

Bruxelles, 12 septembrie 2022
(OR. en)

12302/22

LIMITE

JUR 579
TELECOM 364
COSI 217
JAI 1155
ENFOPOL 451

**Dosar interinstituțional:
2021/0106(COD)**

AVIZUL SERVICIULUI JURIDIC¹

Sursă:	Serviciul juridic
Subiect:	Propunere de regulament al Parlamentului European și al Consiliului de stabilire a unor norme armonizate privind inteligența artificială – Pertinența temeiurilor juridice reprezentate de articolele 114 și 16 din TFUE în legătură cu dispozițiile aplicabile autorităților judiciare și de aplicare a legii

I. INTRODUCERE

1. Propunerea de regulament stabilește norme armonizate pentru introducerea pe piață și punerea în funcțiune a sistemelor de inteligență artificială („sisteme de IA”) în Uniune („propunerea de regulament”)².

¹ Prezentul document conține consultanță juridică care este protejată conform articolului 4 alineatul (2) din Regulamentul (CE) nr. 1049/2001 al Parlamentului European și al Consiliului din 30 mai 2001 privind accesul public la documentele Parlamentului European, ale Consiliului și ale Comisiei și care nu este pusă la dispoziția publicului de către Consiliul Uniunii Europene. Consiliul își rezervă toate drepturile legale în privința publicării neautorizate.

² Documentul 8115/21.

2. În cadrul reuniunii Grupului de lucru pentru telecomunicații și societatea informațională din 7 aprilie 2022, Serviciul juridic al Consiliului („SJC”) a intervenit cu privire la pertinența temeiului juridic dublu (articolele 16 și 114 din TFUE) pentru propunerea de regulament privind sistemele de inteligență artificială („sistemele de IA”). Explicațiile au confirmat faptul că articolele 16 și 114 din TFUE sunt temeiurile juridice corecte ale propunerii și că recurgerea la articolul 87 alineatul (2) din TFUE, în loc de articolul 114 din TFUE, nu este adecvată. La solicitarea grupului de lucru, prezentul aviz furnizează în scris și dezvoltă suplimentar intervenția reprezentantului SJC în cadrul respectivei reuniuni.
3. Sistemele de IA sunt definite la articolul 3 punctul 1 din propunerea de regulament. În general, acestea corespund anumitor tipuri de software. Propunerea de regulament se aplică atât furnizorilor care introduc sisteme de IA pe piață, cât și furnizorilor care pun în funcțiune sisteme de IA. În plus, propunerea de regulament se aplică și utilizatorilor. Un furnizor poate fi o persoană fizică sau juridică sau o autoritate publică/un organism public 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. Un utilizator poate fi orice persoană fizică sau juridică, autoritate publică, agenție sau orice alt organism care utilizează un sistem de IA aflat sub autoritatea sa.

4. În conformitate cu definițiile de la articolul 3, autoritățile de aplicare a legii și autoritățile judiciare ar putea fi considerate furnizori și/sau utilizatori ai unui sistem de IA. Sistemele de IA al căror scop preconizat, astfel cum este definit de furnizor, este asigurarea respectării legii sau administrarea justiției sunt clasificate ca având un grad ridicat de risc în temeiul anexei III. Ca atare, acestea fac obiectul unor cerințe esențiale (gestionarea riscurilor, testare, guvernanta datelor, documentația tehnică, transparența, supravegherea umană, acuratețea, robustețea și securitatea cibernetică) și al unor obligații (cum ar fi sistemele de management al calității, documentația tehnică, evaluarea conformității, acțiunile corective, obligația de informare, obligațiile importatorilor și distribuitorilor), precum și al unor standarde și al evaluării conformității. Aceste norme armonizate se inspiră din cele care se aplică în cazul siguranței produselor în Directiva 2006/42/CE (echipamentele tehnice)³ și în Regulamentul 2017/745 (dispozitivele medicale)⁴.
5. În ceea ce privește sistemele de IA care implică utilizarea sistemelor de identificare biometrică la distanță „în timp real” în spațiile accesibile publicului în scopul asigurării respectării legii, acestea se încadrează în categoria sistemelor de IA interzise. Această interdicție de utilizare a sistemelor de IA face totuși obiectul unor excepții. Într-adevăr, utilizarea unor astfel de sisteme poate fi autorizată sau nu de statele membre. În cazul în care sunt autorizate, ele fac obiectul unor restricții și garanții detaliate pentru a limita utilizarea lor la ceea ce este strict necesar și pentru a proteja dreptul fundamental la protecția datelor cu caracter personal. Aceste restricții și garanții sunt prevăzute în propunerea de regulament în temeiul articolului 16 din Tratatul privind funcționarea Uniunii Europene („TFUE”) și trebuie să fie completate de dreptul național. Articolul 5 alineatul (1) litera (d) și articolul 5 alineatele (2), (3) și (4) din propunerea de regulament constituie o *lex specialis* față de Directiva 2016/680 (Directiva privind protecția datelor în materie de asigurare a respectării legii), care a fost adoptată în temeiul articolului 16 alineatul (2) din TFUE.

³ Directiva 2006/42/CE a Parlamentului European și a Consiliului din 17 mai 2006 privind echipamentele tehnice și de modificare a Directivei 95/16/CE, JO L 157, 9.6.2006, p. 24-86.

⁴ Regulamentul (UE) 2017/745 al Parlamentului European și al Consiliului din 5 aprilie 2017 privind dispozitivele medicale, de modificare a Directivei 2001/83/CE, a Regulamentului (CE) nr. 178/2002 și a Regulamentului (CE) nr. 1223/2009 și de abrogare a Directivelor 90/385/CEE și 93/42/CEE ale Consiliului, JO L 117, 5.5.2017, p. 1-175.

În conformitate cu articolul 5 alineatul (1) litera (d), obiectivele acestor sisteme se limitează la:

- i) căutarea specifică a potențialelor victime ale infracționalității, inclusiv a copiilor dispăruți;
- ii) prevenirea unei amenințări specifice, substanțiale și iminente la adresa vieții sau a siguranței fizice a persoanelor fizice sau a unui atac terorist;
- iii) detectarea, localizarea, identificarea sau urmărirea penală a autorului unei infracțiuni sau a unei persoane suspectate de o infracțiune menționată la articolul 2 alineatul (2) din Decizia privind mandatul european de arestare⁵ și pedepsită în statul membru în cauză cu o pedeapsă sau o măsură de siguranță privativă de libertate pentru o perioadă maximă de cel puțin trei ani, astfel cum este stabilit de legislația statului membru respectiv.

În conformitate cu articolul 5 alineatul (3), utilizarea unor astfel de tehnologii de către autoritățile de aplicare a legii trebuie să facă obiectul unei autorizări prealabile din partea unei autorități judiciare sau administrative. Cu toate acestea, într-o situație de urgență justificată în mod corespunzător, utilizarea sistemului poate începe fără autorizație, iar autorizația poate fi solicitată în timpul utilizării sau ulterior.

În temeiul articolului 5 alineatul (4), un stat membru poate decide să autorizeze utilizarea sistemelor de identificare biometrică la distanță „în timp real” în spațiile accesibile publicului în scopul asigurării respectării legii și să definească normele detaliate necesare pentru solicitarea, eliberarea și exercitarea autorizației prealabile, precum și infracțiunile aferente.

6. Temeiurile juridice ale propunerii de regulament sunt articolul 16 din TFUE (protecția datelor cu caracter personal) și articolul 114 din TFUE (funcționarea pieței interne). Prin urmare, se pune problema pertinentei acestor temeuri juridice în raport cu normele armonizate aplicabile sistemelor de IA furnizate sau utilizate de autoritățile de aplicare a legii și de autoritățile judiciare.

⁵ Decizia-cadru 2002/584/JAI a Consiliului din 13 iunie 2002 privind mandatul european de arestare și procedurile de predare între statele membre, JO L 190, 18.7.2002, p. 1.

7. Prezentul aviz se axează în primul rând pe relevanța temeiului juridic reprezentat de articolul 114 din TFUE, în contextul special al autorităților de aplicare a legii care sunt menționate în mai multe dispoziții ale propunerii de regulament, și anume în ceea ce privește sistemele de identificare biometrică la distanță „în timp real” din spațiile accesibile publicului și sistemele de IA cu grad ridicat de risc menționate la punctul 6 din anexa III. Prin urmare, avizul răspunde la întrebarea dacă articolul 87 alineatul (2) din TFUE (cooperarea polițienească) ar fi un temei juridic mai adecvat pentru a reglementa furnizarea și utilizarea sistemelor de IA de către autoritățile de aplicare a legii, în loc de articolul 114 din TFUE (secțiunea II). Prin analogie, concluzia prezentei note poate fi aplicată autorităților judiciare menționate în anexa III în ceea ce privește sistemele de IA cu grad ridicat de risc.
8. Prezenta notă abordează, de asemenea, relevanța temeiului juridic suplimentar reprezentat de articolul 16 din TFUE și aplicarea Protocoalelor 21 și 22 în contextul utilizării sistemelor de identificare biometrică la distanță „în timp real” în spațiile accesibile publicului de către autoritățile de aplicare a legii (secțiunea III).

II. PERTINENȚA TEMEIULUI JURIDIC REPREZENTAT DE ARTICOLUL 114 DIN TFUE

9. În conformitate cu jurisprudența constantă, temeiul juridic al unui act al Uniunii nu depinde de convingerea unei instituții în ceea ce privește obiectivul urmărit, ci trebuie să fie determinat conform unor criterii obiective care pot fi supuse controlului jurisdicțional, printre care figurează în special scopul și conținutul măsurii. Dacă prin analizarea unei măsuri se dovedește că aceasta urmărește o dublă finalitate sau că are o componentă dublă și dacă una dintre acestea poate fi identificată ca fiind principală ori preponderentă, iar cealaltă nu este decât accesorie, măsura respectivă trebuie să aibă un temei juridic unic, și anume temeiul impus de finalitatea sau de componenta principală ori preponderentă. Numai în cazuri excepționale, dacă se stabilește că actul urmărește simultan mai multe obiective legate în mod indisolubil, fără ca unul dintre ele să fie secundar sau indirect în raport cu celălalt, actul în cauză poate fi adoptat pe baza diferitor temeiuri juridice corespunzătoare, cu excepția cazului în care aceste temeiuri juridice prevăd proceduri care sunt incompatibile între ele. Ar trebui remarcat, de asemenea, că articolul 114 alineatul (1) prima teză din TFUE precizează că dispozițiile articolului se aplică „[c]u excepția cazului în care tratatele dispun altfel”. Drept urmare, utilizarea articolului 114 din TFUE nu se justifică decât dacă nicio dispoziție mai specifică nu este capabilă să constituie temeiul juridic pentru adoptarea măsurii în cauză⁶. Dacă tratatul conține o dispoziție mai specifică ce poate constitui temeiul juridic pentru măsura respectivă, măsura trebuie să se întemeieze pe respectiva dispoziție⁷.

⁶ Avizul Serviciului juridic al Consiliului din 17 mai 2016, 9007/16, punctul 6.

⁷ Hotărârea din 29 aprilie 2004, Comisia/Consiliul, C-338/01, EU:C:2004:253, punctul 60.

A. SCOPUL PROPUNERII DE REGULAMENT

10. Propunerea de regulament armonizează introducerea pe piață, punerea în funcțiune și utilizarea unui tip special de software (sistemele de IA). Faptul că autoritățile publice și operatorii privați pot fi furnizori sau utilizatori ai unor astfel de sisteme de IA nu este incompatibil în sine cu temeiul juridic reprezentat de articolul 114 din TFUE⁸.
11. În plus, faptul că autoritățile de aplicare a legii sau cele care acționează în numele acestora pot fi printre furnizorii sau utilizatorii unor astfel de sisteme de IA nu este suficient pentru a justifica recurgerea la temeiul juridic reprezentat de articolul 87 din TFUE. Trebuie analizate scopul și conținutul propunerii de regulament pentru a stabili dacă acest lucru este necesar.
12. Propunerea de regulament urmărește, în general, inclusiv în ceea ce privește sistemele de identificare biometrică la distanță „în timp real” în spațiile accesibile publicului și sistemele de IA cu grad ridicat de risc, să asigure un nivel constant și ridicat de protecție în întreaga Uniune, prevenind în același timp posibilitatea ca divergențele să împiedice libera circulație a sistemelor de IA și a produselor și serviciilor conexe în cadrul pieței interne. Propunerea stabilește obligații uniforme pentru operatori și garantează protecția uniformă a motivelor imperative de interes public major și a drepturilor persoanelor pe întreaga piață internă (considerentul 2). Mai precis, propunerea de regulament stabilește norme care să reglementeze introducerea pe piață și punerea în funcțiune a anumitor sisteme de IA, asigurând astfel buna funcționare a pieței interne și permițând acestor sisteme să beneficieze de principiul liberei circulații a bunurilor și serviciilor (considerentul 5). În general, propunerea urmărește să instituie o IA de încredere încă din faza de proiectare, aplicabilă în toate domeniile, cu un set complet de norme pentru dezvoltarea, comercializarea și utilizarea produselor, a serviciilor și a sistemelor bazate pe IA. Având în vedere că IA a fost introdusă deja într-un număr mare de servicii și produse și că acest lucru va continua să se întâmple în viitor, propunerea urmează o logică a pieței interne prin stabilirea unui „cadru privind siguranța produselor” construit în jurul unui set de patru categorii de risc. Propunerea impune cerințe pentru intrarea pe piață și certificarea sistemelor de IA cu grad ridicat de risc prin intermediul unei proceduri obligatorii de marcaj CE.

⁸ A se vedea avizul juridic al SJC (documentul ST 11395/14, punctele 39-41) și precedentele, cum ar fi Directiva (UE) 2016/2102, Directivele 2014/24/UE, 2014/25/UE și 2014/23/UE.

13. Niciunul dintre scopurile declarate ale propunerii de regulament nu se referă la asigurarea unor obiective de siguranță publică. Chiar dacă obiectivele de siguranță publică urmează să fie îndeplinite indirect prin procesul de armonizare a introducerii pe piață/punerii în funcțiune/utilizării sistemelor de IA de către autoritățile de aplicare a legii, Curtea⁹, interpretând articolul 87 alineatul (2) din TFUE în lumina articolului 67 din TFUE, a afirmat că, pentru ca un act al Uniunii, având în vedere scopul și conținutul său, să se întemeieze pe primul dintre respectivele articole, acesta trebuie să fie direct legat de obiectivele prevăzute la articolul 67 din TFUE (și anume, în acest caz, prevenirea criminalității și cooperarea polițienească). Acest lucru este exclus în contextul propunerii de regulament, deoarece singurele norme armonizate privind utilizarea unor astfel de sisteme de către autoritățile de aplicare a legii sunt fie (1) norme de tipul celor privind siguranța produselor care se aplică în mod uniform tuturor furnizorilor și utilizatorilor în ceea ce privește introducerea pe piață/punerea în funcțiune sau utilizarea sistemelor de IA, fie (2) norme privind protecția datelor cu caracter personal pentru care a fost adăugat temeiul juridic reprezentat de articolul 16 din TFUE (a se vedea partea III de mai jos).
14. Într-o altă cauză¹⁰, chiar dacă obiectivul modificării Directivei privind armele de foc consta în asigurarea unui nivel mai ridicat de siguranță publică în raport cu amenințarea teroristă și cu alte forme de criminalitate, Curtea a statuat că armonizarea aspectelor referitoare la siguranța mărfurilor este unul dintre elementele esențiale pentru asigurarea bunei funcționări a pieței interne, întrucât reglementările disparate în această materie sunt susceptibile să creeze obstacole în calea comerțului¹¹.

⁹ Hotărârea din 6 mai 2014, Comisia Europeană/Parlamentul European și Consiliul Uniunii Europene, C-43/12, ECLI: EU:C:2014:298.

¹⁰ Hotărârea din 3 decembrie 2019, Republica Cehă/Parlamentul European, C482/17, EU:C:2019:1035.

¹¹ Ibid., punctul 57: „Or, având în vedere că particularitatea armelor de foc, în mod contrar celor susținute de Republica Polonă, este pericolozitatea acestora nu numai pentru utilizatori, ci și pentru publicul larg, astfel cum a arătat deja Curtea la punctul 54 din Hotărârea din 23 ianuarie 2018, Buhagiar și alții (C- 267/16, EU:C:2018:26), motive de siguranță publică par, după cum se amintește în al cincilea considerent al Directivei 91/477, indispensabile în cadrul unei reglementări privind achiziționarea și deținerea acestor mărfuri”. A se vedea, de asemenea, Hotărârea din 23 ianuarie 2018, Albert Buhagiar și alții/Minister for Justice, C-267/16, EU:C:2018:26, punctul 54: „În această privință, trebuie subliniat că, având în vedere riscul pentru securitatea persoanelor pe care îl prezintă armele de foc, libera lor circulație nu a putut fi atinsă decât prin intermediul unei încadrări stricte a condițiilor privind transferul acestora între statele membre, printre care figurează principiul autorizării prealabile de către statele membre vizate de un transfer al unor asemenea mărfuri”.

15. Obiectivele propunerii de regulament, inclusiv articolul 5 alineatul (1) litera (d) și articolul 5 alineatele (2), (3) și (4) privind utilizarea sistemelor de identificare biometrică la distanță „în timp real” în spațiile accesibile publicului în scopul asigurării respectării legii și dispozițiile referitoare la sistemele de IA cu grad ridicat de risc menționate la punctul 6 din anexa III, nu sunt direct legate de un obiectiv de siguranță publică. Dimpotrivă, propunerea răspunde principalelor preocupări legate de modul în care sistemele de IA afectează sănătatea, siguranța și drepturile fundamentale. Prin urmare, dispozițiile relevante sunt direct legate de obiectivul asigurării unor condiții de concurență echitabile în ceea ce privește introducerea pe piață/punerea în funcțiune sau utilizarea sistemelor de IA pe piața internă, protejând în același timp sănătatea, siguranța și drepturile fundamentale ale utilizatorilor.
16. Având în vedere cele de mai sus, principalul obiectiv al propunerii de regulament este de a îmbunătăți funcționarea pieței interne în sensul articolului 114 din TFUE, iar obiectivele menționate la articolul 67 din TFUE nu sunt legate decât în mod indirect și accesoriu de acest obiectiv principal.

B. CONȚINUTUL PROPUNERII DE REGULAMENT

17. Propunerea de regulament conține, în esență, norme privind ceea ce este necesar pentru a introduce pe piață (sau pentru a pune în funcțiune) un anumit produs (un software de IA), astfel încât să se asigure că acesta este sigur și respectă drepturile fundamentale. Ea stabilește un set complet de norme pentru dezvoltarea, comercializarea și utilizarea produselor, a serviciilor și a sistemelor bazate pe IA. Propunerea de regulament nu obligă autoritățile de aplicare a legii să utilizeze un sistem de IA care este introdus în mod legal pe piață și nici nu reglementează în mod direct modul în care autoritățile de aplicare a legii ar trebui să utilizeze un astfel de sistem de IA. În schimb, ea delimitează în mod clar situațiile în care utilizarea preconizată este considerată ca prezentând un grad ridicat de risc pentru simplul motiv că un sistem de IA va fi utilizat de autoritățile de aplicare a legii sau de autoritățile judiciare.

18. De altfel, articolul 29 din propunerea de regulament conține norme privind condițiile de utilizare a sistemelor de IA cu grad ridicat de risc, dar o astfel de dispoziție nu este specifică sectorului, are un domeniu de aplicare limitat (în principal în ceea ce privește instrucțiunile de utilizare a produsului) și este intrinsec legată de obligațiile impuse dezvoltatorilor de sisteme de IA în temeiul propunerii de regulament. De asemenea, propunerea oferă statelor membre o anumită marjă de manevră pentru a prevedea norme suplimentare privind utilizarea unor astfel de sisteme de IA cu grad ridicat de risc. În ceea ce privește sistemele de identificare biometrică la distanță „în timp real” în spațiile accesibile publicului utilizate în scopul asigurării respectării legii (articolul 5), propunerea de regulament reglementează parțial utilizarea unor astfel de sisteme din perspectiva protecției datelor în temeiul articolului 16 din TFUE (a se vedea partea III de mai jos).
19. În plus, numai statele membre pot decide să prevadă posibilitatea de a autoriza integral sau parțial utilizarea unor astfel de sisteme de identificare biometrică la distanță „în timp real”. Condițiile specifice pentru o astfel de utilizare urmează să fie stabilite în dreptul național, dar trebuie să respecte criteriile și garanțiile generale prevăzute în regulament: autorizarea judiciară sau administrativă prealabilă, solicitarea, eliberarea și exercitarea autorizației prealabile, precum și indicarea infracțiunilor în legătură cu care pot fi utilizate astfel de sisteme.

20. Sistemele de IA reprezintă un tip special de software. Normele armonizate aplicabile introducerii pe piață sau punerii în funcțiune/utilizării sistemelor de IA sunt, prin urmare, norme armonizate de tipul celor privind siguranța produselor. Acestea se aplică în mod uniform, fără a face distincție între utilizatorii publici și cei privați. În conformitate cu considerentele relevante din propunerea de regulament, ar trebui, prin urmare, să se asigure un nivel ridicat și constant de protecție în întreaga Uniune. În același timp, ar trebui prevenite divergențele care împiedică libera circulație a sistemelor de IA și a produselor și serviciilor conexe în cadrul pieței interne. Acest lucru ar fi obținut prin stabilirea unor obligații uniforme pentru operatori și garantarea protecției uniforme a motivelor imperative de interes public major și a drepturilor persoanelor pe întreaga piață internă în temeiul articolului 114 din TFUE¹².
21. Propunerea de regulament conține mai multe trimiteri la asigurarea respectării legii, la gestionarea controlului la frontiere și la administrarea justiției în anexa III privind sistemele de IA cu grad ridicat de risc (punctele 6, 7 și, respectiv, 8). Acestea includ o enumerare detaliată și exhaustivă corespunzând articolului 6 alineatul (2), în plus față de alte sisteme cu grad ridicat de risc în ceea ce privește riscurile pentru siguranța produselor menționate la articolul 6 alineatul (1). Într-adevăr, în conformitate cu articolul 6 alineatul (1), unele sisteme de IA trebuie considerate ca prezentând un grad ridicat de risc prin definiție din cauza gravității preconizate și a riscurilor ridicate la adresa drepturilor fundamentale, a sănătății și a siguranței. Alte sisteme considerate ca prezentând un grad ridicat de risc și enumerate în anexa III includ educația, gestionarea infrastructurilor critice, ocuparea forței de muncă, identificarea și clasificarea biometrică, precum și accesul la servicii publice și private esențiale.

¹² Prin urmare, este necesar un cadru juridic al Uniunii care să stabilească norme armonizate privind inteligența artificială pentru a încuraja dezvoltarea, utilizarea și adoptarea inteligenței artificiale pe piața internă și care să asigure, în același timp, un nivel ridicat de protecție a intereselor publice, cum ar fi sănătatea, siguranța și protecția drepturilor fundamentale, astfel cum sunt recunoscute și protejate de dreptul Uniunii. Pentru atingerea acestui obiectiv, ar trebui stabilite norme care să reglementeze introducerea pe piață și punerea în funcțiune a anumitor sisteme de IA, asigurând astfel buna funcționare a pieței interne și permițând acestor sisteme să beneficieze de principiul liberei circulații a bunurilor și serviciilor (a se vedea considerentele 2 și 5 din propunere).

22. Cu toate acestea, astfel de norme privind sistemele de IA cu grad ridicat de risc nu prevăd dacă autoritățile de aplicare a legii și autoritățile judiciare (sau cele din celelalte domenii identificate) ar trebui sau nu să utilizeze aceste sisteme. Regulamentul propus va produce efecte doar indirect asupra dezvoltării efective a sistemelor de IA care pot fi utilizate de autoritățile de aplicare a legii și asupra sistemelor de IA utilizate în prezent și în viitor. Astfel, normele se referă la sistemele de IA care sunt „destinate a fi utilizate” de către astfel de autorități [a se vedea, de exemplu, articolul 3 punctul 12, articolul 8 alineatul (2) și anexa III]. Consecința includerii unui anumit sistem de IA pe lista celor cu grad ridicat de risc este aplicarea unui set specific de norme privind gestionarea riscurilor, guvernanta datelor și specificațiile tehnice. Utilizatorii unor astfel de sisteme de IA cu grad ridicat de risc trebuie să respecte instrucțiunile de utilizare, să păstreze fișierele de jurnalizare și să efectueze evaluări ale impactului asupra protecției datelor.
23. În plus, alte obligații ale utilizatorilor decât cele referitoare la instrucțiunile de utilizare pot fi prevăzute în dreptul Uniunii sau în dreptul național, fără a aduce atingere libertății utilizatorului de a-și organiza propriile resurse și activități în scopul punerii în aplicare a măsurilor de supraveghere umană indicate de furnizor [articolul 29 alineatul (2) din propunerea de regulament]. Aceste norme prevăd garanții suplimentare în materie de drepturi fundamentale pentru sistemele de IA cu grad ridicat de risc.

24. Având în vedere cele de mai sus, ar trebui subliniat faptul că propunerea de regulament nu conține norme care urmăresc să permită sau să împiedice utilizarea de către autoritățile de aplicare a legii a unui sistem de IA cu grad ridicat de risc introdus pe piață. În virtutea normelor propuse, un sistem de IA dezvoltat sau utilizat de autoritățile de aplicare a legii va fi încadrat într-o categorie distinctă („grad ridicat de risc”) ca urmare a utilizării sale preconizate. Această utilizare ar fi reglementată de dreptul național și, într-o anumită măsură, ar fi decisă chiar de autoritățile de aplicare a legii. Într-adevăr, propunerea de regulament stabilește condiții minime de utilizare la articolul 29 (limitate la instrucțiunile de utilizare) pentru sistemele de IA cu grad ridicat de risc, inclusiv cele enumerate la punctele 6, 7 și 8 din anexa III, care vor fi completate de dreptul național. Prin urmare, ar trebui să se facă o distincție, în conformitate cu jurisprudența Curții, între, pe de o parte, scopul urmărit de propunerea de regulament, care nu este de a reglementa utilizarea sistemelor de IA de către autoritățile de aplicare a legii, și, pe de altă parte, efectele pe care le poate produce indirect¹³ și care sunt irelevante în scopul analizării pertinentei temeiului juridic.
25. Domeniile menționate la punctele 6, 7 și 8 (privind asigurarea respectării legii, migrația și, respectiv, administrarea justiției) nu sunt predominante în rândul sistemelor de IA cu grad ridicat de risc. Într-adevăr, în temeiul propunerii de regulament, un sistem de IA cu grad ridicat de risc nu este neapărat unul enumerat în anexa III. Majoritatea sistemelor cu grad ridicat de risc sunt, de fapt, cele enumerate în mod generic la articolul 6 alineatul (1) litera (a) și litera (b) din propunerea de regulament (în legătură cu siguranța produselor). Alte sisteme de IA cu grad ridicat de risc sunt enumerate în anexa III, care conține punctele 1 (identificarea biometrică), 2 (infrastructuri critice), 3 (educație și formare profesională) și 4 (ocuparea forței de muncă, gestionarea lucrătorilor și accesul la activități independente) care se referă la alte domenii decât justiția și afacerile interne („JAI”). Toți utilizatorii unor astfel de sisteme de IA cu grad ridicat de risc sunt supuși unui regim uniform instituit nu având în vedere statutul lor specific (de exemplu, faptul că sunt operatori economici sau autorități publice), ci din perspectiva protejării sănătății, a siguranței și a drepturilor fundamentale.

¹³ A se vedea Hotărârea Curții din 21 iunie 2018, Republica Polonă/Parlamentul European, Consiliul Uniunii Europene, C-5/16, EU:C:2018:483, punctele 63-68, și Hotărârea Curții din 22 iunie 2022, Leistritz AG/LH, C-534/20, EU:C:2022:495, punctul 28.

26. Prin urmare, propunerea de regulament conține norme armonizate privind introducerea pe piață, punerea în funcțiune și utilizarea sistemelor de IA, indiferent dacă acestea sunt utilizate de operatori privați sau de autorități publice, inclusiv, în mod incidental¹⁴, de autoritățile de aplicare a legii și de autoritățile judiciare.
27. Făcând abstracție de utilizarea sistemelor de identificare biometrică la distanță „în timp real” în spațiile accesibile publicului în scopul asigurării respectării legii, care face obiectul unor norme specifice privind prelucrarea datelor cu caracter personal (a se vedea partea III de mai jos), propunerea de regulament nu conține norme armonizate privind utilizarea sistemelor de IA cu grad ridicat de risc. Astfel cum s-a explicat la punctele 18 și 19 de mai sus, trimiterea la utilizarea sistemelor de IA cu grad ridicat de risc se referă, în esență, la instrucțiunile de utilizare a produsului (articolul 29) și este legată de obligațiile impuse programatorilor. Astfel cum s-a subliniat la punctul 22, decizia de a stabili dacă autoritățile de aplicare a legii sau autoritățile judiciare pot utiliza sau nu un sistem de IA cu grad ridicat de risc care este introdus pe piață în mod legal în temeiul propunerii de regulament aparține dreptului național și autorităților naționale.
28. Prin urmare, articolul 87 alineatul (2) din TFUE, în special litera (a), nu este un temei juridic pertinent pentru regulamentul propus. Normele din propunere nu promovează și nici nu împiedică colectarea, stocarea, prelucrarea, analizarea și schimbul de informații relevante. Pur și simplu, atunci când astfel de activități sunt efectuate de autoritățile de aplicare a legii, vor trebui respectate o serie de condiții nespecifice și armonizate pentru a garanta drepturile utilizatorilor. În mod similar, obiectivele declarate ale propunerii de regulament nu includ dezvoltarea unor tehnici comune de investigare. Cerințele propuse privind utilizarea sistemelor de IA cu grad ridicat de risc nu sunt specifice domeniului JAI și nu se referă la cooperarea polițienească *stricto sensu*, astfel cum este definită în TFUE.

¹⁴ A se vedea Avizul Curții referitor la Convenția de la Istanbul, A-1/19, EU:C:2021:198, în special punctele 298 și 301.

29. În ceea ce privește dispozițiile de la articolul 5 alineatul (4) din propunerea de regulament, un stat membru poate totuși decide să autorizeze utilizarea sistemelor de identificare biometrică la distanță „în timp real” în spațiile accesibile publicului în scopul asigurării respectării legii. În cazul în care decide astfel, statul membru are obligația de a stabili normele detaliate necesare pentru solicitarea, eliberarea și exercitarea autorizației prealabile, precum și infracțiunile aferente pentru a căror investigare sau urmărire penală este autorizată utilizarea¹⁵. Pe baza rezultatului discuțiilor din cadrul Consiliului, aceste norme propuse nu ar avea ca rezultat acordarea de noi competențe autorităților naționale respective. În schimb, utilizarea mecanismelor existente sau a eventualelor mecanisme viitoare este limitată în vederea asigurării apărării dreptului la viață privată și a datelor cu caracter personal.
30. Având în vedere cele de mai sus, articolul 114 din TFUE este singurul temei juridic pertinent pentru norme armonizate privind sistemele de IA cu grad ridicat de risc, inclusiv cele utilizate de autoritățile de aplicare a legii și de autoritățile judiciare, iar orice temei juridic JAI din partea a treia titlul V din TFUE, cum ar fi articolul 87 din TFUE în ceea ce privește respectivele norme armonizate, nu este nici justificat, nici pertinent.

¹⁵ Este demn de remarcat faptul că articolul 5 alineatul (4) din propunere prezintă anumite caracteristici similare cu articolul 15 alineatul (1) din Directiva 2002/58 asupra confidențialității și comunicațiilor electronice. În special, acesta prevede posibilitatea ca statele membre să deroge de la anumite interdicții prevăzute în dreptul Uniunii. Având în vedere jurisprudența constantă, dispozițiile naționale menite să deroge de la respectivele interdicții vor intra în mod necesar în domeniul de aplicare al dreptului Uniunii care, la rândul său, va determina aplicarea Cartei în privința lor.

III. PERTINENȚA ARTICOLULUI 16 DIN TFUE CA TEMEI JURIDIC SUPLIMENTAR

31. Propunerea de regulament include articolul 16 din TFUE ca temei juridic, referitor la prelucrarea datelor cu caracter personal în domeniul asigurării respectării legii, iar considerentele sale 25 și 26 includ o trimitere la articolul 6a din Protocolul nr. 21 și la articolul 2a din Protocolul nr. 22 privind prelucrarea datelor cu caracter personal în domeniul prevenirii criminalității. Din perspectiva Comisiei, articolul 16 din TFUE este menit să servească exclusiv ca temei juridic pentru dispozițiile care impun restricții în ceea ce privește prelucrarea datelor biometrice cu caracter personal într-un mod complementar față de Directiva 2016/680 („Directiva privind prelucrarea datelor cu caracter personal în domeniul asigurării respectării legii”). Articolul 5 alineatul (1) litera (d) este formulat ca o interdicție în principiu, căreia i se aplică un set de trei excepții. În mod concret, utilizarea sistemelor de identificare biometrică la distanță „în timp real” în spațiile accesibile publicului în scopul asigurării respectării legii este interzisă, cu excepția cazului în care este strict necesară (a) pentru a efectua căutări specifice ale potențialelor victime ale criminalității, (b) a preveni un atac terorist iminent sau un atac la adresa integrității fizice/vieții unei persoane, (c) a localiza sau a identifica ori urmări penal un autor al unei infracțiuni sau o persoană suspectată de o infracțiune gravă (cu o trimitere la mandatul european de arestare). Această utilizare specifică a sistemelor de IA de către autoritățile de aplicare a legii face obiectul unor cerințe suplimentare, menționate la articolul 5 alineatele (2), (3) și (4), în particular o evaluare a necesității și a proporționalității, o autorizare prealabilă (cu excepția situațiilor de urgență) și o decizie a statelor membre de a autoriza sau nu la nivel național utilizarea specifică a instrumentelor de IA în astfel de situații.
32. Articolul 5 este o dispoziție detaliată care reglementează o utilizare specifică a instrumentelor de IA care nu numai că vizează completarea cadrului legislativ existent al Uniunii (Directiva privind prelucrarea datelor cu caracter personal în domeniul asigurării respectării legii, ea însăși bazată pe articolul 16 din TFUE), dar necesită și un cadru național de punere în aplicare.

33. În esență, în pofida formulării sale ca interdicție, norma specifică de la articolul 5 poate fi descrisă ca stabilind un cadru strict și excepțional al monitorizării generalizate, „în timp real”, de către instrumentele de IA a persoanelor în spații deschise, în scopul identificării lor. Interdicția depășește, de asemenea, simpla utilizare a camerelor pentru înregistrare și se referă la utilizarea instrumentelor de IA pentru recunoașterea automată a trăsăturilor umane în spațiile accesibile publicului (trăsături cum ar fi fețele, dar și mersul, amprente digitale, ADN-ul, vocea, apăsarea de taste și alte semnale biometrice sau comportamentale). Ea implică, de asemenea, obținerea de imagini și identificarea concomitentă a persoanelor prin analizarea comparativă/verificarea datelor. În plus, norma trebuie evaluată și în lumina faptului că poate fi permisă și identificarea „în timp real” de către utilizatorii privați în spațiile publice (pentru evenimente precum meciurile de fotbal).
34. Clarificările suplimentare oferite de Comisie par să indice că, în prezent, niciun stat membru nu a reglementat această chestiune specifică (sau poate un număr foarte mic de state membre au făcut acest lucru), cu scopul de a permite autorităților de aplicare a legii să utilizeze instrumente de IA pentru detectarea „în timp real” a persoanelor în spațiile publice. Cu toate acestea, în practică, deși nu au fost prezentate dovezi concrete pentru a demonstra că practicile și instrumentele existente vor trebui să se schimbe, pare clar că viitoarele tehnici de investigare, metode criminalistice și norme privind colectarea probelor vor trebui să integreze această abordare bazată pe interdicții/excepții.
35. În ceea ce privește temeiul juridic, reiese că dispozițiile care impun restricții în ceea ce privește prelucrarea datelor biometrice cu caracter personal într-un mod complementar (în comparație cu Directiva privind prelucrarea datelor cu caracter personal în domeniul asigurării respectării legii) urmăresc obiectivul protejării datelor cu caracter personal prin stabilirea unor garanții adecvate. Un astfel de obiectiv este indisolubil legat de obiectivul dispozițiilor care intră în domeniul de aplicare al articolului 114 din TFUE, fără ca unul să fie secundar și indirect în raport cu celălalt. Propunerea de regulament vizează stabilirea unui cadru general privind sistemele de IA, urmând o abordare bazată pe riscuri. În acest context, reglementarea orizontală a sistemelor de IA poate include garanții stricte aplicabile acestui sistem de IA specific de detectare „în timp real”. Un astfel de sistem de IA specific care conține garanții adecvate de protecție a datelor cu caracter personal este, prin urmare, indisolubil legat de obiectivul general de îmbunătățire a funcționării pieței interne și nu este secundar sau indirect în raport cu acesta din urmă. Prin urmare, propunerea de regulament ar trebui să se întemeieze pe un temei dublu, în conformitate cu jurisprudența relevantă (a se vedea punctul 9 de mai sus).

36. Trebuie totuși stabilit care temei juridic ar trebui utilizat pentru reglementarea prelucrării datelor cu caracter personal pentru utilizarea sistemelor menționate la articolul 5 alineatul (1) litera (c) și la articolul 5 alineatele (2)-(4) din propunerea de regulament. Într-adevăr, articolul 87 alineatul (2) litera (a) din TFUE constituie un temei juridic pentru măsurile luate de serviciile de aplicare a legii în legătură cu prevenirea, depistarea și investigarea infracțiunilor, în ceea ce privește colectarea, stocarea, prelucrarea, analizarea și schimbul de informații relevante.
37. Cu toate acestea, astfel cum a explicat avocatul general în concluziile sale referitoare la Avizul privind Acordul PNR cu Canada (Avizul 1/15), articolul 16 din TFUE, pe de o parte, și articolul 87 alineatul (2) litera (a) și articolul 82 alineatul (1) litera (d) din TFUE, pe de altă parte, nu pot avea relații de tip ierarhic „*lex generalis – lex specialis*”¹⁶. Articolul 16 alineatul (2) din TFUE este singura dispoziție care se aplică normelor referitoare la protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal de către autoritățile de aplicare a legii din statele membre atunci când acestea desfășoară activități de prevenire a criminalității. Simplul fapt că articolul 5 face trimitere la lista infracțiunilor grave din Decizia-cadru privind mandatul european de arestare nu modifică această evaluare: respectiva trimitere nu înseamnă că decizia-cadru menționată se aplică ca atare¹⁷. Enumerarea infracțiunilor grave nu este decât o tehnică legislativă care permite să nu fie necesară crearea unei anexe separate.
38. Nu este mai puțin adevărat că norma prevăzută la articolul 5 nu este instituită ca mijloc de delimitare suplimentară a condițiilor de aplicare a respectivelor măsuri legate de JAI, ci pentru a garanta că, în viitor, orice utilizare a identificării biometrice „în timp real” de către sistemele de IA va răspunde în mod adecvat îngrijorărilor legate de drepturile fundamentale și, în primul rând, necesității de a se asigura că datele biometrice sunt colectate și prelucrate cu respectarea dreptului la viață privată și a dreptului la protecția datelor cu caracter personal.

În acest sens, regulamentul nu urmărește să stabilească o nouă procedură obligatorie, specifică JAI, ci se bazează mai degrabă pe mijloace procedurale consacrate și testate pentru a asigura respectarea drepturilor fundamentale.

¹⁶ A se vedea Concluziile AG P. Mengozzi din 8 septembrie 2016, Proiect de acord între Canada și Uniunea Europeană, Avizul 1/15, EU:C:2016:656, punctele 112-120.

¹⁷ Cu privire la punerea în aplicare a acestei liste de infracțiuni grave de către statele membre, a se vedea Hotărârea Curții din 21 iunie 2022, Ligue des droits humains/Conseil des ministres, C-817/19, EU:C:2022:65, punctele 150-152.

39. Dacă articolul 16 din TFUE este un temei juridic suplimentar pertinent, acest lucru ridică semne de întrebare cu privire la aplicarea articolelor 6a și 2a din Protocolul 21 și, respectiv, Protocolul 22. Astfel cum se explică în considerentele 25 și 26 din propunere, acest lucru înseamnă că, atunci când autoritățile de aplicare a legii din Irlanda sau din Danemarca utilizează sisteme de identificare biometrică la distanță „în timp real” în spații accesibile publicului pentru prevenirea criminalității și atât timp cât Irlanda sau Danemarca nu sunt obligate să aplice normele corespunzătoare privind cooperarea polițienească sau cooperarea judiciară în materie penală, aceste două state membre nu vor avea obligații în temeiul articolului 5 alineatul (1) litera (d) și al articolului 5 alineatele (2) și (3) din propunerea de regulament. Aceasta nu înseamnă că articolul 5 alineatul (1) litera (d) și articolul 5 alineatele (2) și (3) conțin norme privind cooperarea polițienească, cum ar fi normele privind schimbul de informații între autoritățile de aplicare a legii. Aceasta înseamnă pur și simplu că articolul 5 alineatul (1) litera (d) și articolul 5 alineatele (2) și (3) din propunerea de regulament, în mod similar Directivei 2016/680 („Directiva privind prelucrarea datelor cu caracter personal în domeniul asigurării respectării legii”), care este *lex generalis* adoptată în temeiul articolului 16 din TFUE, reglementează prelucrarea datelor biometrice cu caracter personal în contextul special al sistemelor de identificare biometrică la distanță „în timp real” în spații accesibile publicului pentru prevenirea criminalității și nimic mai mult. În acest sens, propunerea Comisiei urmează abordarea reținută de legiuitorul Uniunii pentru Directiva privind prelucrarea datelor cu caracter personal în domeniul asigurării respectării legii și, ca atare, confirmă că recurgerea la articolul 87 alineatul (2) din TFUE în acest context nu este, prin urmare, justificată.
40. Adăugarea articolului 16 din TFUE la articolul 114 din TFUE în acest caz este justificată de faptul că articolul 5 alineatul (1) litera (d) și articolul 5 alineatele (2) și (3) sunt singurele dispoziții care reglementează utilizarea unui sistem de IA care a fost autorizat și care interferează cu dreptul la protecția datelor cu caracter personal, care este *lex specialis* față de cadrul general de protecție a datelor. Astfel de norme *lex specialis* privind protecția datelor care afectează utilizarea acestor sisteme de IA sensibile nu pot fi considerate secundare sau indirecte în raport cu temeiul juridic referitor la piața internă. Prin urmare, adăugarea articolului 16 din TFUE ca temei juridic este justificată suficient în propunerea de regulament, iar recurgerea la articolul 87 alineatul (2) litera (a) din TFUE nu este adecvată.

IV. CONCLUZIE

41. Având în vedere cele menționate mai sus, SJC consideră că:

- a) recurgerea la articolele 16 și 114 din TFUE ca temeiuri juridice pentru propunerea de regulament este justificată și adecvată;
 - b) recurgerea la articolul 87 alineatul (2) din TFUE sau la orice alt temei juridic JAI nu este justificată sau adecvată în ceea ce privește normele armonizate aplicabile sistemelor de IA care pot fi furnizate sau utilizate de autoritățile de aplicare a legii sau de autoritățile judiciare.
-