

# Poziția comună a ENNHRI cu privire la Legea UE privind inteligența artificială

## Introducere

Rețeaua Europeană a Instituțiilor Naționale pentru Drepturile Omului (ENNHRI) salută adoptarea viitoare a Legii UE privind inteligența artificială („EU AIA”). Acesta reprezintă un act legislativ care are potențialul de a asigura o mai bună protecție a drepturilor fundamentale. Prezentul document de poziție comună al ENNHRI prevede recomandări prin care să se îmbunătățească și asigure potențialul legii pentru o mai bună protecție a drepturilor fundamentale.

Comisia Europeană („Comisia”) a publicat prima [propunere](#) de reglementare a inteligenței artificiale în Uniunea Europeană în aprilie 2021. Consiliul a adoptat [abordarea generală](#) în decembrie 2022. În iunie 2023, Parlamentul European („Parlamentul”) a adoptat [poziția sa](#) cu privire la Legea privind inteligența artificială.

ENNHRI prezintă mai jos recomandările sale pentru îmbunătățirea Legii privind inteligența artificială înainte de finalizarea acesteia, cu referire la următoarele domenii:

- Asigurarea unui domeniu vast de aplicare a Legii privind inteligența artificială;
- Îmbunătățirea transparenței, răspunderii și măsurilor reparatorii;
- Asigurarea monitorizării eficiente în cooperare cu instituțiile naționale pentru drepturile omului;
- Abținerea de la supravegherea dăunătoare și discriminatorie de către autoritățile de securitate națională, de aplicare a legii și de migrație.

## 1. Asigurarea unui domeniu de aplicare vast și eliminarea lacunelor necesare

### a. Asigurarea clasificării obiective a sistemelor cu grad ridicat de risc

ENNHRI subliniază importanța **clasificării obiective a sistemelor cu grad ridicat de risc**. Propunerea Comisiei oferă o asemenea abordare. ENNHRI este îngrijorată de includerea de către Parlament a calificativului dublu în articolul 6. Acesta presupune o evaluare suplimentară subiectivă de către furnizorii de inteligență artificială (IA) cu privire la gradul în care sistemul de IA în cauză presupune un risc „semnificativ” pentru drepturile fundamentale. Această abordare creează incertitudine juridică și ar fi dificil de pus în aplicare. De asemenea, ar stimula furnizorii de IA să minimalizeze riscurile pe care le prezintă sistemele lor de IA pentru a reduce controlul de reglementare.

## **b. Evitarea excepțiilor extinse de la interdicții**

Tehnologia poate avea un caracter vătămător inerent sau poate fi utilizată necorespunzător, ducând la încălcarea drepturilor fundamentale. ENNHRI salută abordarea propusă de a interzice sistemele de IA care contravin drepturilor fundamentale (articolul 5). Cu toate acestea, domeniul de aplicare și lista de sisteme de IA interzise în propunerile Comisiei și a Consiliului European („Consiliu”) sunt prea restrânse și nu includ anumite sisteme de IA care nu sunt compatibile cu convențiile internaționale și europene în materie de drepturile omului. ENNHRI sprijină amendamentele înaintate de Parlament în acest sens. ENNHRI este îngrijorată de propunerile Comisiei și Consiliului care prevăd un domeniu de aplicare și o gamă largă de excepții de la interdicții. Tehnologiile de recunoaștere a emoțiilor, categorisirea biometrică pentru prezicerea etniei, genului, orientării sexuale sau politice sau alte caracteristici protejate, precum și evaluările de risc în domeniul azilului și justiției penale ar trebui interzise complet. A se vedea și III. B

## **c. Asigurarea că obligațiile nu se limitează doar la furnizorii de IA**

ENNHRI este îngrijorată că obligațiile se referă în general doar la furnizorii de IA<sup>1</sup> (articolul 43 alin. (2), articolele 8-15) și nu sunt avute în vedere cele ce țin de utilizatorii de IA<sup>2</sup> (articolul 29), înțelegi în mod obișnuit ca cei care pun în aplicare sisteme de IA. ENNHRI îndeamnă factorii responsabili să elaboreze obligații similare și pentru utilizatorii sistemelor de IA (de ex., evaluare privind impactul asupra drepturilor fundamentale, a se vedea și secțiunea II.a), în special cei care acționează în sectorul public, având în vedere că aceștia sunt cel mai bine poziționați pentru a înțelege contextul specific în care sunt utilizate sistemele și, mai important, impactul pe care acestea le vor avea asupra titularilor de drepturi afectați.

## **d. Asigurarea aplicării cooperării în afara Uniunii Europene**

ENNHRI subliniază că Legea privind IA ar trebui să se aplice în contextul cooperării și acordurilor internaționale pentru organismele de aplicare a legii și de cooperare judiciară cu autoritățile publice din țări din afara Uniunii Europene și cu organizații internaționale. ENNHRI salută necesitatea unei „verificări a nivelului de adecvare” propus de Parlament (articolul 2 alin. (4)) având în vedere că Legea privind inteligența artificială se va aplica integral cu excepția cazului în care se dovedește că organizația internațională sau statul non-UE în cauză oferă o titularilor de drepturi protecție echivalentă cu cea ferită de Legea privind inteligența artificială. Absența unor mecanisme de control și echilibru în contextul cooperării internaționale ar permite furnizorilor să eludeze cu ușurință Legea privind inteligența artificială, ceea ce ar duce la utilizarea IA într-o manieră contradictorie Legii privind IA de către state

---

<sup>1</sup> Articolul 3 alin. (2) definește „furnizorul” ca o persoană fizică sau juridică, o autoritate publică, o agenție sau un alt organism care dezvoltă un sistem de IA sau care dispune de un sistem de IA dezvoltat în vederea introducerii sale pe piață sau a punerii sale în funcțiune sub propriul nume sau propria marcă comercială, contra cost sau gratuit.

<sup>2</sup> Articolul 3 alin. (4) definește „utilizatorul” ca orice persoană fizică sau juridică, autoritate publică, agenție sau alt organism care utilizează un sistem de IA aflat sub autoritatea sa, cu excepția cazului în care sistemul de IA este utilizat în cursul unei activități neprofesionale, personale.

non-UE sau organizații internaționale.

#### e. Asigurarea unui cadru robust pentru modelele de bază, generale și cu dublu scop de IA

Reglementările trebuie să prevadă reguli clare cu privire la **sistemele de IA cu scop general și de bază**. Având în vedere versatilitatea acestora, ele pot crea riscuri importante legate de drepturile fundamentale și ar trebui să fie tratate ca sisteme cu grad ridicat de risc. Cel puțin, Legea ar trebui să introducă cerințe tehnice robuste, creșterea obligațiilor privind transparența și asigurarea monitorizării umane eficiente.

#### f. Asigurarea aplicării reglementării în activități de cercetare

ENNHRI este, de asemenea, îngrijorată de propunerea Consiliului de a exclude aplicarea reglementării „oricărei activități de cercetare și dezvoltare privind sistemele de inteligență artificială” (articolul 2.2.7). O excludere a acestor activități din domeniul de aplicare a reglementării ar submina substanțial eficacitatea acestuia. În special, ar submina obiectivul conform căruia sistemele de IA trebuie să fie dezvoltate și concepute de la început într-o manieră care reduce riscurile pentru drepturile fundamentale.

## 2. Îmbunătățirea transparenței, răspunderii și măsurilor reparatorii

#### a. Asigurarea evaluărilor adecvate de impact asupra drepturilor fundamentale

ENNHRI salută amendamentele înaintate de Parlamentul European asupra **evaluărilor de impact asupra drepturilor fundamentale (EIDF)**. În timp ce obligația de a efectua o evaluare de impact asupra drepturilor fundamentale este limitată la sistemele de IA cu grad ridicat de risc, sistemele de IA care nu sunt considerate ca fiind cu grad ridicat de risc ar putea, de asemenea, afecta negativ persoanele care sunt (conștient sau neconștient) supuse unui asemenea sistem. ENNHRI subliniază că **(o formă de) EIDF** ar trebui să fie obligatorie pentru furnizori și utilizatori înainte de orice utilizare pentru **toate sistemele de IA**. Sistemele de IA care nu intră în categoria celor cu grad ridicat de risc ar trebui, cel puțin, să facă obiectul unei evaluări periodice „ușoare”, cu participarea reală a părților interesate, astfel încât posibilele riscuri semnificative să fie detectate din timp și, în acest caz, să se realizeze o EIDF integrală pentru a le revizui și include în categoria de sisteme de IA cu grad ridicat de risc. Pentru a evita ca această formă „ușoară” de EIDF să reprezinte doar o formalitate, ar trebui să presupună, ca cerință minimă, cartarea și documentarea posibilelor riscuri pentru drepturile fundamentale, evaluarea acestor riscuri în timpul evaluărilor periodice și raportarea către autoritățile naționale de supraveghere dacă are loc un posibil risc.

În plus, în ceea ce privește frecvența, o (formă de) EIDF ar trebui realizată periodic pe întreg ciclul de viață a sistemului IA, nu doar înainte de punerea acestuia în funcțiune sau la momentul la care utilizatorul consideră că criteriile prevăzute de amendament (articolul 29 lit. A)) nu mai sunt respectate.

Întrebarea dacă un sistem IA servește scopului pentru care este destinat ar trebui să fie una dintre primele întrebări care trebuie luate în considerare. Dacă un sistem de IA nu (mai) servește scopului pentru care a fost creat, utilizatorul ar trebui să se abțină de la utilizarea acestuia. ENNHRI recomandă

ca acest lucru să fie specificat în textul Legii privind inteligența artificială.

În aceeași măsură, este important să se prevadă explicit **participarea reală a părților interesate**, în special a grupurilor marginalizate și vulnerabile, în procesul de evaluare a impactului (de exemplu, articolul 43.3)

#### **b. Extinderea obligației de a înregistra sistemele de IA**

Un sistem de înregistrare pentru IA, precum propunerea de bază de date a UE, este un element important pentru obținerea transparenței. În plus, permite societății să înțeleagă pentru ce scop și în ce context se utilizează inteligența artificială și în ce măsură poate fi/este afectată fiecare persoană de aceasta. În prezent, cerința de înregistrare se aplică doar sistemelor cu grad ridicat de risc. **ENNHRI recomandă înregistrarea obligatorie a tuturor sistemelor de IA care realizează sau asistă în procesul de luare de decizii cu privire la persoane sau în procesul de evaluare a acestora**, precum sisteme care încearcă să prezică comportamentul sau sisteme care sortează candidaturi eligibile pentru locuri de muncă, acces în învățământ superior etc. Deși unele tipuri de sisteme pot avea un impact (de amploare) asupra (unei părți a) vieții unei persoane, acestea nu sunt întotdeauna clasificate ca fiind cu grad ridicat de risc.

**În ceea ce privește sectorul public, toate sistemele de IA utilizate ar trebui făcute publice** datorită poziției pe care o are guvernul față de cetățeni și posibile consecințe (de amploare) pe care le pot avea deciziile guvernului. În plus, organizațiile din sectorul privat ar trebui încurajate de Legea privind inteligența artificială să înregistreze la rândul lor sistemele bazate pe IA pe care le folosesc.

Totodată, ENNHRI ia notă de faptul că transparența luării deciziilor de către organismele publice nu este abordată nici în textul Legii privind inteligența artificială, nici în amendamente. Este de dorit să se **standardizeze cerințele în materie de transparență pentru deciziile organismelor publice referitoare la persoane și să se ofere îndrumări cu privire la ce informații ar trebui incluse**. ENNHRI consideră că atunci când se iau decizii cu privire la persoane, organismele publice ar trebui să explice într-o manieră cuprinzătoare nu doar faptul că au făcut obiectul unui sistem de IA și felul în care funcționează algoritmul (conform articolului 52), ci și cum a funcționat pentru persoana respectivă în acel caz specific și cum pot obține măsuri reparatorii.

#### **c. Asigurarea dreptului la un remediu eficient**

ENNHRI salută amendamentele Parlamentului European cu privire la măsurile reparatorii (articolul 68 lit. a, b, c și d), respectiv, **introducerea dreptului de a depune o plângere la autoritatea națională de supraveghere**.

Aceste prevederi sunt esențiale și trebuie să rămână în textul final. Cu toate acestea, trebuie să fie consolidate în conformitate cu articolul 47 al Cartei drepturilor fundamentale a Uniunii Europene privind dreptul la o cale de atac eficientă și la un proces echitabil.

O cale de atac poate fi considerată eficientă conform articolului 47 al Cartei UE doar când este accesibilă persoanei în cauză, ceea ce presupune un nivel minim de transparență și informații cu privire la sistemul

de IA în cauză. ENNHRI salută articolul 68 lit. c, care prevede **dreptul la explicație** și subliniază că acest drept ar trebui să fie însoțit de o **EIDF disponibilă public** astfel încât aceasta să fie reală (II. a). Mai mult, persoanele afectate de sisteme IA ar trebui să fie **notificate când sunt afectate de deciziile și rezultatele obținute prin asistență IA**. Atunci când furnizorii sau utilizatorii nu respectă una dintre aceste obligații, sarcina probei ar trebui să revină furnizorului/utilizatorului și nu celor afectați, ceea ce ar face ineficient dreptul la o cale de atac.

În cele din urmă, ENNHRI subliniază necesitatea de a aborda corespunzător impactul colectiv și societal asupra drepturilor fundamentale al sistemelor de IA și salută punctul 3.5 din expunerea de motive a Legii privind inteligența artificială și articolul 68 lit. d propus în acest sens. Amendamentul propus nu prevede o protecție adecvată pentru toate grupurile afectate, întrucât nu toți cei care sunt supuși unui sistem IA sunt „consumatori” (respectiv, implicați printr-o relație contractuală cu cel care pune în funcțiune sistemul bazat pe IA). **Dreptul de reprezentare a tuturor persoanelor fizice** este esențial pentru a asigura dreptul la o cale de atac eficientă. ENNHRI recomandă ca organizațiile de interes public să poată depună plângeri la autoritatea de supraveghere, inclusiv în numele lor și fără a exista cerința unei victime identificabile în conformitate cu articolul 80 din RGPD „Reprezentarea persoanelor vizate”.

### 3. Supraveghere eficientă în cooperare cu Instituțiile Naționale pentru Drepturile Omului

#### a. Asigurarea cooperării reale cu structurile existente de drepturile omului

ENNHRI subliniază importanța mecanismelor de supraveghere și de punere în aplicare independente la nivel național și al UE, mandatate să primească și să răspundă la plângeri și salută amendamentele Parlamentului (preambul (84 a) și articolul 68 lit. a).

ENNHRI salută abordarea de punere în aplicare generală propusă în Legea privind inteligența artificială pentru a exista o **coordonare** a autorităților de supraveghere relevante (**articolul 63**) și salută amendamentele Parlamentului European care subliniază explicit importanța **cooperării cu structurile naționale de drepturile omului**, precum INDO-urile, în **considerentul 79**. ENNHRI reamintește că membri săi, prin mandatul lor vast de a promova și proteja drepturile omului, prin puterile și expertiza lor, pot furniza asistență la nivel național pentru a se asigura că orice utilizare a sistemelor de IA respectă standardele existente în materie de IA. Un obiectiv specific al reglementării este de a se asigura faptul că sistemele de IA puse și utilizate pe piața Uniunii sunt sigure și că respectă legislația existentă în materie de drepturi fundamentale. Pentru a consolida eficient aplicarea drepturilor fundamentale, autoritățile de supraveghere ar trebui să **coopereze cu mecanismele existente de aplicare a drepturilor fundamentale**, nu doar să le coordoneze. Cooperarea interinstituțională dintre autoritățile de supraveghere și alte autorități care protejează drepturile fundamentale este concretizată în articolul 64, care prevede **accesul la date și la documentație și posibilitatea de a declanșa investigații**. Cooperarea eficientă presupune **măsuri de siguranță privind accesibilitatea și claritatea, precum și resurse pentru mecanismele existente de aplicare a drepturilor fundamentale, precum INDO-uri, pentru a asigura cooperarea reală în implementarea Legii privind inteligența**

**artificială a UE.** ENNHRI recomandă specificarea acestui element explicit în textul Legii privind inteligența artificială.

#### **b. Asigurarea alocării unor resurse suficiente**

Legea privind inteligența artificială ar trebui să asigure că vor fi alocate resurse adecvate autorității naționale de supraveghere pentru a-și putea desfășura mandatul eficient, inclusiv în ceea ce privește finanțarea, personalul și expertiza. ENNHRI salută amendamentele înaintate de Parlamentul European la articolul 59, subliniind nevoia de **personal specializat în cadrul autorităților naționale de supraveghere**, inclusiv o **înțelegere profundă a drepturilor fundamentale**. Pentru a asigura aceste cunoștințe necesare, ENNHRI propune amendarea articolului 59 astfel încât să includă faptul că formarea personalului autorităților de supraveghere în domeniul nediscriminării și al drepturilor fundamentale este sprijinită de colaborarea cu INDO-urile și alte autorități sau organisme naționale relevante care supraveghează aplicarea legislației Uniunii în materia drepturilor fundamentale. Evident, această nevoie de expertiză se aplică și mecanismelor din domeniul căilor de atac.

#### **4. Abținerea autorităților de securitate națională, de aplicare a legii și de migrație de la supraveghere discriminatorie și vătămătoare**

##### **a. Interzicerea practicilor biometrice și predictive discriminatorii**

ENNHRI salută amendamentele propuse de Parlamentul European referitoare la migrație, inclusiv **interzicerea deplină a supravegherii biometrice** (articolul 5.1). Interzicerea deplină a identificării biometrice în timp real, precum utilizarea recunoașterii faciale, în spații publice și majoritatea utilizărilor post sau retroactive a identificării biometrice în timp real, precum și interzicerea recunoașterii emoțiilor în aplicarea legii, în gestionarea frontierelor, la locul de muncă și în educație sunt de importanță esențială în contextul migrației. ENNHRI salută, de asemenea, interzicerea **categorisirii biometrice discriminatorii, activități polițienești predictive**, precum și **extragerea în masă a datelor biometrice** pentru a crea baze de date de supraveghere.

ENNHRI ia notă de faptul că Legea privind inteligența artificială poate fi consolidată în continuare pentru a proteja migranții. Utilizarea de analize predictive cu scopul de a reduce sau preveni migrația ar trebui să fie interzise.

Aceste sisteme generează predicții referitoare la locurile unde există riscul de „migrație ilegală”, iar asemenea tehnologii prezintă riscul de a facilita încălcări de drepturile omului precum respingeri și violențe la frontieră, subminând dreptul de a solicita azil și principiul nereturnării.

#### **b. Includerea bazelor de date ale UE privind migrația în domeniul de aplicare a Legii privind inteligența artificială**

ENNHRI salută amendamentul Parlamentului de a extinde aplicarea Legii privind inteligența artificială la **sisteme de IA existente care fac parte din sisteme IT de dimensiuni mari stabilite de legislația Uniunii Europene (articolul 83)**. Acestea includ majoritatea bazelor de date existente în prezent, utilizate în cadrul UE pentru a colecta, partaja și utiliza informații din cadrul sistemelor de migrație și aplicarea legii (a se vedea anexa IX). Această excludere din propunerile Consiliului și Comisiei facilitează încălcări sistemice ale drepturilor fundamentale, inclusiv prin crearea automată a profilului de risc al migranților.

#### **c. Evitarea lacunelor pentru aplicarea legii și controlul migrației**

ENNHRI ia notă, de asemenea, de faptul că poziția Consiliului **introduce o serie de excepții privind aplicabilitatea Legii privind inteligența artificială referitoare la sistemele folosite de organismele de aplicare a legii și control al migrației**. Acestea reduc considerabil necesitatea supravegherii umane (articolul 14.5) sau obligația de a înregistra operatorii sistemelor de IA de risc ridicat (articolul 51.2). Această abordare nu recunoaște faptul că utilizarea inteligenței artificiale în contextul aplicării legii și a controlului migrației poate duce la încălcări sistematice a drepturilor fundamentale ale persoanelor vulnerabile. ENNHRI recomandă ca cerințele de supraveghere în contextele respective să fie consolidate, în loc de a fi slăbite.

Co-funded by  
the European Union

