 275, 360–366 (infracțiuni informatice), 135; Legea nr. 111/1996; Legea nr. 361/2022 (represalii – contravenție)	Nu există paralelism: faptele incriminate (exploatare neautorizată, fals în evaluare, dezvoltare de sisteme interzise) nu au corespondent în Codul penal. Represaliile împotriva avertizorilor sunt contravenție în Legea nr. 361/2022 și devin infracțiune numai în domeniul legii, prin normă specială. Norma inițial preconizată privind aplicarea legii penale în spațiu a fost eliminată din proiect, art. 8 alin. (4) și art. 9–11 din Codul penal fiind suficiente; urmările mai grave se impută în

Dispoziția din proiect	Act normativ în vigoare cu obiect apropiat	Concluzia verificării și soluția adoptată
		condițiile art. 16 alin. (4) C. pen., iar răspunderea pentru neîmpiedicarea faptei (art. 44) este angajată numai față de persoana cu obligația juridică și posibilitatea efectivă de a interveni, cu stabilirea individuală a vinovăției.
Art. 45 – competența DIICOT și măsurile provizorii	OUG nr. 78/2016, art. 11 alin. (1); Codul de procedură penală, art. 36, 168, 249	Competența se stabilește prin completarea expresă a art. 11 alin. (1) din OUG nr. 78/2016 (art. 45 alin. (3)), potrivit art. 59–62 din Legea nr. 24/2000, evitând norma paralelă; măsurile provizorii ale procurorului (alin. (2)) sunt specifice (oprirea sistemului, sigilarea infrastructurii, indisponibilizarea ponderilor), limitate la 30 de zile, confirmate de judecătorul de drepturi și libertăți în 48 de ore, contestabile și reexaminate periodic, și nu reproduc măsurile asigurătorii din Codul de procedură penală.
Art. 31–34 – Autoritatea	Memorandumul Guvernului privind desemnarea autorităților pentru Regulamentul privind IA (ANCOM, ASF, BNR, ANSPDCP)	Nu există paralelism, ci integrare: Autoritatea se organizează în cadrul ANCOM, autoritatea propusă de memorandum ca punct unic de contact; autoritățile desemnate exercită atribuțiile din Regulament, Autoritatea pe cele din lege. Art. 31 alin. (5) și art. 48 alin. (6) reglementează cooperarea și tranziția; art. 31 alin. (2) derogă de la OUG nr. 22/2009 numai pentru funcția de vicepreședinte; art. 32 alin. (2)–(4) separă funcțiile de evaluare, investigare și decizie sancționatorie, condiționează inspecția de ordin scris și limitează standardele la detalierea metodelor de evaluare.

1[1]. Compatibilitatea proiectului de act normativ cu legislația în domeniul achizițiilor publice	Nu este cazul.

2. Conformitatea proiectului de act normativ cu legislația comunitară în cazul proiectelor ce transpun prevederi comunitare	Proiectul nu transpune directive. El este compatibil cu Regulamentul (UE) 2024/1689, cu Regulamentul (UE) 2016/679, cu Directiva (UE) 2019/1937 și cu Directiva (UE) 2024/2853, intervenind exclusiv în domeniile lăsate în competența statelor membre (art. 2 alin. (3) din Regulamentul privind IA; art. 4 alin. (2) TUE), în privința activităților desfășurate pe teritoriul național și în materie penală, civilă și instituțională; delimitarea este exprimată la art. 1 alin. (4), art. 9 alin. (7), art. 17 alin. (6), art. 19 alin. (1) și art. 27 alin. (6). Art. 9 alin. (7) și art. 19 alin. (1) asigură respectarea art. 56 TFUE (libera prestare a serviciilor), iar art. 4 alin. (4) și art. 39 alin. (4) a art. 3 din Directiva 2000/31/CE. Formalitățile prevăzute la art. 18 din Directiva (UE) 2024/2853 se îndeplinesc de Guvern (art. 35 alin. (5)). Necesitatea notificării proiectului potrivit Directivei (UE) 2015/1535 (HG nr. 1016/2004) se verifică înainte de depunere.
3. Măsuri normative necesare aplicării directe a actelor normative comunitare	Legea creează cadrul național complementar Regulamentului (UE) 2024/1689 în privința sistemelor de vârf, desemnează Autoritatea ca punct de legătură cu Oficiul pentru IA (art. 31 alin. (5)) și stabilește autoritatea competentă, procedura și sancțiunile pentru încălcările art. 50 din Regulament, în limitele art. 99 alin. (4) (art. 17 alin. (6), art. 37 alin. (1) lit. e)).
4. Hotărâri ale Curții de Justiție a Uniunii Europene	Hotărârea din 5 mai 1998, National Farmers' Union, C-157/96 (principiul precauției); Hotărârea Tribunalului din 11 septembrie 2002, Pfizer Animal Health, T-13/99 (măsuri de protecție în condiții de incertitudine științifică); Hotărârea din 9 noiembrie 2023, Google Ireland și alții, C-376/22, ECLI:EU:C:2023:835, pct. 25–35 (măsurile derogatorii prevăzute la art. 3 alin. (4) din Directiva 2000/31/CE pot fi numai individuale, pentru un serviciu determinat, nu generale și abstracte – avută în vedere la art. 4 alin. (4), art. 19 alin. (1) și art. 39 alin. (4)).

5. Alte acte normative şi/sau documente internaţionale din care decurg angajamente	Convenţia-cadru a Consiliului Europei privind inteligenţa artificială şi drepturile omului, democraţia şi statul de drept (CETS nr. 225, 2024); Rezoluţia Adunării Generale a ONU 78/241 (2023) privind sistemele de arme autonome letale; Declaraţia de la Bletchley (noiembrie 2023) şi angajamentele de la Seul (mai 2024) privind siguranţa inteligenţei artificiale de vârf, la care Uniunea Europeană este parte.
6. Alte informaţii	Nu este cazul.

Secţiunea a 6-a – Consultările efectuate în vederea elaborării proiectului de act normativ

1. Informaţii privind procesul de consultare cu organizaţii neguvernamentale, institute de cercetare şi alte organisme implicate	Proiectul urmează a fi supus dezbaterii publice potrivit Legii nr. 52/2003 privind transparenţa decizională în administraţia publică, republicată. Se propune consultarea Academiei Române, a universităţilor cu facultăţi de informatică (Universitatea din Bucureşti, Universitatea Politehnica Bucureşti, Universitatea Babeş-Bolyai, Universitatea Tehnică din Cluj-Napoca, Universitatea „Alexandru Ioan Cuza" din Iaşi), a Institutului de Cercetări pentru Inteligenţă Artificială „Mihai Drăgănescu" al Academiei Române, a asociaţiilor profesionale din domeniul tehnologiei informaţiei şi a organizaţiilor pentru drepturile digitale.
2. Fundamentarea alegerii organizaţiilor cu care a avut loc consultarea, precum şi a modului în care activitatea acestor organizaţii este legată de obiectul proiectului de act normativ	Organizaţiile propuse deţin expertiza tehnică necesară evaluării pragurilor şi capabilităţilor critice, respectiv reprezintă interesele operatorilor economici şi ale cetăţenilor afectaţi.
3. Consultările organizate cu autorităţile administraţiei publice locale, în situaţia în care proiectul de act normativ are ca obiect activităţi ale acestor autorităţi, în condiţiile Hotărârii Guvernului nr. 521/2005	Nu este cazul.

4. Consultările desfășurate în cadrul consiliilor interministeriale, în conformitate cu prevederile Hotărârii Guvernului nr. 750/2005	Nu este cazul.
5. Informații privind avizarea de către: a) Consiliul Legislativ; b) Consiliul Suprem de Apărare a Țării; c) Consiliul Economic și Social; d) Consiliul Concurenței; e) Curtea de Conturi	Proiectul se depune spre avizare la Consiliul Legislativ (art. 79 din Constituție), la Consiliul Economic și Social (Legea nr. 248/2013), la Consiliul Suprem de Apărare a Țării (pentru art. 23–24) și la Consiliul Superior al Magistraturii (pentru dispozițiile penale și de competență, potrivit Legii nr. 305/2022 privind Consiliul Superior al Magistraturii). Se solicită punctul de vedere al Autorității Naționale pentru Administrare și Reglementare în Comunicații, al Autorității Naționale de Supraveghere a Prelucrării Datelor cu Caracter Personal și al Directoratului Național de Securitate Cibernetică.

Secțiunea a 7-a – Activități de informare publică privind elaborarea și implementarea proiectului de act normativ

1. Informarea societății civile cu privire la necesitatea elaborării actului normativ	Inițiatorul a informat publicul cu privire la necesitatea reglementării prin intermediul platformelor sale de comunicare, pornind de la avertismentele publice ale comunității științifice (interviul CNN din 2 mai 2023 cu Geoffrey Hinton și Connor Leahy, declarația Center for AI Safety din 30 mai 2023, Raportul internațional privind siguranța inteligenței artificiale din 2025). Proiectul și expunerea de motive se publică integral pe pagina de internet a inițiatorului.
2. Informarea societății civile cu privire la eventualul impact asupra mediului în urma implementării proiectului de act normativ, precum și efectele asupra sănătății și securității cetățenilor sau diversității biologice	Proiectul are ca obiect chiar protecția vieții, sănătății și securității cetățenilor; impactul asupra mediului este indirect pozitiv (Secțiunea a 3-a, pct. 4).
3. Alte informații	Nu este cazul.

Secțiunea a 8-a – Măsuri de implementare

1. Măsurile de punere în aplicare a proiectului de act normativ de către autoritățile administrației publice centrale și/sau locale – înființarea unor noi organisme sau extinderea competențelor instituțiilor existente	Se înființează Autoritatea pentru Siguranța Inteligenței Artificiale, structură de specialitate în cadrul ANCOM, condusă de un vicepreşedinte al ANCOM cu rang de secretar de stat numit de Parlament (art. 31), cu personal recrutat prin concurs în fața unei comisii cu profesori universitari din domeniul IT și telecomunicații (art. 33) și cu Consiliu științific consultativ (art. 34). Se extind competențele Direcției de Investigare a Infracțiunilor de Criminalitate Organizată și Terorism (art. 45) și ale Consiliului Suprem de Apărare a Țării (art. 23). Furnizorii de rețele și servicii de comunicații electronice execută deciziile de blocare (art. 39). Ca măsură organizatorică internă a ANCOM, funcțiile de evaluare, de investigare și de decizie sancționatorie se exercită de structuri distincte în cadrul Autorității, persoana care a efectuat evaluarea sau investigația neparticipând la decizia sancționatorie (art. 32 alin. (2)); organismele de evaluare se desemnează pe criterii publice, cu reguli de recuzare. Până la numirea vicepreşedintelui, toate atribuțiile Autorității, inclusiv măsurile urgente, se exercită de președintele ANCOM, care răspunde pentru acestea în condițiile legii (art. 48 alin. (6)).
2. Alte informații	Calendarul unic de implementare, raportat la data publicării legii în Monitorul Oficial (P): P+30 de zile – intrarea în vigoare a legii, inclusiv a garanției prevăzute la art. 43 (art. 50); P+60 – numirea vicepreşedintelui de către Parlament și completarea structurii ANCOM (art. 49 alin. (1)); P+90 – notificarea sistemelor aflate în exploatare, adică 60 de zile de la intrarea în vigoare (art. 48 alin. (2)); P+120 – adoptarea normelor metodologice, după consultare publică de 30 de zile (art. 49 alin. (2)), și împlinirea termenului de 90 de zile de la intrarea în vigoare pentru obligațiile care nu depind de norme, inclusiv marcajul perceptibil, informarea utilizatorului și desemnarea reprezentantului (art. 48 alin. (1) și (4)), după care devin aplicabile art. 38–39 (art. 48

	alin. (3)); P+210 – depunerea cererilor de autorizare, marcajul tehnic încorporat şi celelalte obligaţii dependente de norme, la 90 de zile de la intrarea în vigoare a normelor, care are loc la data publicării lor, în 5 zile de la adoptare, dacă acestea sunt adoptate la termen (art. 48 alin. (2), (4) şi (5)); P+270 – intrarea în vigoare a art. 40–42, 44 şi 45 (art. 50). Sistemele notificate pot fi menţinute în exploatare până la decizia Autorităţii, cel mult 12 luni de la intrarea în vigoare, termen prelungit de drept cu întârzierea adoptării normelor ori a soluţionării cererii, solicitantul diligent neputând fi sancţionat pentru întârzierea instituţiilor (art. 48 alin. (2)). Până la adoptarea normelor, evaluările se fac potrivit codurilor de bună practică adoptate în temeiul Regulamentului privind IA, iar Autoritatea publică orientări provizorii (art. 49 alin. (3)). Termenele sunt cele maxime prevăzute de lege; fezabilitatea lor se verifică cu ANCOM la avizare.

Faţă de cele prezentate, a fost elaborată propunerea legislativă alăturată, pe care o supunem Parlamentului spre dezbatere şi adoptare.

Iniţiator,

Deputat
Coarnă Dumitru



NOTĂ DOCUMENTARĂ

Sursele avute în vedere la elaborarea propunerii

1. Regulamentul (UE) 2024/1689 al Parlamentului European și al Consiliului din 13 iunie 2024 de stabilire a unor norme armonizate privind inteligența artificială, JO L, 12.7.2024 – în special art. 2, 3, 5, 14, 51–56, 68, 72–73, 78, 87, 99–101 și anexa XIII.

2a. Dario Amodei, „We Must Pace the Frontier", 12 septembrie 2026 (darioamodei.com); relatările VentureBeat, TechRadar, Newsweek, The Spokesman-Review din 12 septembrie 2026 privind eseul, incidentul Hugging Face și reacțiile lui Sam Altman și Elon Musk; interviul lui Sam Altman pentru Fortune (13 septembrie 2026), citat de Bloomberg și Business Standard.

2g. Republica Coreea – „Framework Act on the Development of Artificial Intelligence and Establishment of Trust" (Legea-cadru privind dezvoltarea inteligenței artificiale și instituirea încrederii), în vigoare din 22 ianuarie 2026: obligația de etichetare a conținutului generat de inteligența artificială generativă, obligația de informare prealabilă a utilizatorilor și obligația furnizorilor străini de a desemna un reprezentant local pentru conformare; traducerea oficială în limba engleză publicată de Center for Security and Emerging Technology, Georgetown University, https://cset.georgetown.edu/wp-content/uploads/t0625_south_korea_ai_law_EN.pdf; analize: Future of Privacy Forum, https://fpf.org/blog/south-koreas-new-ai-framework-act-a-balancing-act-between-innovation-and-regulation/ ; Cooley LLP, 27 ianuarie 2026, https://www.cooley.com/news/insight/2026/2026-01-27-south-koreas-ai-basic-act-overview-and-key-takeaways.

2h. Regulamentul (UE) 2024/1689, art. 50 (obligații de transparență, aplicabil de la 2 august 2026) și art. 54 (reprezentantul autorizat al furnizorilor de modele de uz general stabiliți în state terțe); Codul de bune practici al Comisiei Europene privind transparența conținutului generat de inteligența artificială (proiect, 2026).

2f. Yoshua Bengio, interviu acordat publicației The Guardian (Dan Milmo), 16 septembrie 2026, privind apropierea unui moment de cotitură al reglementării, comparabil cu cel al pandemiei; scrisoarea a 42 de membri și membri străini ai Societății Regale din Regatul Unit privind „îngrijorarea extremă" față de ritmul dezvoltării; relatarea Digi24 din 16 septembrie 2026, https://www.digi24.ro/stiri/sci-tech/lumea-digitala/nasul-inteligentei-artificiale-spune-ca-reglementarea-ai-se-apropie-de-un-punct-de-cotitura-similar-cu-cel-al-pandemiei-de-covid-3950743; Time, „The AI Tipping Point", 15 septembrie 2026, privind propunerile legislative aflate în dezbatere în Congresul Statelor Unite.

2e. Dezbaterea publică din septembrie 2026: demisia publică a cercetătorului Jacob Coxon (Anthropic), 8 septembrie 2026, și reacțiile conducătorilor departamentelor de aliniere și de cercetare ale Anthropic și OpenAI – relatările CBC News, Time (15 septembrie 2026), Forbes și Fortune (9-10 septembrie 2026); pozițiile exprimate la conferința anuală Salesforce din San Francisco, 15 septembrie 2026, de Sam Altman, Mark Zuckerberg, Jensen Huang, Jack Clark și Dario Amodei – relatările BBC News (16 septembrie 2026), The Irish Times, CNBC și Forbes.

2c. Cronologia incidentului din vara anului 2026 (evadarea agenților din mediul de testare al OpenAI și compromiterea platformei Hugging Face): Cloud Security Alliance, „The Great Sandbox Escape" (28 iulie 2026), https://cloudsecurityalliance.org/blog/2026/07/28/openai-and-hugging-face-security-incident-inside-the-great-sandbox-escape; Malwarebytes Labs, „The AI agent swarm that attacked Hugging Face is a warning for the future" (august 2026), https://www.malwarebytes.com/blog/ai/2026/08/the-ai-agent-swarm-that-attacked-hugging-face-is-a-warning-for-the-future; Axios, „OpenAI Hugging Face breach exposes AI agent security limits" (1 septembrie 2026), https://www.axios.com/2026/09/01/openai-hugging-face-ai-agent-security; TechCrunch, „OpenAI's rogue agents keep escaping, with no formal process to investigate them" (4 septembrie 2026), https://techcrunch.com/2026/09/04/openais-rogue-agents-keep-escaping-with-no-formal-process-to-investigate-them/; Noma Security, „The Great (Sandbox) Escape" (2026), https://noma.security/blog/the-great-sandbox-escape-analyzing-the-openai-hugging-face-security-incident; declarația comună OpenAI – Hugging Face din 21 iulie 2026.

2d. Propuneri legislative depuse în Congresul Statelor Unite ale Americii ca reacție la incident: „AI Kill Switch Act" (23 iulie 2026) și „Ban Artificial Superintelligence Act" (3 septembrie 2026); scrisoarea deschisă a peste 1.100 de angajați ai laboratoarelor de vârf privind mecanismele de temperare a ritmului de dezvoltare (28 iulie 2026).

2b. Senatorul Alex Antic (Senatul Australiei), discurs parlamentar difuzat public în 2026 privind „închisoarea digitală" (economia abonamentului, identitatea digitală, conformarea ca preț al participării în societate), https://www.facebook.com/reel/1059873890017722/.

2. CNN, „Amanpour", 2 mai 2023 – interviu cu Geoffrey Hinton și Connor Leahy („We do not know how to control these things"; Hinton: dispariția umanității „nu este de neconceput"; Leahy: „din păcate, destul de probabil").

3. Center for AI Safety, „Statement on AI Risk", 30 mai 2023; declarațiile publice ale lui Geoffrey Hinton (BBC, decembrie 2024; CBS, aprilie 2025) privind probabilitatea de 10–20% și comparația cu „puiul de tigru"; „International AI Safety Report", ianuarie 2025 (coord. Y. Bengio); RAND Corporation, „Securing AI Model Weights", 2024; scrisoarea „A Right to Warn about Advanced Artificial Intelligence", 4 iunie 2024.

4. ANCOM, comunicat „Regulamentul privind inteligența artificială în România – stadiul actual al cadrului de implementare" (iulie 2026); presa de specialitate (Juridice.ro, Bursa.ro, august 2026) privind imposibilitatea sancționării până la adoptarea legii naționale.

5. California SB 53 – Transparency in Frontier Artificial Intelligence Act (29 septembrie 2025); Ordinul executiv al SUA nr. 14110 (30 octombrie 2023, revocat în ianuarie 2025); Măsurile provizorii ale Republicii Populare Chineze privind serviciile de IA generativă (15 august 2023); Convenția-cadru a Consiliului Europei privind inteligența artificială (CETS nr. 225, 2024); Rezoluția AG ONU 78/241 (22 decembrie 2023); apelul comun al Secretarului General al ONU și al Comitetului Internațional al Crucii Roșii (5 octombrie 2023).

6. Legea nr. 24/2000 privind normele de tehnică legislativă pentru elaborarea actelor normative, republicată, cu modificările și completările ulterioare – în special art. 6, 7, 13, 16, 30–31, 36–38, 40–56, 63; Hotărârea Guvernului nr. 561/2009 pentru aprobarea Regulamentului privind procedurile, la nivelul Guvernului, pentru elaborarea, avizarea și prezentarea proiectelor

de documente de politici publice, a proiectelor de acte normative, precum și a altor documente, în vederea adoptării/aprobării – anexa nr. 1 (structura expunerii de motive).

7. Constituția României, republicată (art. 1, 22, 34, 53, 73, 75, 76, 78, 117, 119, 142, 148); Codul civil (art. 11, 25, 1246–1250, 1376); Codul penal (art. 8, 9–11, 21, 135, 275, 303, 345, 395); Codul de procedură penală (art. 36, 168, 249); Legea nr. 111/1996; Legea nr. 703/2001; Legea nr. 182/2002; Legea nr. 415/2002; Legea nr. 240/2004; Legea nr. 95/2006; Legea nr. 190/2018; Legea nr. 129/2019; Legea nr. 361/2022; Legea nr. 365/2002; Legea-cadru nr. 153/2017; OUG nr. 77/2009; OG nr. 2/2001; OUG nr. 27/2003; OUG nr. 78/2016; OUG nr. 155/2024; OUG nr. 195/2005.

8. Jurisprudență: CJUE, C-157/96, National Farmers' Union (1998); Tribunalul UE, T-13/99, Pfizer Animal Health (2002); CJUE, C-376/22, Google Ireland și alții, hotărârea din 9 noiembrie 2023, ECLI:EU:C:2023:835 (pct. 25–35); Curtea Constituțională a României, Decizia nr. 51/2016 (claritatea și previzibilitatea legii).

9. Analiza juridică independentă a proiectului (forma din 20 septembrie 2026), cu sursele verificate indicate în aceasta: Regulamentul (UE) 2024/1689 (text consolidat, 27 iulie 2026), Regulamentul (UE) 2022/2065 (considerentul 9, art. 14, 17, 20), Directiva 2000/31/CE (art. 3), Directiva (UE) 2024/2853 (art. 2–3, 18), Directiva (UE) 2019/1937 (art. 6, 15, 21), Directiva (UE) 2015/1535 și HG nr. 1016/2004, Legea nr. 120/2018 de aprobare a OUG nr. 78/2016.

COARNĂ DUMITRU DEPUTAT



CONSILIUL ECONOMIC ȘI SOCIAL
INTRARE Nr. 7321
IEȘIRE
06 11 2026

PARLAMENTUL ROMÂNIEI

CAMERA DEPUTAȚILOR **SENATUL**

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, capabilități 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 capabilităților 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 capabilitățile – intensitatea obligațiilor crește odată cu capabilitățile 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) capabilitate 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 capabilitate 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, apță 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 exploatate 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 acesteia 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 stabileşte 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) şi 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 depăşeşte pragul de calcul notifică Autoritatea cu cel puțin 60 de zile înainte de începerea antrenării.

(2) Notificarea cuprinde: identitatea dezvoltatorului şi a persoanelor fizice responsabile; descrierea arhitecturii şi a volumului de calcul preconizat; locul şi 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 şi 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 şi, în termen de 5 zile lucrătoare, orice solicitare de capacitate aptă să depăşească pragul de calcul. Informațiile astfel notificate sunt utilizate exclusiv pentru aplicarea prezentei legi şi 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 acesteia 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 stabileşte, 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 depăşi o pătrime din volumul total preconizat, precum şi la apariția unor indicii privind o capabilitate critică ori la modificarea configurației de antrenare; măsurile de atenuare şi 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 ținuți 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 mecanismele de siguranță aplicate la nivelul utilizatorului. Accesul se realizează într-un mediu securizat, cu trasabilitatea tuturor operațiunilor; evaluatorii sunt ținuți 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 exploatantul 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, şi nu poate fi revocat fără notificarea prealabilă a Autorităţii şi 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 instanţei.

(2) Conducătorul funcţiei de evaluare a siguranţei are dreptul şi obligaţia 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 activităţii fiind permisă numai în condiţiile prevăzute de articolele respective. Suspendarea dispusă din precauţie, în afara acestor cazuri, poate fi reexaminată numai de organul de conducere, prin hotărâre motivată, comunicată Autorităţii în termen de 24 de ore.

(3) Remuneraţia personalului funcţiei de evaluare a siguranţei nu poate fi condiţionată de rezultatele comerciale ale dezvoltatorului. Dezvoltatorul verifică, cel puţin semestrial, dacă măsurile de monitorizare, de detectare şi de control instituite potrivit prezentei legi funcţionează potrivit destinaţiei lor, consemnează rezultatul verificării şi îl comunică comitetului de supraveghere a siguranţei 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 siguranţei, format din cel puţin doi membri ai acestui organ care nu exercită funcţii executive şi nu au interese în dezvoltarea comercială ori în rezultatele financiare ale dezvoltatorului; nu constituie asemenea interes deţinerea de acţiuni ori de părţi sociale sub 1% din capital, fără putere de decizie, şi nici remuneraţia fixă primită în calitate de membru al organului de conducere, iar remuneraţia variabilă legată de rezultatele comerciale constituie un asemenea interes. Dezvoltatorul asigură ca comitetul să primească raportările funcţiei de evaluare a siguranţei, făcute potrivit alin. (1), şi 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 şi, dacă există potrivit legii ori actului constitutiv, rapoartele auditorului financiar şi ale structurii de audit intern, să urmărească remedierea deficienţelor constatate şi să se întrunească cel puţin trimestrial, precum şi de îndată ce este sesizat de conducătorul funcţiei de evaluare a siguranţei. Sesizările primite, ordinea de zi, deliberările şi hotărârile comitetului se consemnează în procese-verbale, care se păstrează cel puţin 10 ani şi se pun la dispoziţia Autorităţii la cererea acesteia. Dezvoltatorul guvernat de o lege străină care nu permite constituirea unui comitet în condiţiile prezentului alineat îndeplineşte obligaţia prin desemnarea, în cadrul organului său de conducere ori în afara acestuia, a unei funcţii de supraveghere a siguranţei care exercită atribuţiile prevăzute în teza a doua, nu se află în subordinea conducerii executive şi raportează potrivit alin. (5).

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

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 capabilități 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 explicitare 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 şi exploatantul verifică, cel puţin trimestrial şi la cererea Autorităţii, inteligibilitatea jurnalelor şi a comunicării prevăzute la alin. (3), prin examinarea unui eşantion reprezentativ, şi consemnează rezultatul verificării, inclusiv proporţia mesajelor a căror semnificaţie nu a putut fi stabilită.

(5) Pierderea inteligibilităţii constituie incident grav şi se raportează potrivit art. 20 alin. (1). Ea se constată atunci când proporţia mesajelor a căror semnificaţie nu poate fi stabilită depăşeşte 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 semnificaţia acţiunilor sistemului; restabilirea inteligibilităţii se constată de aceleaşi persoane şi se comunică Autorităţii. Până la restabilirea inteligibilităţii, dezvoltatorul sau exploatantul suspendă funcţionalităţile care implică acţiuni autonome ale sistemului şi comunicarea dintre componentele, instanţele ori agenţii acestuia, cu excepţia cazului în care Autoritatea dispune altfel, prin decizie motivată, pentru cel mult 90 de zile şi 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 dispoziţie mijloacele prevăzute la alin. (2), precum şi orice acţiune de înlăturare, alterare sau limitare a acestor mijloace. Prezentul alineat nu interzice criptarea comunicării, cu condiţia ca dezvoltatorul să deţină şi să pună la dispoziţie, potrivit alin. (2), mijloacele de decriptare.

Articolul 17

(1) Rezultatele generate prin intermediul unui sistem de inteligenţă artificială care constau în înregistrări audio, imagini ori înregistrări video şi care, prin conţinutul 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 provenienţă, alcătuit din:

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

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

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

(3) Este interzisă înlăturarea, alterarea, ascunderea ori falsificarea marcajului de provenienţă, precum şi punerea la dispoziţie a unor produse sau servicii având ca scop principal aceste operaţiuni. Persoana care pune la dispoziţie 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 condiţiile standardelor prevăzute la alin. (2), care reglementează şi situaţiile 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 marcare 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 şi nu limitează răspunderea dezvoltatorului ori a exploatantului. Reprezentantul are dreptul, stabilit prin actul de desemnare, de a obține de la cel reprezentat documentele, informațiile şi mijloacele necesare îndeplinirii atribuțiilor sale; el răspunde numai pentru neîndeplinirea propriilor obligații prevăzute la alin. (3) şi (4), nu şi 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 şi pentru atribuțiile prevăzute la alin. (3) şi 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) şi 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 şi 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 înlocuieşte raportarea către Oficiul pentru IA prevăzută la art. 55 alin. (1) lit. c) din Regulamentul privind IA şi nici raportarea prevăzută la art. 73 din acelaşi 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 şi cooperarea cu Autoritatea constituie circumstanțe atenuante şi 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 şi notificării prevăzute la alin. (5). Notificarea prevăzută la alin. (5) şi 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 şi 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 şi exploatantul notifică şi 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 capabilități 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 succesor 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 vicepreşedintele 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 şi cu Comitetul ştiințific prevăzut de Regulamentul privind IA şi cooperează cu autoritățile naționale desemnate potrivit acestuia, care îşi păstrează competențele proprii; Autoritatea exercită exclusiv atribuțiile prevăzute de prezenta lege în privința sistemelor de vârf şi informează Oficiul pentru IA asupra deciziilor care privesc modele de uz general.

Articolul 32

(1) Autoritatea are următoarele atribuții principale:

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

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

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

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

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

f) desemnează şi supraveghează organismele de evaluare;

g) primeşte sesizările persoanelor privind încălcarea art. 26 şi 27, constată încălcările şi 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 şi 27 şi recomandările legislative;

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

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

(2) Funcțiile de evaluare, de investigare şi 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 şi de prevenire a conflictelor de interese, şi nu pot evalua sisteme ale unor persoane cu care se află în raporturi economice.

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

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

Articolul 33

(1) Personalul de specialitate al Autorităţii se numeşte exclusiv în urma unui concurs organizat de ANCOM, la care participarea este deschisă oricărei persoane care îndeplineşte condiţiile de studii şi de experienţă stabilite prin anunţul de concurs, publicat cu cel puţin 30 de zile înainte de data desfăşurării. Rezultatele concursului pot fi contestate la instanţa de contencios administrativ.

(2) Comisia de concurs este formată din cel puţin 5 membri, dintre care cel puţin 3 sunt profesori universitari din domeniul tehnologiei informaţiei şi al telecomunicaţiilor ori specialişti cu experienţă practică recunoscută în securitatea şi evaluarea sistemelor de inteligenţă artificială, propuşi de instituţiile de învăţământ superior acreditate care organizează studii universitare de doctorat în aceste domenii, la solicitarea ANCOM. Membrii comisiei nu pot deţine nicio funcţie, participaţie sau remuneraţie din partea unui dezvoltator ori exploatant şi nu pot avea, cu candidaţii, raporturi dintre cele care atrag incompatibilitatea. Componenţa comisiei şi rezultatele concursului se publică pe pagina de internet a ANCOM.

(3) Personalul de specialitate al Autorităţii este remunerat, potrivit sistemului de salarizare al ANCOM, la un nivel competitiv cu cel practicat în sectorul privat pentru funcţii echivalente, stabilit anual de preşedintele ANCOM, cu avizul vicepreşedintelui pentru siguranţa inteligenţei artificiale, pe baza unui studiu de piaţă publicat.

(4) Personalul Autorităţii este supus obligaţiilor de confidenţialitate şi incompatibilităţilor prevăzute la art. 31 alin. (3), pe durata raporturilor de serviciu şi timp de 2 ani după încetarea acestora.

(5) Autoritatea se finanţează din bugetul ANCOM, prin alocare distinctă, aprobată anual şi evidenţiată separat, precum şi din taxele de notificare, de evaluare şi de autorizare stabilite prin normele metodologice în raport cu costul serviciului prestat. Amenzile aplicate potrivit prezentei legi se fac venit la bugetul de stat şi nu pot determina resursele Autorităţii. Cercetarea prevăzută la art. 32 alin. (1) lit. j) se finanţează prin alocare bugetară distinctă, fără legătură cu sancţiunile aplicate. Bugetul iniţial al Autorităţii, inclusiv personalul şi 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 şi nu pot afecta drepturile victimelor ori acoperirea prevăzută la art. 36.

(4) Dreptul la acţiune se prescrie în termen de 10 ani de la data la care victima a cunoscut sau trebuia să cunoască prejudiciul şi 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 şi exploatarea sistemului, şi nu modifică regimul armonizat al răspunderii pentru produsele cu defecte; el nu aduce atingere dreptului victimei de a obţine repararea prejudiciului în temeiul acestui regim sau al altor temeiuri prevăzute de lege, fără a putea fi însă reparat de două ori acelaşi prejudiciu. În măsura în care excluderea prevăzută la alin. (2) privind lipsa cunoaşterii ştiinţifice intră în domeniul Directivei (UE) 2024/2853 a Parlamentului European şi a Consiliului din 23 octombrie 2024, Guvernul îndeplineşte formalităţile prevăzute la art. 18 din directivă.

Articolul 36

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

(2) Garanţia financiară se constituie prin scrisoare de garanţie bancară, depozit ori garanţie emisă de o instituţie financiară autorizată, executabilă la cererea victimei în temeiul hotărârii judecătoreşti definitive sau al tranzacţiei. Victima are acţiune directă împotriva asigurătorului sau, după caz, a emitentului garanţiei.

Secţiunea a 2-a. Răspunderea contravenţională

Articolul 37

(1) Constituie contravenţii, dacă nu au fost săvârşite în astfel de condiţii încât să fie considerate, potrivit legii, infracţiuni, următoarele fapte:

a) neîndeplinirea obligaţiei de notificare prevăzute la art. 7 şi art. 10 alin. (2) ori furnizarea de informaţii incomplete, cu amendă de la 1% la 3% din cifra de afaceri mondială totală din exerciţiul financiar precedent;

b) nerespectarea planului de siguranţă, a obligaţiilor de separare a funcţiilor, de notificare prealabilă a revocării conducătorului funcţiei de evaluare a siguranţei, de dispunere a suspendării şi de comunicare a hotărârii de reexaminare, prevăzute la art. 13 alin. (2) teza întâi

şi teza a treia, de necondiţionare a remuneraţiei personalului funcţiei de evaluare a siguranţei de rezultatele comerciale şi de verificare semestrială a funcţionării măsurilor de monitorizare, de detectare şi de control, de desemnare şi de funcţionare a comitetului de supraveghere a siguranţei ori de încredinţare a atribuţiilor acestuia expertului independent, de motivare şi de comunicare a hotărârii de refuz şi de transmitere a raportului prevăzut la art. 13 alin. (5), toate prevăzute la art. 13 alin. (1), alin. (2) teza întâi şi teza a treia şi alin. (3)–(7), de jurnalizare, de asigurare şi de verificare a inteligibilităţii prevăzute la art. 16 alin. (1)–(5), de menţinere şi de testare a capacităţii de oprire, prevăzute la art. 14 alin. (1), (5) şi (6), cu excepţia faptelor care intră sub incidenţa art. 28, de desemnare a persoanelor responsabile de supravegherea umană, prevăzută la art. 14 alin. (3), ori de raportare şi de notificare a incidentelor, în condiţiile art. 20 alin. (1), (5) şi (6), cu amendă de la 2% la 5% din cifra de afaceri mondială;

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

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

e) nerespectarea obligaţiilor de marcare prevăzute la art. 17 alin. (1), (2) şi (4) ori încălcarea interdicţiei 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 obligaţiei de informare prevăzute la art. 18 ori a obligaţiilor 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 contravenţiile prevăzute la alin. (1) lit. e) şi f), săvârşite 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 şi de la 5.000 lei la 200.000 lei pentru persoanele fizice.

(3) Sancţiunea amenzii poate fi însoţită de sancţiunile complementare ale suspendării sau revocării autorizaţiei, ale interzicerii desfăşurării activităţii de dezvoltare pe o perioadă de până la 5 ani, ale confiscării ponderilor şi ale publicării deciziei, aplicate proporţional cu gravitatea faptei; ponderile confiscate se păstrează de Autoritate în condiţiile art. 12.

(4) Contravenţiilor prevăzute de prezenta lege le sunt aplicabile dispoziţiile Ordonanţei Guvernului nr. 2/2001 privind regimul juridic al contravenţiilor, aprobată cu modificări şi completări prin Legea nr. 180/2002, cu modificările şi completările ulterioare. Prin derogare de la art. 28 din Ordonanţa Guvernului nr. 2/2001, contravenientul nu poate achita jumătate din minimul amenzii. Prin derogare de la art. 13 alin. (1) din aceeaşi ordonanţă, aplicarea sancţiunii se prescrie în termen de 5 ani de la data săvârşirii faptei.

(5) La individualizarea sancţiunii se au în vedere gravitatea şi întinderea faptei, pericolul creat, controlul efectiv al persoanei asupra faptei, cooperarea cu Autoritatea şi 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 pedepsesc 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 înşelător privind elemente esenţiale ale capabilităţilor, ale volumului de calcul, ale securităţii ponderilor, ale capacităţii de oprire şi ale rezultatelor testării acesteia sau ale incidentelor unui sistem de vârf, precum şi configurarea sistemului în scopul de a induce în eroare evaluatorii asupra configuraţiei evaluate ori a capabilităţilor reale, se pedepsesc cu închisoare de la 3 la 10 ani şi interzicerea exercitării unor drepturi.

(2) Împiedicarea, în orice mod, a accesului Autorităţii, exercitat în limitele competenţei sale şi 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 infracţiune refuzul întemeiat pe lipsa competenţei Autorităţii ori pe protecţia secretului profesional al avocatului sau a altui secret ocrotit de lege, asupra căruia se pronunţă instanţa.

(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 pedepseşte cu închisoare de la 6 luni la 3 ani sau cu amendă.

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

Articolul 42

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

(2) Divulgarea, transmiterea sau punerea la dispoziţie, fără drept, a ponderilor unui sistem de vârf de categoria a II-a sau a III-a se pedepseşte cu închisoare de la 5 la 15 ani şi interzicerea exercitării unor drepturi. Nu constituie infracţiune transferurile permise potrivit art. 12 alin. (2) şi 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 intervenţia umană, urmată de acţiuni autonome ale sistemului cu consecinţe asupra persoanelor, a mediului fizic ori a infrastructurii critice, pedeapsa este închisoarea de la 10 la 20 de ani şi interzicerea exercitării unor drepturi. Dacă urmarea constă într-un prejudiciu patrimonial deosebit de grav ori într-o pierdere temporară a controlului uman, fără consecinţele prevăzute în teza întâi, pedeapsa este închisoarea de la 7 la 15 ani şi interzicerea exercitării unor drepturi. Urmările se impută în condiţiile 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 exploatanţilor neconformi, inclusiv prin eludarea măsurii de blocare dispuse potrivit art. 39, nu constituie infracţiune sau contravenţie şi nu poate atrage nicio sancţiune 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 cuantumurile 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 şi modalitatea de transmitere a raportului prevăzut la art. 13 alin. (5), onorariul expertului independent prevăzut la art. 13 alin. (6), procedura de testare şi durata prevăzute la art. 14 alin. (1) şi (6), cerinţele minime ale izolării prevăzute la art. 3 alin. (1) lit. bb), cuantumul indemnizaţiei compensatorii prevăzute la art. 31 alin. (3), cuantumul taxelor, stabilit în raport cu costul serviciului, şi cuantumul asigurării ori al garanţiei financiare prevăzute la art. 36. Normele detaliază cadrul stabilit prin prezenta lege şi nu pot stabili conţinutul esenţial al obligaţiilor, al interdicţiilor şi al sancţiunilor; standardele se publică. Normele metodologice se publică în Monitorul Oficial al României, Partea I, în termen de 5 zile de la adoptare şi 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 şi metodelor recunoscute ştiinţific, 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 excepţia art. 40–42, 44 şi 45, care intră în vigoare la 270 de zile de la data publicării. Dispoziţiile art. 43 intră în vigoare odată cu prezenta lege.

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

PREŞEDINTELE CAMEREI DEPUTAŢILOR

PREŞEDINTELE SENATULUI