

UNIVERSITATEA ECOLOGICĂ DIN BUCUREȘTI
FACULTATEA DE DREPT
MASTER DREPTUL INTELIGENȚEI ARTIFICIALE

INTELIGENȚA ARTIFICIALĂ ÎN JUSTIȚIE
- suport de curs -

Profesor

Conf. univ. dr. Gabriel Manu

Conf. univ. dr. Petruța-Elena Ispas

2024-2025

Cuprins

Capitolul 1 Considerații introductive privind inteligența artificială și justiția	p. 3
Capitolul 2 Organizarea activității judiciare în România	p. 5
Capitolul 3 Fundamentele justiției digitale. Elemente de etică și problematica drepturilor fundamentale	p. 15
Capitolul 4 Open data în activitatea judiciară	p. 22
Capitolul 5 Inteligența artificială. Principiile administrării justiției și IA. Reglementarea instrumentelor de IA în justiție. Controlul utilizării IA în justiție. Regulamentul privind IA	p. 26
Capitolul 6 Răspunderea pentru prejudiciile cauzate de inteligența artificială. Riscuri ale utilizării IA în activitatea judiciară	p. 56
Capitolul 7 Sancțiuni pentru nerespectarea prevederilor regulamentului	p. 62
Capitolul 8 Utilizarea IA în sistemul de justiție. Perspective privind IA și justiția. Justiția asistată de IA. IA în proceduri judiciare	p. 65
Bibliografie	p. 75

Capitolul 1

Considerații introductive privind inteligența artificială și justiția

În ultima perioadă, dezvoltarea tehnologică a avansat foarte mult, generând provocări în toate domeniile de activitate în care noile tehnologii pot fi utilizate.

Deși justiția reprezintă un pilon important al oricărei societăți democratice, implementarea inteligenței artificiale (în continuare IA) în acest domeniu extrem de vast poate da naștere unor reale provocări, fiind ridicate probleme de etică, protecție a datelor cu caracter personal și protecție a drepturilor fundamentale ale omului.

În vederea unei implementări unitare a principiilor aplicabile digitalizării și IA, la nivel european au fost adoptate o serie de acte normative care trasează liniile generale în domeniul IA și deschide o nouă viziune asupra posibilităților concrete de implementare inclusiv în justiție.

Aceste sisteme reprezintă în fapt capacitatea unei mașini de a imita funcții umane, cum ar fi raționamentul, învățarea, planificarea și creativitatea.

Sistemele de IA permit sistemelor tehnice să perceapă mediul în care funcționează, să prelucreze această percepție și să rezolve probleme, acționând pentru a atinge un anumit obiectiv. Calculatorul primește datele, le prelucrează și reacționează. Sistemele de IA sunt capabile să își adapteze, într-o anumită măsură, comportamentul, analizând efectele acțiunilor anterioare și funcționând autonom.

Astfel cum s-a reținut în preambulul Regulamentului UE 2024/1689 privind inteligența artificială, sistemele de IA pot fi implementate cu ușurință într-o mare varietate de sectoare ale economiei și în multe părți ale societății, inclusiv la nivel transfrontalier, și pot circula cu ușurință în întreaga Uniune. Anumite state membre au explorat deja adoptarea unor norme naționale pentru a se asigura că IA este sigură și de încredere și că este dezvoltată și utilizată în conformitate cu obligațiile în materie de drepturi fundamentale. Divergențele dintre normele naționale pot duce la fragmentarea pieței interne și pot reduce gradul de securitate juridică pentru operatorii care dezvoltă, importă sau utilizează sisteme de IA.

După cum vom analiza pe parcursul prezentei lucrări, actul normativ european reglementează și stabilește reguli aplicabile diferitelor sisteme de IA și modalitatea concretă în care protecția individuală va fi asigurată deoarece IA poate genera riscuri și poate aduce prejudicii intereselor publice și drepturilor fundamentale care sunt protejate de dreptul Uniunii Europene (în continuare UE). Un astfel de prejudiciu ar putea fi material sau moral, inclusiv de natură fizică, psihologică, societală sau economică. Ținând seama de impactul major pe care IA îl poate avea asupra societății și având în vedere și necesitatea de a genera încredere, este esențial ca IA și cadrul său de reglementare să fie dezvoltate în concordanță cu valorile Uniunii consacrate la articolul 2 din Tratatul privind Uniunea Europeană (în continuare TUE) și cu drepturile și libertățile fundamentale consacrate în tratate și, potrivit articolului 6 din TUE, în cartă. Ca o condiție prealabilă, IA ar trebui să fie o tehnologie centrată pe factorul uman. Aceasta ar trebui să le servească oamenilor ca un instrument, cu scopul final de a le spori bunăstarea.

În analiza incidenței sistemelor de IA în justiție, trebuie analizat cu mare atenție raportul beneficiu-risc, în vederea stabilirii unui echilibru al aplicării noilor tehnologii în actul de justiție *lato sensu*.

Nu este de neglijat nici problematica răspunderii civile pentru prejudiciile cauzate de sistemele de IA. O reală și veritabilă a acestor sisteme trebuie să fie însoțită de reguli de utilizare, de limitare a erorii care poate fi incidentă în programarea sistemului de IA. Pe parcursul prezentei lucrări vom încerca să facem o analiză a formelor de răspundere care pot interveni în situația producerii unui prejudiciu ca urmare a implementării unui sistem de IA.

Capitolul 2

Organizarea activității judiciare în România

2.1. Aspecte introductive

Constituția României prevede, în art. 1 alin. (4) faptul că Statul se organizează potrivit principiului separației și echilibrului puterilor - legislativă, executivă și judecătorească - în cadrul democrației constituționale. Ca o consecință a principiului separației puterilor, autoritatea judecătorească trebuie să își păstreze independența și imparțialitatea, fără a se putea accepta o influență a legislativului sau executivului în autoritatea judecătorească.

Astfel cum s-a reținut în Avizul nr. 18 (2015) al Consiliului Consultativ al Judecătorilor Europeni, puterea judecătorească trebuie să fie independentă pentru a-și îndeplini rolul cu privire la celelalte puteri ale statului, societatea în general și părțile din litigii. Independența judecătorilor nu este o prerogativă sau un privilegiu acordat în interesul lor propriu, ci în interesul statului de drept și al tuturor celor care caută și doresc justiție. Independența judiciară este mijlocul prin care se asigură imparțialitatea judecătorilor. Ea este așadar condiția preliminară care garantează că toți cetățenii (și celelalte puteri ale statului) sunt egali în fața instanțelor judiciare. Independența judiciară este un element intrinsec al datoriei de a decide sentințele în mod imparțial. Numai o putere judecătorească independentă poate pune efectiv în aplicare drepturile tuturor membrilor societății, în special ale acelor grupuri care sunt vulnerabile sau nepopulare. Astfel, independența este o cerință fundamentală care permite judecătorilor să apere democrația și drepturile omului.

Potrivit aceluiași Aviz, principiul separării puterilor în stat este în sine o garanție a independenței judiciare. Dar, deși importanța independenței judiciare este exprimată atât de frecvent, trebuie precizat faptul că nimeni – inclusiv puterea judecătorească – nu poate fi complet independent de orice influență, în special de influențele sociale și culturale din interiorul societății în care acționează. La urma urmei: “Nimeni nu este o insulă de sine stătătoare”. Nicio putere judecătorească – la fel ca orice putere dintr-un stat democratic – nu este complet independentă. Puterea judecătorească se sprijină pe celelalte pentru a oferi resurse și servicii, în special pe legislativ, care îi asigură finanțarea și cadrul legal pe care trebuie să-l interpreteze și să-l pună în aplicare. Deși sarcina de a soluționa cazurile în conformitate cu legea este încredințată puterii judecătorești, publicul apelează la puterea executivă pentru punerea în aplicare a deciziilor judecătorești. Deficiențele de executare a deciziilor judecătorești subminează autoritatea judiciară și pun sub semnul întrebării separarea puterilor. Deși toate cele trei puteri au responsabilitate comună în a asigura corecta separație dintre ele, nici acest principiu, nici acela al independenței judiciare nu trebuie să împiedice dialogul dintre puterile statului. Mai curând, este o nevoie fundamentală de discurs respectuos între toate acestea, care să țină seama atât de separarea necesară, cât și de interdependența necesară între puteri. Rămâne vitală însă condiția ca puterea judecătorească să fie liberă de conexiuni nepotrivite și de influență necuvenită din partea celorlalte puteri ale statului.

Potrivit art. 126 din Constituția României, justiția se realizează prin Înalta Curte de Casație și Justiție și prin celelalte instanțe judecătorești stabilite de lege. Legea care reglementează organizarea judiciară este reprezentată de Legea nr. 304/2022, publicată în Monitorul Oficial al României nr. 1104/16.11.2022. Potrivit Legii nr. 304/2002, organizarea judiciară reprezintă un

ansamblu de principii și reguli care guvernează funcționarea instanțelor judecătorești și parchetelor în activitatea judiciară, în scopul garantării respectării Constituției României, republicată, și realizării drepturilor și libertăților fundamentale ale persoanei prin înfăptuirea justiției ca serviciu public. Dispozițiile legii reiau prevederile art. 126 din Constituție, tocmai pentru a se întări principiul constituțional al legalității instanțelor de judecată, astfel încât conform Legii nr. 304/2022, justiția se realizează prin Înalta Curte de Casație și Justiție și prin celelalte instanțe judecătorești stabilite de lege.

Garantul independenței justiției este Consiliul Superior al Magistraturii care, potrivit dispozițiilor Legii nr. 304/2022 contribuie la buna organizare și administrare a justiției, prin atribuțiile și competențele sale stabilite prin lege.

Interesele generale ale societății sunt reprezentate de Ministerul Public, acesta având competența de a apăra ordinea de drept, precum și drepturile și libertățile cetățenilor, exercitându-și atribuțiile prin procurori constituiți în parchete, în condițiile legii.

Conform art. 2 din Legea nr. 304/2022, justiția se înfăptuiește de către judecători în numele legii, fiind unică, imparțială și egală pentru toți. Instanțele judecătorești care contribuie la înfăptuirea justiției sunt: Înalta Curte de Casație și Justiție, curțile de apel, tribunalele, tribunalele specializare, instanțele militare și judecătoriile. Pe lângă instanțele de judecată funcționează parchetele care conduc și supraveghează activitatea de cercetare penală.

Dincolo de aspectele referitoare la organizarea judiciară în România, pe care le vom analiza succint, se impune a menționa faptul că utilizarea sistemelor de IA în activități specific activității judiciare și conexe nu mai este un subiect îndepărtat de realitate.

Este adevărat că utilizarea sistemelor de IA în justiție nu poate fi una aleatorie, ci este necesar un control exercitat asupra algoritmilor folosiți în implementarea acestor sisteme complexe care sunt de natură a înlocui persoanele, având un raționament propriu bazat pe o programare anterioară.

Luând în considerare riscurile utilizării necorespunzătoare a uneltelor bazate pe IA și pe alte tipuri de algoritmi avansați, Comitetul de Justiție și Afaceri Interne al Marii Britanii a publicat pe 30 martie 2022 un raport numit “*Technology rules? The advent of new technologies in the justice system*”¹. Printre măsurile propuse în cadrul acestui raport se numără: (a) crearea unui registru obligatoriu de algoritmi utilizați de poliție și organele judiciare, (b) reglementarea acestui domeniu prin legislație primară și secundară, (c) introducerea obligativității efectuării unor training-uri prealabile pentru utilizatorii acestor tehnologii din sistemul judiciar, (d) constituirea la nivel național a unui organism central de autorizare și supraveghere, precum și organizarea unor comitete de etică în cadrul inspectoratelor de poliție.

Preocupări în acest sens există și la nivelul Consiliului Europei și al Uniunii Europene. În decembrie 2018, Comisia Europeană pentru Eficiență în Justiție (CEPEJ) din cadrul Consiliului Europei a adoptat “*Carta Etică Europeană în privința utilizării inteligenței artificiale în sistemele judiciare și domeniile adiacente*”. Totodată, Comisia Europeană a propus noi reguli și acțiuni pentru a transforma Uniunea Europeană într-un hub global pentru tehnologii de IA sigure

¹ <https://publications.parliament.uk/pa/ld5802/ldselect/ldjusthom/180/180.pdf>

și fiabile, prin “Pachetul AI”². Preocuparea UE este una constantă în privința implementării sistemelor de IA, însă implementarea acestora este dependentă de siguranța în exploatarea acestor sisteme, de respectarea principiilor și normelor de drept, în vederea garantării tuturor persoanelor respectarea drepturilor fundamentale.

2.2 Organizarea judiciară

Prin raportare la prevederile Legii nr. 304/2022, se impune a prezenta sistemul organizării judiciare în România, prin prezentarea activității și competenței instanțelor de judecată și a parchetelor, dar și prin prezentarea activității și competențelor Consiliului Superior al Magistraturii care, conform dispozițiilor legale, este garantul independenței justiției.

Astfel cum arătam și anterior, în conformitate cu dispozițiile art. 2 din Legea nr. 304/2022, justiția se realizează prin următoarele instanțe judecătorești: a) Înalta Curte de Casație și Justiție; b) curți de apel; c) tribunale; d) tribunale specializate; e) instanțe militare; f) judecătorii.

2.2.1. Înalta Curte de Casație și Justiție

Înalta Curte de Casație și Justiție este instanța supremă din România, cu sediul în București. Instanța supremă asigură interpretarea și aplicarea unitară a legii de către celelalte instanțe judecătorești, potrivit competenței sale, în conformitate cu dispozițiile art. 20 din Legea nr. 304/2022.

Componența Înaltei Curți este reglementată de dispozițiile art. 21 din Legea nr. 304/2022, după cum urmează: (1) Înalta Curte de Casație și Justiție se compune din: președinte, 2 vicepreședinți, 4 președinți de secții și judecători. (2) Înalta Curte de Casație și Justiție este organizată în 4 secții - Secția I civilă, Secția a II-a civilă, Secția penală, Secția de contencios administrativ și fiscal și Secțiile Unite, cu competență proprie. (3) În cadrul Înaltei Curți de Casație și Justiție funcționează Completul pentru soluționarea recursului în interesul legii, Completul pentru dezlegarea unor chestiuni de drept, precum și completurile de 5 judecători.

În privința competenței secțiilor Înaltei Curți de Casație și Justiție, prevederile art. 23 și 24 din Legea nr. 304/2022 stabilesc domeniile în care secțiile Înaltei Curți judecă, respectiv:

”Secția I civilă, Secția a II-a civilă și Secția de contencios administrativ și fiscal ale Înaltei Curți de Casație și Justiție judecă recursurile împotriva hotărârilor pronunțate de curțile de apel și a altor hotărâri, în cazurile prevăzute de lege, precum și recursurile declarate împotriva hotărârilor nedefinitive sau a actelor judecătorești, de orice natură, care nu pot fi atacate pe nicio altă cale, iar cursul judecății a fost întrerupt în fața curților de apel. (2) Hotărârea de respingere a cererii de sesizare a Curții Constituționale cu soluționarea excepției de neconstituționalitate, pronunțată de ultima instanță, este supusă căii de atac a recursului. (3) Secția I civilă, Secția a II-a civilă și Secția de contencios administrativ și fiscal ale Înaltei Curți de Casație și Justiție judecă printr-un complet diferit al acestora recursul formulat împotriva hotărârilor pronunțate de aceste secții, prin care a fost respinsă cererea de sesizare a Curții Constituționale cu soluționarea excepției de neconstituționalitate”. Potrivit art. 24 alin. (1) din Legea nr. 304/2022, Secția penală a Înaltei Curți de Casație și Justiție judecă: a) în primă instanță, procesele și cererile date prin lege în competența de primă instanță a Înaltei Curți de

² <https://digital-strategy.ec.europa.eu/en/policies/european-approach-artificial-intelligence>

Casație și Justiție; b) apelurile împotriva hotărârilor penale pronunțate în primă instanță de curțile de apel și de Curtea Militară de Apel; c) contestațiile împotriva hotărârilor penale pronunțate în primă instanță de curțile de apel, de Curtea Militară de Apel și de Secția penală a Înaltei Curți de Casație și Justiție; d) apelurile declarate împotriva hotărârilor nedefinitive sau a actelor judecătorești, de orice natură, care nu pot fi atacate pe nicio altă cale, iar cursul judecății a fost întrerupt în fața curților de apel; e) recursurile în casație împotriva hotărârilor definitive, în condițiile prevăzute de lege; f) recursurile împotriva hotărârilor de respingere a cererii de sesizare a Curții Constituționale cu soluționarea excepției de neconstituționalitate pronunțate de curțile de apel; g) sesizările în vederea pronunțării unei hotărâri prealabile pentru dezlegarea unei probleme de drept. Totodată, potrivit art. 24 alin. (2) din Legea nr. 304/2022, ”Secția penală a Înaltei Curți de Casație și Justiție, când judecă în ultimă instanță, judecă printr-un complet diferit al acesteia recursul formulat împotriva hotărârilor pronunțate de această secție prin care a fost respinsă cererea de sesizare a Curții Constituționale cu soluționarea excepției de neconstituționalitate”.

Tot cu privire la competența de judecată a Înalte Curți, trebuie menționate și cererile de strămutare exercitate în conformitate cu dispozițiile Codurilor de procedură, conflictele de competență dar și orice alte cereri date de lege în competența instanței supreme.

Potrivit art. 27 din Legea nr. 304/2022, Înalta Curte de Casație și Justiție se constituie în Secții Unite pentru: a) soluționarea, în condițiile prezentei legi, a sesizărilor privind schimbarea jurisprudenței Înaltei Curți de Casație și Justiție; b) sesizarea Curții Constituționale pentru controlul constituționalității legilor înainte de promulgare.

2.2.2. Curțile de apel

În conformitate cu dispozițiile art. 39 din Legea nr. 304/2022, ”(1) Curțile de apel sunt instanțe cu personalitate juridică, în circumscripția cărora funcționează mai multe tribunale și tribunale specializate, potrivit anexei nr. 1. (2) În cadrul curților de apel funcționează, în raport cu complexitatea și numărul cauzelor, secții sau, după caz, completuri specializate pentru cauze civile, cauze penale, cauze cu minori și de familie, cauze de contencios administrativ și fiscal, cauze privind conflicte de muncă și asigurări sociale, cauze civile izvorând din exploatarea unei întreprinderi, insolvență, concurență neloială sau pentru alte materii, precum și completuri specializate pentru cauze maritime și fluviale.

În privința competenței de judecată dată de Codul de procedură civilă în sarcina curților de apel, prevederile art. 96 stabilesc următoarele domenii de competență: ”Curțile de apel judecă: 1. în primă instanță, cererile în materie de contencios administrativ și fiscal, potrivit legii speciale; 2. ca instanțe de apel, apelurile declarate împotriva hotărârilor pronunțate de tribunale în primă instanță; 3. ca instanțe de recurs, recursurile declarate împotriva hotărârilor pronunțate de tribunale în apel sau împotriva hotărârilor pronunțate în primă instanță de tribunale, care, potrivit legii, nu sunt supuse apelului, precum și în orice alte cazuri expres prevăzute de lege; 4. orice alte cereri date prin lege în competența lor”.

Competența curților de apel în materie penală este reglementată de art. 38 Cod procedură penală care stabilește următoarea competență de judecată în sarcina curților de apel: ”(1) Curtea de apel judecă în primă instanță: a) infracțiunile prevăzute de Codul penal la art. 394-397, 399-412 și 438-445; b) infracțiunile privind securitatea națională a României, prevăzute în legi speciale; c)

infracțiunile săvârșite de judecătorii de la judecătorii, tribunale și de procurorii de la parchetele care funcționează pe lângă aceste instanțe³; d) infracțiunile săvârșite de avocați, notari publici, executori judecătorești, de controlorii financiari ai Curții de Conturi, precum și auditori publici externi; e) infracțiunile săvârșite de șefii cultelor religioase organizate în condițiile legii și de ceilalți membri ai înaltului cler, care au cel puțin rangul de arhiereu sau echivalent al acestuia; f) infracțiunile săvârșite de magistrații-asistenți de la Înalta Curte de Casație și Justiție; g) infracțiunile săvârșite de membrii Curții de Conturi, de președintele Consiliului Legislativ, de Avocatul Poporului, de adjuncții Avocatului Poporului și de chestori; h) cererile de strămutare, în cazurile prevăzute de lege. (2) Curtea de apel judecă apelurile împotriva hotărârilor penale pronunțate în primă instanță de judecătorii și de tribunale. (3) Curtea de apel soluționează conflictele de competență ivite între instanțele din circumscripția sa, altele decât cele prevăzute la art. 36 alin. (2), precum și contestațiile formulate împotriva hotărârilor pronunțate de tribunale în cazurile prevăzute de lege; (4) Curtea de apel soluționează și alte cauze anume prevăzute de lege”.

În privința Curților militare de apel, prevederile art. 39 Cod procedură penală stabilesc în competența acestor instanțe următoarele litigii: ”(1) Curtea militară de apel judecă în primă instanță: a) infracțiunile prevăzute de [Codul penal](#) la art. 394-397, 399-412 și 438-445, săvârșite de militari; b) infracțiunile privind securitatea națională a României, prevăzute în legi speciale, săvârșite de militari; c) infracțiunile săvârșite de judecătorii tribunalelor militare și de procurorii militari de la parchetele militare care funcționează pe lângă aceste instanțe; d) infracțiunile săvârșite de generali, mareșali și amirali; e) cererile de strămutare, în cazurile prevăzute de lege. (2) Curtea militară de apel judecă apelurile împotriva hotărârilor penale pronunțate de tribunalele militare. (3) Curtea militară de apel soluționează conflictele de competență ivite între tribunalele militare din circumscripția sa, precum și contestațiile formulate împotriva hotărârilor pronunțate de acestea în cazurile prevăzute de lege. (4) Curtea militară de apel soluționează și alte cauze anume prevăzute de lege.

2.2.3. Tribunalele

În privința tribunalelor, legea privind organizarea judiciară prevede în art. 40 faptul că aceste instanțe se organizează la nivelul fiecărui județ și al municipiului București și că în circumscripția fiecărui tribunal sunt cuprinse toate judecătoriile din județ sau, după caz, din municipiul București. Totodată, potrivit art. 40 alin. (3) din Legea nr. 304/2022, în cadrul tribunalelor funcționează, în raport cu complexitatea și numărul cauzelor, secții sau, după caz, completuri specializate pentru cauze civile, cauze penale, cauze cu minori și de familie, cauze de contencios administrativ și fiscal, cauze privind conflicte de muncă și asigurări sociale, cauze civile izvorând din exploatarea unei întreprinderi, insolvență, concurență neloială sau pentru alte materii, precum și completuri specializate pentru cauze maritime și fluviale.

³ Prin Decizia nr. [23/2022](#) Înalta Curte de Casație și Justiție admite recursul în interesul legii și stabilește că, în interpretarea și aplicarea unitară a dispozițiilor art. 38 alin. (1) lit. c) și art. 40 alin. (1) din Codul de procedură penală, competența instanței de judecată în soluționarea cauzelor penale având ca obiect infracțiuni săvârșite de judecători și procurori care au dobândit un grad profesional superior celui al instanței/parchetului în care își desfășoară efectiv activitatea se determină prin raportare la instanța/parchetul la care își desfășoară efectiv activitatea magistratul cercetat, și nu la gradul profesional superior al acestuia.

Codul de procedură civilă stabilește în art. 95 ca și competență a tribunalelor următoarele litigii: Tribunalele judecă: 1. în primă instanță, toate cererile care nu sunt date prin lege în competența altor instanțe⁴; 2. ca instanțe de apel, apelurile declarate împotriva hotărârilor pronunțate de judecătorii în primă instanță; 3. ca instanțe de recurs, recursurile declarate împotriva hotărârilor pronunțate de judecătorii, care, potrivit legii, nu sunt supuse apelului și în orice alte cazuri expres prevăzute de lege; 4. orice alte cereri date prin lege în competența lor⁵.

În privința Codului de procedură penală, competența tribunalului și a tribunalului militar este stabilită în art. 36 și 37. În privința tribunalelor, art. 36 Cod procedură penală stabilește ca și litigii care se judecă de aceste instanțe următoarele ”(1) Tribunalul judecă în primă instanță: a) infracțiunile prevăzute de [Codul penal](#) la art. 188-191, art. 209-211, art. 254, 256¹, 263, 282, art. 289-294, art. 303, 304, 306, 307, 309, 345, 346, 354 și art. 360-367; b) infracțiunile săvârșite cu intenție depășită care au avut ca urmare moartea unei persoane; c) infracțiunile cu privire la care urmărirea penală a fost efectuată de către Direcția de Investigare a Infracțiunilor de Criminalitate Organizată și Terorism sau Direcția Națională Anticorupție, dacă nu sunt date prin lege în competența altor instanțe ierarhic superioare; c¹) infracțiunile de spălare a banilor și infracțiunile de evaziune fiscală prevăzute de art. 9 din Legea nr. [241/2005](#) pentru prevenirea și combaterea evaziunii fiscale, cu modificările ulterioare; c²) infracțiunile cu privire la care urmărirea penală a fost efectuată de către Parchetul European, potrivit Regulamentului (UE) [2017/1.939](#) al Consiliului din 12 octombrie 2017 de punere în aplicare a unei forme de cooperare consolidată în ceea ce privește instituirea Parchetului European (EPPO); d) alte infracțiuni date prin lege în competența sa. (2) Tribunalul soluționează conflictele de competență ivite între judecătoriile din circumscripția sa, precum și contestațiile formulate împotriva hotărârilor pronunțate de judecătore în cazurile prevăzute de lege. (3) Tribunalul soluționează și alte cauze anume prevăzute de lege. În privința tribunalului militar, art. 37 Cod procedură penală stabilește următoarele: (1) Tribunalul militar judecă în primă instanță toate infracțiunile comise de militari până la gradul de colonel inclusiv, cu excepția celor date prin lege în competența altor instanțe. (2) Tribunalul militar soluționează și alte cauze anume prevăzute de lege.

2.2.4. Judecătoriile

⁴ *) Prin Decizia nr. [5/2022](#), Înalta Curte de Casație și Justiție admite recursul în interesul legii și stabilește că, în interpretarea și aplicarea unitară a prevederilor art. 95 pct. 1, competența materială de soluționare a cauzelor având ca obiect obligarea pe temei delictual a pârâților la achitarea daunelor materiale și/sau morale pentru malpraxis, în situația în care nu a fost urmată procedura reglementată de dispozițiile art. 679-685 din Legea nr. 95/2006, aparține judecătoriei.

*) Prin Decizia nr. [1/2023](#) Înalta Curte de Casație și Justiție admite recursul în interesul legii și stabilește că, în interpretarea și aplicarea unitară a dispozițiilor art. 94 pct. 1 lit. h) și k) și art. 95 pct. 1 din Codul de procedură civilă, tribunalul este instanța competentă material în ce privește soluționarea cauzelor având ca obiect cereri de constatare a caracterului ilicit al faptei care aduce atingere unor drepturi nepatrimoniale, cereri întemeiate pe prevederile art. 253 alin. (1) lit. c) din [Codul civil](#), atunci când acestea sunt formulate simultan cu cereri întemeiate pe dispozițiile art. 253 alin. (4) din [Codul civil](#) de a se acorda despăgubiri pentru prejudiciul nepatrimonial cauzat care nu depășesc valoarea de 200.000 lei inclusiv.

⁵ *) În interpretarea și aplicarea unitară a prevederilor art. 95, secțiile civile ale tribunalelor sunt competente funcțional să soluționeze apelurile declarate împotriva hotărârilor pronunțate de judecătorii asupra contestațiilor formulate împotriva executărilor silite pornite în temeiul dispozițiilor art. 260 din Legea nr. [207/2015](#) privind [Codul de procedură fiscală](#), cu modificările și completările ulterioare.

În privința judecătoriilor, Legea nr. 304/2022 stabilește în art. 42 că judecătoriile sunt organizate în județe și în sectoarele municipiului București și că acele localități care fac parte din circumscripțiile judecătoriilor din fiecare județ se stabilesc prin Hotărâre a Guvernului, la propunerea ministrului justiției, cu avizul Consiliului Superior al Magistraturii.

Potrivit art. 43 din Legea nr. 304/2022, în raport cu natura și numărul cauzelor, în cadrul judecătoriilor se pot înființa secții sau completuri specializate și că în cadrul judecătoriilor se vor organiza secții sau completuri specializate pentru minori și familie.

În privința competenței judecătoriilor, și cu privire la aceste instanțe regăsim reglementare atât în dispozițiile Codului de procedură civilă, cât și în dispozițiile Codului de procedură penală.

Astfel, conform art. 94 Cod procedură civilă, judecătoriile judecă următoarele cauze: 1. în primă instanță, următoarele cereri al căror obiect este evaluabil sau, după caz, neevaluabil în bani: a) cererile date de Codul civil în competența instanței de tutelă și de familie, în afară de cazurile în care prin lege se prevede în mod expres altfel; b) cererile referitoare la înregistrările în registrele de stare civilă, date de lege în competența instanțelor judecătorești⁶; c) cererile având ca obiect administrarea clădirilor cu mai multe etaje, apartamente sau spații aflate în proprietatea exclusivă a unor persoane diferite, precum și cele privind raporturile juridice stabilite de asociațiile de proprietari cu alte persoane fizice sau persoane juridice, după caz; d) cererile de evacuare; e) cererile referitoare la zidurile și șanțurile comune, distanța construcțiilor și plantațiilor, dreptul de trecere, precum și la orice servituți sau alte limitări ale dreptului de proprietate prevăzute de lege, stabilite de părți ori instituite pe cale judecătorească; f) cererile privitoare la strămutarea de hotare și cererile în grănițuire; g) cererile posesorii; h) cererile privind obligațiile de a face sau de a nu face neevaluabile în bani, indiferent de izvorul lor contractual sau extracontractual, cu excepția celor date de lege în competența altor instanțe⁷; i) cererile de declarare judecătorească a morții unei persoane; j) cererile de împărțeață judiciară, indiferent de valoare; j¹) cererile în materie de moștenire, indiferent de valoare; j²) cererile privind uzucapiunea, indiferent de valoare; j³) cererile în materia fondului funciar, cu excepția celor date prin lege specială în competența altor instanțe; k) orice alte cereri evaluabile în bani în valoare de până la 200.000 lei inclusiv, indiferent de calitatea părților, profesioniști sau neprofesioniști⁸; 2. căile de atac

⁶ *) Prin Decizia nr. 28/2021, Înalta Curte de Casație și Justiție admite recursul în interesul legii și stabilește că, în interpretarea și aplicarea unitară a dispozițiilor art. 94 pct. 1 lit. b) din Legea nr. 134/2010 privind Codul de procedură civilă, republicată, cu modificările și completările ulterioare (atât în redactarea anterioară Legii nr. 310/2018, cât și în redactarea ulterioară acestei legi), revine judecătoriilor competența materială procesuală de soluționare în primă instanță a cererilor în anulare/contestațiilor formulate împotriva dispozițiilor emise de primari în soluționarea cererilor de rectificare a actelor de stare civilă.

⁷ *) Prin Decizia nr. 1/2023 Înalta Curte de Casație și Justiție admite recursul în interesul legii și stabilește că, în interpretarea și aplicarea unitară a dispozițiilor art. 94 pct. 1 lit. h) și k) și art. 95 pct. 1 din Codul de procedură civilă, tribunalul este instanța competentă material în ce privește soluționarea cauzelor având ca obiect cereri de constatare a caracterului ilicit al faptei care aduce atingere unor drepturi nepatrimoniale, cereri întemeiate pe prevederile art. 253 alin. (1) lit. c) din Codul civil, atunci când acestea sunt formulate simultan cu cereri întemeiate pe dispozițiile art. 253 alin. (4) din Codul civil de a se acorda despăgubiri pentru prejudiciul nepatrimonial cauzat care nu depășesc valoarea de 200.000 lei inclusiv.

⁸ *) Prin Decizia nr. 5/2022, Înalta Curte de Casație și Justiție admite recursul în interesul legii și stabilește că, în interpretarea și aplicarea unitară a prevederilor 94 pct. 1 lit. k), competența materială de soluționare a cauzelor având ca obiect obligarea pe temei delictual a părților la achitarea daunelor materiale și/sau morale pentru malpraxis, în situația în care nu a fost urmată procedura reglementată de dispozițiile art. 679-685 din

împotriva hotărârilor autorităților administrației publice cu activitate jurisdicțională și ale altor organe cu astfel de activitate, în cazurile prevăzute de lege; 3. orice alte cereri date prin lege în competența lor.

În ceea ce privește competența judecătorei în materie penală, prevederile art. 35 Cod procedură penală prevăd că judecătoria judecă în primă instanță cu excepția celor date prin lege în competența altor instanțe și faptul că judecătoria soluționează și alte cauze anume prevăzute de lege.

2.2.5. Ministerul Public

În conformitate cu dispozițiile art. 66 din Legea nr. 304/2022, Ministerul Public își exercită atribuțiile în temeiul legii și este condus de procurorul general al Parchetului de pe lângă Înalta Curte de Casație și Justiție. Activitatea procurorilor se desfășoară în conformitate cu principiile legalității, imparțialității și controlului ierarhic, sub autoritatea ministrului justiției, în condițiile legii.

Dispozițiile legale incidente reglementează în mod expres prezumția de nevinovăție care trebuie să fie respectată de parchete în comunicarea publică. Totodată, art. 66 alin. (3) din Legea nr. 304/2022 reglementează obligația procurorilor de a respecta și apăra drepturile și libertățile fundamentale ale persoanelor, de a respecta prezumția de nevinovăție, dreptul la un proces echitabil, principiul egalității de arme, independența instanțelor și forța executorie a hotărârilor judecătorești.

Atribuțiile exercitate de Ministerul Public prin procurori sunt reglementate de art. 67 din Legea nr. 304/2022, după cum urmează: a) efectuează urmărirea penală în cazurile și în condițiile prevăzute de lege și participă, potrivit legii, la soluționarea conflictelor prin mijloace alternative; b) conduce și supraveghează activitatea de cercetare penală a poliției judiciare, conduce și controlează activitatea altor organe de cercetare penală; c) sesizează instanțele judecătorești pentru judecarea cauzelor penale, potrivit legii; d) exercită acțiunea civilă, în cazurile prevăzute de lege; e) participă, în condițiile legii, la ședințele de judecată; f) exercită căile de atac împotriva hotărârilor judecătorești, în condițiile prevăzute de lege; g) apără drepturile și interesele legitime ale minorilor, ale persoanelor care beneficiază de consiliere judiciară sau tutelă specială, ale dispăruților și ale altor persoane, în condițiile legii; h) acționează pentru prevenirea și combaterea criminalității, sub coordonarea ministrului justiției, pentru realizarea unitară a politicii penale a statului; i) studiază cauzele care generează sau favorizează criminalitatea, elaborează și prezintă ministrului justiției propuneri în vederea eliminării acestora, precum și pentru perfecționarea legislației în domeniu; j) verifică respectarea legii la locurile de deținere

Legea	nr.	95/2006,	aparține	judecătorei.
-------	-----	----------	----------	--------------

*) Prin Decizia nr. 1/2023 Înalta Curte de Casație și Justiție admite recursul în interesul legii și stabilește că, în interpretarea și aplicarea unitară a dispozițiilor art. 94 pct. 1 lit. h) și k) și art. 95 pct. 1 din Codul de procedură civilă, tribunalul este instanța competentă material în ce privește soluționarea cauzelor având ca obiect cereri de constatare a caracterului ilicit al faptei care aduce atingere unor drepturi nepatrimoniale, cereri întemeiate pe prevederile art. 253 alin. (1) lit. c) din Codul civil, atunci când acestea sunt formulate simultan cu cereri întemeiate pe dispozițiile art. 253 alin. (4) din Codul civil de a se acorda despăgubiri pentru prejudiciul nepatrimonial cauzat care nu depășesc valoarea de 200.000 lei inclusiv.

preventivă; k) exercită atribuțiile prevăzute de Legea contenciosului administrativ nr. 554/2004, cu modificările și completările ulterioare; l) exercită orice alte atribuții prevăzute de lege.

Parchetele se organizează pe lângă fiecare instanță de judecată, în conformitate cu prevederile legale. În cadrul Înaltei Curți de Casație și Justiție funcționează Direcția de Investigare a Infracțiunilor de Criminalitate Organizată și Terorism, în conformitate cu art. 85 și urm. din Legea nr. 304/2022. Tot în cadrul Parchetului de pe lângă Înalta Curte de Casație și Justiție funcționează Direcția Națională Anticorupție, în conformitate cu art. 93 și urm. din Legea nr. 304/2022.

În conformitate cu art. 100 și urm. din Legea nr. 304/2022, pe lângă fiecare curte de apel, tribunal, tribunal pentru minori și familie și judecătore funcționează un parchet.

În privința parchetelor militare, acestea funcționează pe lângă fiecare instanță militară, astfel cum prevede art. 109 din Legea nr. 304/2022 privind organizarea judiciară.

2.2.6. Consiliul Superior al Magistraturii

Consiliul Superior al Magistraturii este, potrivit art. 1 din Legea nr. 305/2022, garantul independenței justiției.

Atribuțiile Consiliului Superior al Magistraturii sunt stabilite în art. 36 și urm. din legea specială care reglementează organizarea, funcționarea și atribuțiile acestei instituții.

Plenul Consiliului Superior al Magistraturii exercită atribuții referitoare la cariera judecătorilor și procurorilor, admiterea în magistratură, formarea și examenele judecătorilor și procurorilor, organizarea și funcționarea instanțelor și a parchetelor. Totodată, plenul Consiliului Superior al Magistraturii adoptă Codul deontologic al judecătorilor și procurorilor, regulamentul de organizare și funcționare propriu, regulamentul privind procedura alegerii membrilor proprii, dar și alte regulamente și hotărâri stabilite de lege în competența sa. Totodată, plenul Consiliului Superior are competența de a aviza proiectele de acte normative care privesc activitatea autorității judecătorești, având totodată competența de a aviza proiectele de regulamente și ordine care se aprobă de ministrul justiției, în condițiile legii.

În cadrul Consiliului Superior al Magistraturii, sunt constituite 2 secții, Secția pentru judecători și Secția pentru procurori, acestea îndeplinind atribuțiile expres prevăzute în art. 40 și urm. din Legea nr. 305/2022, după cum urmează: Secția pentru judecători a Consiliului Superior al Magistraturii numește și revocă din funcție președintele, vicepreședinții și președinții de secții ai Înaltei Curți de Casație și Justiție, iar Secția pentru procurori a Consiliului Superior al Magistraturii avizează, în condițiile legii, propunerea ministrului justiției de numire și revocare a procurorului general al Parchetului de pe lângă Înalta Curte de Casație și Justiție, prim-adjunctului și adjunctul acestuia, procurorului-șef al Direcției Naționale Anticorupție și al Direcției de Investigare a Infracțiunilor de Criminalitate Organizată și Terorism, adjunctilor acestora, procurorilor șefi de secție ai Parchetului de pe lângă Înalta Curte de Casație și Justiție, ai Direcției Naționale Anticorupție și Direcției de Investigare a Infracțiunilor de Criminalitate Organizată și Terorism.

Secțiile Consiliului Superior al Magistraturii au atribuții stabilite prin lege și în privința organizării și funcționării instanțelor judecătorești (art. 41 alin. (1) din Legea nr. 305/2022) și în privința organizării și funcționării parchetelor (art. 41 alin. (2) din Legea nr. 305/2022).

Secția pentru judecători are în atribuțiile stabilite de lege încuviințarea percheziției, reținerii, arestării preventive, arestului la domiciliu cu privire la judecători, în timp de secția pentru

procurori are aceleași atribuții în privința procurorilor. Tot în atribuțiile fiecărei secții în parte se numără și încuviințarea măsurii controlului judiciar și a controlului judiciar pe cauțiune dacă urmează să fie dispusă obligația de a nu exercita funcția de judecător sau, după caz, funcția de procuror.

Nu în ultimul rând, trebuie menționate și atribuțiile secțiilor Consiliului Superior al Magistraturii în domeniul răspunderii disciplinare a judecătorilor și procurorilor.

În conformitate cu dispozițiile art. 44 din Legea nr. 305/2022, Consiliul Superior al Magistraturii îndeplinește, prin secțiile sale, rolul de instanță de judecată în domeniul răspunderii disciplinare a judecătorilor și procurorilor, în privința faptelor prevăzute de lege ca reprezentând abateri disciplinare. În cazul abaterilor disciplinare săvârșite de judecători sau procurori, acțiunea disciplinară se exercită de către Inspekția Judiciară, prin inspectorul judiciar. Pentru exercitarea acțiunii disciplinare, este obligatorie efectuarea cercetării disciplinare prealabile de către Inspekția Judiciară.

Capitolul 3

Fundamentele justiției digitale

3.1. Considerații introductive

În ultimii ani, la nivelul Uniunii Europene și la nivelul statelor membre, s-a simțit o preocupare apăsătoare în privința digitalizării activităților din justiție. Pandemia COVID-19 a generat noi provocări în gestionarea activităților desfășurate la nivel national și totodată în domeniul cooperării judiciare în materie civilă, comercială și penală.

În Strategia privind e-justiția europeană 2024-2028⁹ se arată că în perioada 2019-2023, la nivelul Consiliului Uniunii Europene, la nivelul Comisiei Europene și Parlamentului European s-au depus eforturi pentru a se accelera procesul digitalizării și pentru promovarea serviciilor digitale în e-justiție. La nivelul Uniunii Europene au fost adoptate mai multe acte normative dintre care se cuvine să menționăm următoarele: Regulamentul privind un sistem informatizat pentru schimbul electronic transfrontalier de date în domeniul cooperării judiciare în materie civilă și penală (sistemul e-CODEX)¹⁰, care a oferit un cadru adecvat pentru schimbul de informații judiciare prin intermediul unor servicii securizate; Regulamentul privind notificarea sau comunicarea actelor¹¹ și Regulamentul privind obținerea de probe¹² care instituie utilizarea, pentru comunicările relevante, a sistemului informatic descentralizat cu puncte de acces interoperabile bazate pe e-CODEX; Regulamentul privind probele electronice¹³ și, în special, Regulamentul și Directiva privind digitalizarea cooperării judiciare transfrontaliere și a accesului la justiție („pachetul privind digitalizarea”)¹⁴.

⁹ Adoptată la Bruxelles în data de 17 noiembrie 2023 (OR. en) 15509/23, disponibilă la adresa web <https://www.consilium.europa.eu/ro/press/press-releases/2023/12/08/eu-takes-important-step-towards-digitalisation-of-justice-systems/>

¹⁰ Regulamentul (UE) 2022/850 al Parlamentului European și al Consiliului din 30 mai 2022 privind un sistem informatizat pentru schimbul electronic transfrontalier de date în domeniul cooperării judiciare în materie civilă și penală (sistemul e-CODEX) și de modificare a Regulamentului (UE) 2018/1726, JO L 150, 1.6.2022, p. 1-19.

¹¹ Regulamentul (UE) 2020/1784 al Parlamentului European și al Consiliului din 25 noiembrie 2020 privind notificarea sau comunicarea în statele membre a actelor judiciare și extrajudiciare în materie civilă sau comercială (notificarea sau comunicarea actelor) (reformare), JO L 405, 2.12.2020, p. 40-78.

¹² Regulamentul (UE) 2020/1783 al Parlamentului European și al Consiliului din 25 noiembrie 2020 privind cooperarea între instanțele statelor membre în domeniul obținerii de probe în materie civilă sau comercială (obținerea de probe) (reformare), JO L 405, 2.12.2020, p. 1-39.

¹³ Regulamentul (UE) 2023/1543 al Parlamentului European și al Consiliului din 12 iulie 2023 privind ordinele europene de divulgare a probelor electronice și ordinele europene de păstrare a probelor electronice în cadrul procedurilor penale și pentru executarea pedepselor privative de libertate în urma unor proceduri penale, JO L 191, 28.7.2023, p. 118-180.

¹⁴ Directiva (UE) 2023/2843 A PARLAMENTULUI EUROPEAN ȘI A CONSILIULUI din 13 decembrie 2023 de modificare a Directivei 2011/99/UE și 2014/41/UE ale Parlamentului European și ale Consiliului, a Directivei 2003/8/CE a Consiliului și a Deciziilor-cadru 2002/584/JAI, 2003/577/JAI, 2005/214/JAI, 2006/783/JAI, 2008/909/JAI, 2008/947/JAI, 2009/829/JAI și 2009/948/JAI ale Consiliului, în ceea ce privește digitalizarea cooperării judiciare.

Astfel cum rezultă din actele normative adoptate la nivelul Uniunii Europene, preocuparea pentru o eficientă digitalizare a justiției există, în acest sens fiind adoptate actele normative la care am făcut referire anterior și la care ne vom referi și în cele ce urmează.

Mai mult decât atât, se impune a preciza faptul că, spre deosebire de regulamente, care se bucură de aplicabilitate directă în statele membre, directivele trebuie transpuse în legislația națională a fiecărui stat membru¹⁵.

Anterior adoptării acestor acte normative în materia analizată, Comisia Europeană a identificat, în comunicarea ”Digitalizarea justiției în Uniunea Europeană- O panoplie de posibilități”, din 2 decembrie 2020, necesitatea de modernizare a cadrului legislativ al procedurilor transfrontaliere în materie civilă, comercială și penală, conform principiului ”digital în mod implicit”.

În privința sporirii eficienței și a eficacității procedurilor judiciare și facilitarea accesului la justiție prin digitalizarea canalelor de comunicare, s-a simțit nevoia unei noi reglementări care să asigure acest deziderat al Comisiei.

La nivel național, se simte necesitatea implementării acestor soluții tehnice pentru a se produce o aliniere efectivă la principiile justiției digitale. Astfel cum s-a apreciat în literatura de specialitate, tehnologia ne stăpânește viața cotidiană într-o anumită măsură, iar justiția nu poate rămâne impasibilă în fața acestui aspect¹⁶. Astfel cum autorul subliniază, digitalizarea justiției apare ca o expresie nouă a unor drepturi și principii consacrate, dar și anumite dileme la care colaborarea dintre aspectul juridic și aspectul tehnic sunt chemate să răspundă.

Pentru o analiză corectă modului în care justiția poate să se adapteze tendinței de digitalizare, nu trebuie neglijate drepturile fundamentale garantate oricărui cetățean și totodată principiile care guvernează litigiile în România. Acest aspect este deosebit de important prin raportare la garanțiile pe care justiția le oferă pe de o parte, iar pe de altă parte, la posibilitatea ca digitalizarea justiției să poată naște ingerințe în aceste drepturi și principii consacrate la nivelul sistemului judiciar din România.

Fără a intra în analiza avantajelor și dezavantajelor pe care inteligența artificială le poate genera în domeniul justiției, în acest capitol ne vom rezuma doar la aspecte privind digitalizarea, aspecte care în mod evident sunt mult mai puțin riscante față de sistemele de inteligență artificială, însă și acestea pot genera anumite atingeri drepturilor fundamentale și principiilor care guvernează justiția *lato sensu*.

Este indiscutabilă preocuparea existentă în literatura de specialitate și la nivelul autorităților cu competențe în gestionarea digitalizării în justiție deoarece dreptul la un proces echitabil și principiul publicității ședinței de judecată trebuie să fie în continuare respectate, în caz contrar prin digitalizare s-ar aduce atingere drepturilor și principiilor care guvernează mare parte din activitatea judiciară.

¹⁵ Gabriel-Liviu Ispas, Daniela Panc, *Dreptul Instituțional al Uniunii Europene, ediția a II-a revizuită și adăugită*, ed. Hamangiu, București, 2021, pp. 97-104

¹⁶ Adrian Onacă, *Transparența justiției în era digitalizării*, articol publicat în revista Themis 1-2/2023, disponibil pe site-ul Institutului Superior al Magistraturii.

3.2. Digitalizarea în justiție și drepturile și principiile fundamentale

Promovarea digitalizării la nivelul Uniunii Europene nu poate aduce atingere drepturilor și principiilor fundamentale existente, astfel încât toate inițiativele legislative dar și actele adoptate la nivelul Uniunii trebuie să respecte independența sistemului judiciar și totodată trebuie să fie conforme statului de drept, una dintre valorile fundamentale ale Uniunii și ale statelor membre.

Inițiativele care se referă la digitalizarea în justiție trebuie să țină cont de respectarea dreptului la un proces echitabil, dreptul de a fi prezent la proces și dreptul la apărare. Astfel cum s-a reținut în strategia privind digitalizarea justiției, o privire atentă a respectării acestor drepturi trebuie acordată în materia justiției penale dar, din punctul nostru de vedere, respectarea drepturilor și principiilor trebuie să se facă în privința oricăror proceduri judiciare deoarece apariția acestor tehnologii inovatoare trebuie precedată de o analiză efectivă pentru a se garanta respectarea drepturilor tuturor cetățenilor.

Tehnologiile și serviciile inovatoare pot da naștere, fără puțință de tăgadă, unor provocări și riscuri, care trebuie contracarate în vederea garantării protecției drepturilor și principiilor fundamentale aplicate la nivelul Uniunii și la nivelul statelor membre.

3.2.1. Digitalizarea justiției și dreptul la un proces echitabil

Dreptul la un proces echitabil este un drept fundamental consfințit de art. 6 din CEDO, art. 21 din Constituția României care reglementează accesul liber la justiție și prevede în alin. 3 dreptul părților la un proces echitabil și la soluționarea cauzelor într-un termen rezonabil.

În contextul digitalizării justiției, autoritățile cu competențe în domeniu nu se pot îndepărta de la acest drept la un proces echitabil deoarece, riscul ca acest drept să fie încălcat este mult mai mare ținând cont că digitalizarea poate genera încălcări ale securității cibernetice, adâncirea decalajului digital sau o discriminare care să fie cauzate de algoritmi utilizați sau alte date cu conținut părtinitor.

Dincolo de simpla digitalizare a serviciilor de justiție oferite cetățenilor, trebuie să avem în vedere și implementarea tehnologiilor bazate pe inteligența artificială care este de natură să faciliteze și să îmbunătățească accesul la justiție, astfel cum vom arăta în capitolul referitor la implementarea sistemelor de IA în justiție.

Pentru a obține efectul dorit, este necesară o analiză amănunțită realizată anterior implementării acestor principii, în vederea oferirii garanțiilor conforme celor care sunt în final destinatarii serviciilor digitale.

Dreptul la un proces echitabil, astfel cum acesta a fost reglementat, asigură participanților la actul de justiție anumite garanții puternice, menite să îi asigure pe aceștia că litigiile sunt judecate într-un termen rezonabil de o instanță imparțială și independentă, instituită prin lege, care să hotărască asupra încălcării drepturilor civile sau asupra temeiniciei oricărei acuzații în materie penală.

În situația în care instanțele de judecată încalcă dreptul la un proces echitabil, părțile din litigiu se pot adresa Curții Europene a Drepturilor Omului care se va pronunța asupra echilibrului dintre

justiția națională și prevederile Convenției. Cu titlu de exemplu, dreptul la un proces echitabil a generat de-a lungul timpului o amplă jurisprudență la nivelul CEDO, statele semnatare ale Convenției fiind condamnate pentru încălcarea art. 6 care reglementează dreptul la un proces echitabil.

În contextul analizat, acela al digitalizării justiției, drepturile fundamentale trebuie să fie garantate de fiecare stat membru în continuare și poate protecția trebuie să fie și mai sporită câtă vreme, prin efectul digitalizării, intervin aspecte de noutate care constau în sisteme, sisteme care înlocuiesc în mare parte persoanele care se asigurau de respectarea acestor drepturi.

Estonia reprezintă un exemplu elocvent în materia implementării sistemului ”judecătorului robot”. În fiecare an, sunt între 30.000 și 34.000 de astfel de cazuri care pot fi soluționate de judecătorul-robot. Restul cazurilor civile care ajung în varianta clasică în instanță sunt tot în jurul a 30.000. În acest moment, doar 10% din cazurile rezolvate de sistemul semiautomatizat actual care presupune în continuare validarea umană sunt contestate și ajung pe masa unui judecător-om. În comparație, cazurile clasice sunt contestate în proporție de 6%. Ambele rate de încredere în justiția estoniană sunt foarte mari, iar numărul de apeluri în cazurile judecate de sistemul semiautomatizat sunt mai multe, dar nu uriaș. Pârâțul are dreptul să obiecteze și nu trebuie să vină cu vreo explicație pentru asta. Pârâțul poate spune doar că nu e de acord și acolo se termină totul. Se încheie partea sistemului automat și dosarul ajunge la un judecător-om. “Este o chestiune la care ne gândim: cum să construim sistemul ca să existe salvamari, căi adiacente de rezolvare pentru a proteja drepturile fundamentale. Cred că sistemul judiciar curent pe jumătate automatizat este bine primit de societate. Nu cred că au fost cazuri care să fi contestat constituționalitatea sistemului”.

Modelul estonian este un exemplu foarte bun de implementare a digitalizării și a inserării în activitatea de justiție a sistemelor bazate pe inteligența artificială. Astfel cum precizam într-un articol de specialitate publicat¹⁷, din punctul nostru de vedere, în privința litigiilor civile de o dificultate redusă, care pot fi soluționate într-un mod automatizat, considerăm că un sistem de IA poate soluționa un astfel de litigiu. Cu toate că cel puțin în mod aparent se poate presupune că această idee nu poate fi pusă în aplicare, la nivel mondial roboții, deci sistemele de IA au luat locul mediatorilor, avocaților, judecătorilor, procurorilor, polițiștilor¹⁸. Potrivit unor articole identificate în presa din România, în Estonia există deja un robot care soluționează dosare cu o valoare de cel mult 6400 EUR, litigii care nu presupun un probatoriu complex care pot avea ca obiect: divorțuri, datorii neachitate, contracte care nu au fost respectate de părți. În Estonia există un grad impresionant de digitalizare, aspect care ușurează inclusiv intentarea acestor litigii care să fie soluționate de judecătorul.... robot. Decizia robotului poate fi contestată, moment în care litigiul va fi soluționat de judecătorul.... om. Din datele existente în articolul citat, dacă judecătorul robot va da dovadă de acuratețe, filtrând în mod corect datele care îi sunt puse la dispoziție, acesta ar putea judeca și litigii care să ajungă la o valoare de 15.000 EUR.

¹⁷ Petruța- Elena Ispas, *Artificial Intelligence. New Challenges*, articol publicat în Central And Eastern European Legal Studies (CEELS) nr. 2/2023, ISSN 2310-2705, paginile 189-204;

¹⁸ <https://mediaflux.ro/judecatorii-roboti-inteligenta-artificiala-da-verdict-e-in-procese-civile-cu-mize-mic/>;
https://www.dcbusiness.ro/ultima-inventie-a-chinezilor-te-infioara-omul-judecat-de-robot_638626.html;

O testare asupra unui jurist robot s-a realizat și în Statele Unite ale Americii, unde societatea Law Geex a organizat un concurs între om și robot, fiind selectate 30 întrebări de către un juriu format din trei experți de la Stanford și Harvard, întrebările fiind referitoare la 5 contracte. Concursul s-a desfășurat între un robot și cei mai buni practicieni din Statele Unite ale Americii, specializați în contractele selectate. Conform datelor puse la dispoziție de experții din juriu, acuratețea răspunsurilor roboților a fost de 90% iar cea a oamenilor juriști a fost de 85%. Roboții au răspuns în 26 secunde la 20 probleme ridicate, în timp ce oamenii juriști au răspuns în aproximativ 80-90 minute. Având în vedere că în această perioadă doar se pot face anumite testări în acuratețea acestor sisteme de IA, nu vedem ca fiind imposibil ca în câțiva ani să vedem o concurență între oameni și roboți în sălile de judecată.

În China a fost testat și un robot procuror care, potrivit detaliilor existente în presă¹⁹, face cercetări pe infracțiuni precum: furt, conducere periculoasă, fraudă cu carduri de credit, fiind programat printr-un sistem de IA. Este adevărat că în China cercetarea este una evoluată, fără a putea emite aceleași pretenții cu privire la statul român care, dincolo de adoptarea unei strategii privind IA, nu observăm niciun studiu publicat, nicio aplecare a autorităților spre a cunoaște și înțelege cât mai bine cum funcționează sistemele de IA.

Exemplele vor fi dezvoltate și în capitolul referitor la inteligența artificială în justiție, însă nu putem nega faptul că digitalizarea reprezintă primul pas în aplicarea sistemelor de IA, astfel încât noțiunile nu pot fi în mod absolut disociate.

Este fără putință de tăgadă faptul că implementarea principiilor raliate digitalizării poate să dea naștere inclusiv unor probleme de etică, pe lângă problemele aferente garantării accesului la un proces echitabil. Rămâne la latitudinea statelor membre să își creeze mecanisme eficiente de protecție a drepturilor și principiilor fundamentale deoarece sistemul de justiție trebuie să țină pasul cu progresul tehnologic, fără însă a face rabat la garanțiile care însoțesc drepturile fundamentale ale cetățenilor.

Nu în ultimul rând, se cuvine a menționa faptul că, așa cum menționam și anterior, dreptul la un proces echitabil nu este un drept lipsit de conținut; dimpotrivă, protecția acestui drept a fost evidențiată în multe cauze, CEDO condamnând statele semnatare ale Convenției pentru ineficiența protecție acordată acestui drept fundamental.

Fără a ne dori să facem o analiză a practicii CEDO, se cuvine a menționa că și România a fost condamnată în numeroase rânduri pentru încălcarea art. 6 din CEDO, atât în litigii civile cât și în litigii penale soluționate de instanțele de judecată naționale cu încălcarea acestui drept fundamental al omului, astfel încât în contextul adaptării sistemului de justiție la noile tehnologii, este imperios necesară respectarea dreptului fundamental la un proces echitabil.

3.3. Digitalizarea justiției și transparența actului de justiție

Transparența, ca principiu fundamental aplicabil în sistemul judiciar are un rol deosebit de important în stabilirea încrederii publicului în actul de justiție și în general în autoritatea

¹⁹ <https://www.express.co.uk/news/science/1542035/china-news-robot-prosecutor-public-crimes-robot-police-dissent>.

judecătorească, al eficienței actului de justiție în ansamblul său dar și al unei eficientizări conforme a procedurilor derulate.

Publicitatea sau transparența actului de justiție nu poate fi disociată de dreptul la un proces echitabil, astfel cum acesta este consfințit în art. 6 din CEDO.

Din modul de reglementare a art. 6 par. 1 din CEDO, potrivit căruia ”Hotărârea trebuie să fie pronunțată în mod public, dar accesul în sala de ședință poate fi interzis presei și publicului pe întreaga durată a procesului sau a unei părți a acestuia în interesul moralității, al ordinii publice ori al securității naționale într-o societate democratică, atunci când interesele minorilor sau protecția vieții private a părților la proces o impun, sau în măsura considerată absolut necesară de către instanță atunci când, în împrejurări speciale, publicitatea ar fi de natură să aducă atingere intereselor justiției”. Astfel, însăși Convenția stabilește anumite limite care trebuie respectate cu privire la publicitatea ședinței de judecată.

Ședința de judecată este publică de regulă, însă se pot întâlni și situații de excepție în care accesul publicului la ședința de judecată poate fi restricționat. Totodată, principiul transparenței sau al publicității ședinței de judecată poate suferi o ingerință dacă publicitatea este de natură să aducă atingere intereselor justiției.

Transparența actului de justiție trebuie să se facă totuși cu respectarea celorlalte drepturi fundamentale, cum sunt datele cu caracter personal. În același context al digitalizării, în prezent în România sunt dezvoltate mai multe aplicații legislative care acordă access la hotărârile judecătorești pronunțate de instanțele naționale. Publicarea acestora se face cu anonimizarea datelor cu caracter personal ale părților implicate în litigiu.

Totodată, se impune a preciza că atât Codul de procedură civilă cât și Codul de procedură penală din România impun regula de publicitate a ședinței de judecată, cu anumite excepții pe care le vom arăta în cele ce urmează.

Astfel, potrivit art. 213 alin. (2) Cod procedură civilă, *”De asemenea, în cazurile în care dezbaterile fondului în ședință publică ar aduce atingere moralității, ordinii publice, intereselor minorilor, vieții private a părților ori intereselor justiției, după caz, instanța, la cerere sau din oficiu, poate dispune ca aceasta să se desfășoare în întregime sau în parte fără prezența publicului”*, în timp ce conform art. 352 alin. (3) Cod procedură penală, *”Dacă judecarea în ședință publică ar putea aduce atingere unor interese de stat, moralei, demnității sau vieții intime a unei persoane, intereselor minorilor sau ale justiției, instanța, la cererea procurorului, a părților ori din oficiu, poate declara ședință nepublică pentru tot cursul sau pentru o anumită parte a judecării cauzei”*. Astfel cum rezultă din dispozițiile legale citate mai sus, codurile de procedură stabilesc, în conformitate cu art. 6 din CEDO acest principiu fundamental al procesului civil sau penal, publicitatea ședinței de judecată putând fi exceptată doar în situațiile expres reglementate de lege.

Digitalizarea în justiție este un fenomen complex care nu poate fi ignorat. Este adevărat că un domeniu care s-a dezvoltat în timp independent de existența suportului digital poate fi ușor mai reticent la schimbare însă, astfel cum vom vedea în cele ce urmează, la nivelul UE digitalizarea justiției este amplu analizată și deja în foarte multe state member implementată.

Digitalizarea trebuie diferențiată de conceptul inteligenței artificiale deoarece al doilea concept este unul mult mai complex, astfel cum vom analiza pe parcursul prezentei lucrări.

Ca și aplicabilitate în digitalizarea justiției, întâlnim accesul la baze de date jurisprudențiale, sistematizarea hotărârilor judecătorești pentru o ușoară identificare după obiectul cererilor de chemare în judecată sau după gradul procesual în care se pronunță o hotărâre judecătorească. Tot ca o aplicație practică a digitalizării justiției este și implementarea dosarului electronic sau site-ul dedicat instanțelor de judecată, în care justițiabilii pot urmări cursul unui dosar din fazele incipiente, în fazele sale intermediare și până la pronunțarea hotărârii judecătorești.

Chiar dacă în aparență aceștia sunt pași mărunți făcuți spre o digitalizare într-o perioadă în care inteligența artificială este prezentă pretutindeni, totuși aceste măsuri de digitalizare vin să ușureze foarte mult activitatea practicienilor dreptului dar și a justițiabililor care tind la apărarea drepturilor pe cont propriu, fără ajutor specializat din partea unui avocat.

Un alt domeniu conex activității de justiție în care digitalizarea este prezentă este și activitatea derulată de Oficiul Național al Registrului Comerțului care a implementat un sistem de lucru electronic, aspect deosebit de important pentru profesioniștii comercianți care își pot înregistra mențiunile în Registrul Comerțului de la distanță, prin folosirea sistemului electronic.

Tot din perspectiva digitalizării domeniilor conexe actului de justiție se poate menționa și comunicarea actelor administrativ- fiscale și a altor acte de executare emise de organele fiscale.

Cu toate că digitalizarea în România este incomparabilă cu alte state membre în care inclusive autentificarea actelor notariale poate fi făcută la distanță, totuși în ultima perioadă s-au făcut pași importanți spre o deschidere cât mai mare a sistemului judiciar față de era digitală.

Este adevărat că implementarea unor soluții digitale trebuie să țină cont și de respectarea principiilor fundamentale care guvernează sistemul judiciar, însă digitalizarea presupune riscuri mai mici la adresa acestor drepturi în comparație cu inteligența artificială care, astfel cum vom analiza în cele ce urmează, poate ridica mari probleme pe protecția drepturilor fundamentale.

Capitolul 4

Open data în activitatea judiciară²⁰

Hotărârile instanțelor judecătorești rămân un relevator important al celor mai semnificative probleme juridice ale indivizilor și societății, care își așteaptă răspunsuri cât mai rapide și mai complete. Jurisprudența se manifestă și ca un factor de cunoaștere și explicitare a mersului dreptului pozitiv, de motor de impunere și exprimare a particularităților anumitor materii.

Disponibilitatea hotărârilor judecătorești, prin publicare sau distribuție electronică, vizează obiective de natură democratică, privind buna funcționare a statului de drept prin cunoașterea lor de către cetățeni. Caracterul public al procesului civil și penal, în înțeles tradițional, satisface acest obiectiv doar formal, în timp ce publicarea tuturor hotărârilor și diseminarea mai largă conduc, cel puțin indirect, la realizarea acestui obiectiv.

Publicitatea neîngrădită a tuturor hotărârilor judecătorești îndeplinește și un obiectiv distinct, de cunoaștere a conținutului lor, întrucât atunci când cercetarea se referă la normele de drept care rezultă din activitatea judiciară, difuzarea publică a hotărârilor poate fi limitată la hotărârile susceptibile de a stabili jurisprudența, aparținând în special instanțelor ierarhic superioare.

La nivel național, implementarea principiului accesului liber și gratuit la hotărâri judecătorești reprezintă un proces în derulare.

Dacă într-o etapă incipientă, jurisprudența națională a fost supusă diseminării prin intermediul unor repertorii de practică sau culegeri de jurisprudență, începând cu anul 2005, implementarea sistemului ECRIS a reprezentat o dimensiune a creșterii transparenței, ca direcție esențială a strategiei de reformă a sistemului judiciar, fiind destinat să furnizeze inclusiv informații referitoare la jurisprudența relevantă.

În acest context, la nivelul Tribunalului Vrancea a fost pusă în practică, experimental, ideea serviciului JURINDEX-index de jurisprudență, întemeiată pe principiul accesului liber, general și gratuit la hotărârile judecătorești, potrivit căruia cetățenii au dreptul să cunoască orice hotărâre judecătorească pronunțată de instanțele din România, indiferent de gradul lor, iar autoritățile au obligația să garanteze exercitarea acestui drept prin publicarea în mod gratuit și integral a tuturor hotărârilor judecătorești pronunțate, în forma lor originală, fără vreo altă intervenție decât eliminarea datelor cu caracter personal. Programul JURINDEX a fost ulterior reorganizat într-un Portal național de centralizare a jurisprudenței instanțelor, gestionat de Institutul Român pentru Informații Juridice-RoLII, cu scopul punerii la dispoziția publicului, în format deschis și gratuit, a surselor primare și secundare de drept, ca parte a patrimoniului comun național și internațional, în scopul promovării justiției și statului de drept.

²⁰ Gabriel Manu, Open data în materia hotărârilor judecătorești, articol publicat în Revista Universul Juridic, Revistă lunară de doctrină și jurisprudență | ISSN 2393-3445, la data de 1 octombrie 2020, disponibil la adresa web: <https://revista.universuljuridic.ro/open-data-materia-hotararilor-judecatoresti/>.

„Open data” (date deschise) desemnează datele digitale, de origine publică sau privată, accesibile și utilizabile în mod liber, iar „big data” (date mari) se referă la seturi de date digitale deosebit de mari produse de noile tehnologii și stocate folosind instrumente informatice de înaltă performanță.

În raport de aceste definiții, aplicarea teoriei „open/big data” în materia jurisprudenței se referă la punerea la dispoziția publicului, într-un format accesibil și reutilizabil, a hotărârilor judecătorești.

Totodată, „open/big data” în domeniul hotărârilor judecătorești are ca rezultat eliminarea diferenței, de natură cantitativă, dintre hotărârile publicate și cele pronunțate, obiectiv cu atât mai important cu cât această diferență este considerabilă. Diferența este și calitativă, întrucât hotărârile publicate sunt alese datorită interesului legal pe care îl prezintă, fără să constituie un eșantion reprezentativ al masei hotărârilor și hotărârilor pronunțate.

Sistemele naționale reglementează în mod diferit dreptul persoanelor de a avea acces general și gratuit la totalitatea hotărârilor judecătorești, de a avea acces la forma originală și completă a acestora, de a utiliza liber și a disemina copii ale hotărârilor judecătorești, precum și dreptul părților din dosare de a le fi protejate datele cu caracter personal și datele de identificare.

În România, actul normativ incident în materie este Legea nr. 544/2001 privind liberul acces la informațiile de interes public, ale cărei dispoziții nu reglementează explicit situația hotărârilor judecătorești ca făcând parte din sfera informațiilor de interes public, ci doar dreptul general al persoanelor de a solicita și obține de la autoritățile și instituțiile publice, în condițiile legii, informațiile de interes public și obligația corelativă a acestora de a asigura persoanelor informațiile de interes public solicitate în scris sau verbal (art. 6).

Acest context normativ, care a permis poziționarea contradictorie, în timp, a Consiliului Superior al Magistraturii față de situația hotărârilor judecătorești ca informații de interes public, au condus la o aplicare neunitară a Legii nr. 544/2001, instanțele oscilând între a considera:

– că informațiile solicitate de către reclamant, respectiv copii ale unor hotărâri judecătorești irevocabile, intră în categoria celor de interes public, prevăzute de art. 2 lit. b) din Legea nr. 544/2001, deoarece privesc sau rezultă din activitățile pârâtei, care este o instituție publică, nefiind necesar ca reclamantul să dovedească motivul pentru care se solicită informațiile. S-a avut în vedere că informațiile solicitate nu fac parte din cele menționate la art. 12 din lege ca fiind exceptate de la a accesul liber al cetățenilor;

– că „o hotărâre judecătorească nu reprezintă o informație de interes public, în sensul art. 2 lit. b) din Legea nr. 544/2001 și privește raporturile dintre părțile cauzei, iar hotărârile judecătorești soluționează, cu preponderență, litigii private”, iar „publicarea hotărârilor judecătorești anonimizate pe paginile de internet ale instanțelor oferă suficiente repere pentru cunoașterea jurisprudenței naționale”. În speță, motivul invocat de reclamant, în sensul că dorea să îi fie comunicată hotărârea judecătorească deoarece „efectuează studii și cercetări în interes propriu” a fost respins, instanța arătând că reclamantul nu a făcut dovada efectuării studiilor și cercetărilor în interes propriu sau de serviciu, ci este interesat din alte motive de hotărârea judecătorească solicitată.

Un model de bune practici în materie este cel francez, cu precizarea că în Franța sistemul instanțelor administrative independente, în frunte cu Consiliul de Stat, este distinct de cel al instanțelor ordinare.

Articolul 10 alin. (2) din Codul de justiție administrativă francez prevede că hotărârile judecătorului administrativ sunt la dispoziția publicului cu titlu gratuit, cu respectarea dreptului la viață privată al persoanelor.

Recent, prin Decretul nr. 2020-797 din 29 iunie 2020 privind punerea la dispoziția publicului a deciziilor instanțelor judiciare și administrative, obligația de punere la dispoziția publicului a deciziilor instanțelor judiciare și administrative a fost generalizată, cu restricții privind anonimizarea anumitor elemente, în special cele ce privesc identitatea persoanelor fizice.

Modul în care această reglementare a fost receptată în Franța la nivel social și judiciar, surprins într-un studiu dedicat, ce urmează a fi redat în ideile principale, poate fi relevant pentru fundamentarea, adoptarea și implementarea unor soluții similare în sistemul nostru național.

Experiența franceză a generat o preocupare specială în privința limitării impuse disponibilității hotărârilor judecătorești, în special prin exceptarea de la regula publicității a anumitor elemente sau a unor categorii de hotărâri.

S-a apreciat că dacă, în această privință, Decretul nr. 2020-797 din 29 iunie 2020 răspunde anumitor întrebări, în special prin desemnarea autorităților responsabile de exceptare/anonimizare, dă naștere altora, prin crearea unor cazuri suplimentare de exceptare, în afara dispozițiilor legale.

Aceasta are în vedere nu doar punerea la dispoziție în formă electronică a hotărârilor (open data), ci și punerea la dispoziție de copii, către terți, în special prin transpunerea anumitor limitări necesare în contextul distribuției pe Internet.

În privința ascunderii elementelor de identitate ale persoanelor fizice, Legea nr. 2018-2022 prevede anonimizarea sistematică – numai în contextul datelor deschise – ale „numelui persoanelor fizice menționate în decizie, atunci când acestea sunt părți sau terți”. Noțiunea de „terț” nu este definită legal, dar s-a stabilit că nu poate viza personalul instanțelor (magistrați, grefieri) ori avocații.

În contextul open data, în cazul emiterii de copii ale hotărârilor judecătorești, se poate lua decizia de a ascunde „orice alt element de identificare” vizând elemente referitoare la părți și la „terți”. Criteriile de aplicare a acestei reguli se raportează la principiul că divulgarea unui astfel de element este „susceptibilă să aducă atingere securității sau respectului pentru viața privată a persoanelor fizice menționate în hotărâre sau a anturajului lor” și, întrucât nu sunt foarte precise, s-a apreciat că aplicarea lor ar putea fi diferită de la o instanță la alta, în special în ceea ce privește magistrații și personalul auxiliar al instanțelor.

Pentru a înlătura temerile astfel manifestate, Curtea de Casație și Ministerul Justiției din Franța au anunțat că, pentru a asigura coerența aplicării exceptărilor suplimentare impuse prin decretul

de aplicare a Legii nr. 2018-2022, regulile de armonizare a practicii vor fi dezvoltate colegial, în special prin intermediul grupurilor de lucru aflate sub egida Curții de Casație.

Dacă ascunderea identității sau a elementelor de identificare este de înțeles în ceea ce privește protecția necesară a datelor cu caracter personal, Decretul nr. 2020-797 din 29 iunie 2020, suplimentar față dispozițiile legii, impune restricții de publicitate și în privința altor elemente ale hotărârilor sau a unor categorii de hotărâri judecătorești. Cu titlu de exemplu, în fața jurisdicțiilor administrative, președintele instanței poate „decide să ascundă orice element al deciziei a cărei divulgare poate încălca interesele fundamentale ale națiunii”, iar în materie penală se poate decide, pe aceeași bază sau din cauza unei vătămări aduse „secretului industrial și comercial”.

Aceste criterii, ce instituie limite în privința publicității hotărârilor judecătorești, prezintă un pronunțat caracter de generalitate, favorizează o aplicare practică neunitară și afectează caracterul accesibil și previzibil al normei.

Oportunitățile create prin aplicarea conceptului open data în materia hotărârilor judecătorești sunt numeroase, în special pentru a dezvolta abordări detaliate ale realității, de natură statistică, sociologică etc., iar importanța și rolul caracterului public al hotărârilor judecătorești, fără restricții și limitări din considerente de oportunitate ori în baza unor criterii subiective, sunt de necontestat, inclusiv din perspectiva realizării unei justiții predictive.

Pornind de la experiența franceză în materie, o viitoare reglementare națională va trebui, prin conținutul său, să elimine incertitudinile privind criteriile pentru limitarea publicării și anonimizarea anumitor elemente ale hotărârilor judecătorești.

Capitolul 5

Inteligența artificială

Principiile administrării justiției și IA. Reglementarea instrumentelor de IA în justiție. Controlul utilizării IA în justiție. Regulamentul privind IA

5.1. Reglementarea europeană

În expunerea de motive a Regulamentului UE 2024/1689, se reiterează faptul că inteligența artificială (în continuare IA) reprezintă o familie de tehnologii cu evoluție rapidă, care poate să genereze o gamă largă de beneficii economice și societale în întregul spectru de industrii și activități sociale. Tot în expunerea de motive s-a statuat că acest de regulament are la bază valorile și drepturile fundamentale ale Uniunii Europene (în continuare UE) și urmărește să ofere oamenilor și altor utilizatori încrederea de a adopta soluții bazate pe IA dar să și garanteze acestora că pot avea încredere că tehnologia este utilizată într-un mod sigur și conform cu legislația, inclusiv cu respectarea drepturilor fundamentale.

Expunerea de motive tratează inclusiv problematica drepturilor fundamentale, prin prisma faptului că deși utilizarea sistemelor de IA poate afecta în mod negativ o serie de drepturi fundamentale consacrate în Carta drepturilor fundamentale a UE, prin regulament se urmărește asigurarea unui nivel ridicat de protecție a dreptului la demnitatea umană, respectarea vieții private și protecția datelor cu caracter personal, nediscriminarea și egalitatea între femei și bărbați, dar și dreptul la liberă exprimare, libertatea de întrunire, protecția dreptului la o cale de atac eficientă și la un proces echitabil, dreptul la apărare și prezumția de nevinovăție și principiul general al bunei administrări.

Este adevărat că reticența în utilizarea sistemelor de IA poate apărea ca justificată în contextul în care însuși regulamentul menționează că există și sisteme care creează un risc inacceptabil, aceste practici fiind interzise prin regulamentul supus analizei. Îngrijorarea asupra acestor sisteme de IA este cu atât mai mare cu cât prin actul normativ european s-a stabilit care sunt aceste practici interzise în domeniul IA și ce marjă de apreciere are fiecare stat membru în autorizarea, spre exemplu, a utilizării anumitor sisteme de identificare biometrică la distanță în timp real. Această reglementare este făcută, din punctul nostru de vedere, în termeni generali care sunt de natură a da naștere cel puțin unor interpretări dacă nu chiar mai mult decât atât să dea naștere unei ingerințe nepermise în drepturile fundamentale ale cetățenilor.

Într-un articol publicat în literatura de specialitate europeană²¹, se analizează evoluția legislativă a identificării biometrice și bineînțeles beneficiile și riscurile utilizării acestui de sistem de IA, autorii apreciază că aceste condiții propuse ar putea avea un efect negativ asupra arestării infractorilor iar obligația de a obține o autorizare judiciară ar putea conduce la scăparea unui făptuitor sau la împiedicarea prevenirii unui atac terorist sau a unei infracțiuni împotriva vieții.

Din punctul nostru de vedere, problematica identificării biometrice trebuie să aibă în vedere și o posibilă încălcare a drepturilor fundamentale. Care ar fi soluția în cazul în care, la trecerea unei

²¹ Vangelis Papakonstantinou, Evangelos Zarkadoulas, *Remote Biometric and emotion recognition in the context of Law Enforcement*, articol disponibil la adresa web <https://eucrim.eu/articles/remote-biometric-identification-and-emotion-recognition-in-the-context-of-law-enforcement/>.

frontiere, pe baza informațiilor create de sistemul de IA o persoană este reținută sau arestată și ulterior se dovedește că persoana respectivă nu se face vinovată de săvârșirea niciunei fapte prevăzute de legea penală? Apreciem că în baza articolului 5 din propunerea de regulament autoritățile trebuie să cântărească foarte bine avantajele și dezavantajeze utilizării identificării biometrice și să aibă în vedere situațiile în care acestea pot fi folosite, mai ales având în vedere că dacă se dovedește că identificarea s-a făcut fără ca persoana să fie vinovată de săvârșirea unei fapte prevăzute de legea penală, aceasta se poate îndrepta cu o acțiune în despăgubiri pentru repararea prejudiciului cauzat. Având în vedere toate aceste considerente, apreciem ca oportun ca la nivelul UE sau, în ipoteza în care statele membre vor stabili în dreptul intern condițiile necesare pentru solicitarea, eliberarea, exercitarea și supravegherea autorizațiilor pentru utilizarea sistemelor privind identificarea biometrică și, totodată, trebuie reglementate cu o atenție deosebită acele infracțiuni pentru care să fie posibilă utilizarea acestor identificări biometrice.

Apreciem ca utilă această abordare deoarece este evident de ce la nivelul UE se consideră că utilizarea datelor biometrice poate fi folosită doar în scopul respectării legii deoarece sistemele la care facem referire conțin date cu caracter personal care sunt protejate de către lege. În acest context, apreciem că se impune ca utilizarea acestor date de identificare să poată fi făcută doar cu o autorizare prealabilă și exclusiv în legătură cu infracțiunile reglementate. Când se pune problema accesării unor date cu caracter special, trebuie cântărit foarte atent interesul care să justifice folosirea identificării biometrice.

În privința utilizării sistemelor de IA destinate administrării justiției și proceselor democratice, regulamentul²² prevede faptul că acestea ar trebui să fie clasificate ca prezentând un grad ridicat de risc, având în vedere impactul potențial semnificativ al acestora asupra democrației, statului de drept și libertăților individuale, precum și asupra dreptului la o cale de atac efectivă și la un proces echitabil. În special, pentru a aborda potențialele riscuri de prejudecăți, erori și opacitate, este oportun să fie calificate drept sisteme cu grad ridicat de risc sistemele de IA destinate să fie utilizate de o autoritate judiciară sau în numele acesteia pentru a ajuta autoritățile judiciare să cerceteze și să interpreteze faptele și legea și să aplice legea unui set concret de fapte. Sistemele de IA destinate a fi utilizate de organismele de soluționare alternativă a litigiilor în aceste scopuri ar trebui, de asemenea, să fie considerate ca având un grad ridicat de risc atunci când rezultatele procedurilor de soluționare alternativă a litigiilor produc efecte juridice pentru părți. Utilizarea instrumentelor de IA poate sprijini puterea de decizie a judecătorilor sau independența sistemului judiciar, dar nu ar trebui să le înlocuiască: procesul decizional final trebuie să rămână o activitate umană. Clasificarea sistemelor de IA ca prezentând un grad ridicat de risc nu ar trebui, totuși, să se extindă la sistemele de IA destinate unor activități administrative pur auxiliare care nu afectează administrarea efectivă a justiției în cazuri individuale, cum ar fi anonimizarea sau pseudonimizarea hotărârilor judecătorești, a documentelor sau a datelor, comunicarea între membrii personalului, sarcinile administrative.

În literatura de specialitate spaniolă²³ sunt analizate propunerile de regulament, fiind salutăta inițiativa legislativă existentă la nivelul UE și clasificarea sistemelor de IA pe categorii de risc.

²² Pct. 61 din Regulament

²³ Carmen Muñoz Garcia, *Regulacion de la inteligencia artificial en Europa*, ed. Tirant lo blanch, Valencia, 2023, pp. 38-43.

Se insistă pe principiile care stau la baza propunerii legislative, respectiv introducerea unor sisteme de IA sigure, transparente, care nu discriminează și care respectă mediul înconjurător. Tot în literatura de specialitate spaniolă se ridică problema eticii în utilizarea sistemelor de IA, fiind analizată posibilitatea interacțiunii între mașină, ca sistem de IA și oameni, cu privire atentă asupra unei interacțiuni stăpân-sclav, omul fiind cel care dictează mașinii ce comportament să aibă, atunci se pune problema unei autonomii limitate în ceea ce privește mașina ca sistem de IA.

În opinia noastră, regulamentul trasează suficiente elemente astfel încât utilizarea sistemelor de identificare biometrică să fie folosite în scopul pentru care a fost făcută legiferarea, respectiv în măsura în care se caută o potențială victimă a infracționalității, inclusiv a copiilor dispăruți, dacă se dorește prevenirea unei amenințări specifice, substanțiale sau iminente la adresa vieții sau a siguranței persoanelor fizice sau prevenirea unui atac terorist ori dacă se încearcă detectarea, localizarea, identificarea sau urmărirea penală a autorului unei infracțiuni. În acest context, folosirea sistemelor de date biometrice se poate face, din punctul nostru de vedere, doar în situațiile expres și limitativ reglementate, fără a putea extinde această aplicabilitate a utilizării sistemelor de IA deoarece, potrivit regulamentului, în afara situațiilor reglementate *expressis verbis*, utilizarea datelor de identificare biometrică este o practică interzisă în domeniul analizat.

Revenind la reglementarea dată prin regulament și legiferarea practicilor interzise în domeniul IA, se cuvine a menționa și faptul că, la nivelul UE, vor reprezenta practici interzise și următoarele: ”(a) introducerea pe piață, punerea în funcțiune sau utilizarea unui sistem de IA care utilizează tehnici subliminale fără ca persoanele să fie conștiente de acest lucru, pentru a denatura în mod semnificativ comportamentul unei persoane într-un mod care aduce sau poate aduce prejudicii fizice sau psihologice persoanei respective sau altei persoane; (b) introducerea pe piață, punerea în funcțiune sau utilizarea unui sistem de IA care exploatează oricare dintre vulnerabilitățile unui anumit grup de persoane din cauza vârstei, a unui handicap fizic sau mental, pentru a denatura în mod semnificativ comportamentul unei persoane care aparține grupului respectiv într-un mod care aduce sau poate aduce prejudicii fizice sau psihologice persoanei respective sau altei persoane; (c) introducerea pe piață, punerea în funcțiune sau utilizarea sistemelor de IA de către autoritățile publice sau în numele acestora pentru evaluarea sau clasificarea credibilității persoanelor fizice într-o anumită perioadă de timp, pe baza comportamentului lor social sau a caracteristicilor personale sau de personalitate cunoscute sau preconizate, cu un punctaj privind comportamentul social care conduce la una dintre următoarele situații sau la ambele: (i) tratamentul prejudiciabil sau nefavorabil al anumitor persoane fizice sau al unor grupuri întregi de persoane în contexte sociale care nu au legătură cu contextele în care datele au fost generate sau colectate inițial; (ii) tratamentul prejudiciabil sau nefavorabil al anumitor persoane fizice sau al unor grupuri întregi de persoane care este nejustificat sau disproporționat în raport cu comportamentul social al acestora sau cu gravitatea acestuia”. La aceste practici se adaugă și utilizarea sistemelor de identificare biometrică la care deja am făcut referire anterior.

Analizând prevederile regulamentului, este evident că la nivelul UE se acordă o atenție deosebită protecției drepturilor fundamentale ale persoanelor, acest aspect reiese fără putință de tăgadă din ceea ce UE consideră a reprezenta o practică interzisă în privința IA. După cum se poate observa, ingerințele permise în drepturile fundamentale sunt justificate de un interes superior, general, aspect care este conform legislației UE.

Regulamentul analizează și situația sistemelor de IA care prezintă un risc ridicat. Intră în această categorie sistemele IA care afectează negativ siguranța sau drepturile fundamentale, acestea urmând a fi împărțite în două categorii: sisteme IA utilizate în produsele care intră sub incidența legislației UE privind siguranța produselor (jucării, aviație, mașini, dispozitive medicale și ascensoare) și sisteme IA din opt domenii specifice care vor trebui înregistrate într-o bază de date a UE, după cum urmează: managementul și operarea infrastructurii critice, educație și formare profesională, ocuparea forței de muncă, managementul lucrătorilor și accesul la activități independente, accesul și folosirea unor servicii private esențiale, precum și a unor servicii și beneficii publice, aplicarea legii, gestionarea migrației, azilului și controlului la frontieră, asistența în interpretarea și aplicarea legii. Toate aceste sisteme cu risc ridicat vor fi evaluate înainte de a fi puse pe piață și, de asemenea, pe parcursul ciclului lor de viață.

După cum am analizat și anterior, UE a ales o reglementare a sistemelor de IA pe baza riscului. Sisteme de AI care vor ridica probleme sunt acele sisteme care prezintă un grad ridicat de risc și care vor fi utilizate după o atentă analiză a conformității acestora cu cerințele legale. Este adevărat că o reglementare nouă presupune și provocări noi, astfel încât cu siguranță la nivelul UE și la nivelul statelor membre se va resimți, cel mai probabil, o nevoie continuă de actualizare a acelor sisteme cu grad ridicat de risc, acest lucru urmând a se realiza în mod efectiv printr-o privire continuă și atentă asupra efectelor utilizării acestor sisteme.

Nu este de neglijat nici posibilitatea ca utilizarea unui sistem de AI să aibă efecte negative asupra sănătății sau siguranței persoanelor. Prin reglementarea adoptată la nivelul UE, se vede o preocupare în acest sens la nivel european, pe tot parcursul reglementării făcându-se referire la necesitatea protejării drepturilor fundamentale de eventualele vătămări care ar putea interveni ca urmare a utilizării unor sisteme de IA care presupun un grad de risc ridicat.

Ca o concluzie asupra necesității adoptării unei reglementări în materia IA, apreciem eforturile făcute la nivelul UE în vederea legiferării. Este de menționat că și în Statele Unite ale Americii, Casa Albă a anunțat la finele anului 2023 adoptarea unui ordin executiv pentru reglementarea IA. Nu este de mirare că dezvoltarea rapidă a sistemelor de IA poate genera pericole în lipsa unei reglementări, aspect care clarifică atât acțiunile de forță desfășurate la nivelul UE în vederea adoptării unui act normativ, cât și preocupările existente la nivelul Statelor Unite ale Americii, la nivelul Chinei etc. Nu este de neglijat nici summit-ul pentru IA, care a avut loc în luna noiembrie 2023 la Marea Britanie, ocazie cu care reprezentanți ai mai multor state, dar și persoane influente în dezvoltarea tehnologiei s-au reunit pentru a discuta despre acest subiect de mare actualitate. Ca urmare a acestei întâlniri, conform informațiilor publice disponibile, s-a decis înființarea unui consiliu consultativ global pentru reglementarea IA.

Dincolo de a epuiza aspectele care țin de reglementarea acestui domeniu atât de amplu și cu multiplele provocări care se vor înfățișa, vom finaliza aspectele referitoare la reglementarea IA la nivelul UE și vom analiza aspecte practice care implică utilizarea sistemelor de IA.

Pentru a se reafirma nivelul de securitate care se cere prin regulament cu privire la utilizarea sistemelor de IA, regulamentul²⁴ stabilește faptul că dacă un sistem de IA este clasificat ca sistem de IA cu grad ridicat de risc în temeiul prezentului regulament nu ar trebui să fie interpretat ca

²⁴ Paragraful 63 din Regulament

indicând că utilizarea sistemului este legală în temeiul altor acte ale dreptului Uniunii sau al dreptului intern compatibil cu dreptul Uniunii, cum ar fi în ceea ce privește protecția datelor cu caracter personal, utilizarea poligrafelor și a instrumentelor similare sau a altor sisteme pentru detectarea stării emoționale a persoanelor fizice. Orice astfel de utilizare ar trebui să continue să aibă loc numai în conformitate cu cerințele aplicabile care decurg din cartă, precum și din legislația secundară aplicabilă a Uniunii și din dreptul intern aplicabil. Regulament nu ar trebui să fie înțeles ca oferind temeiul juridic pentru prelucrarea datelor cu caracter personal, inclusiv a categoriilor speciale de date cu caracter personal, după caz, cu excepția cazului în care se specifică altfel în cuprinsul acestuia. Altfel spus, regulamentul privind IA nu trebuie privit ca un instrument juridic menit să încalce sau prin care să se deroge de la reguli imperative reglementate prin efectul legislației UE, ci prevederile regulamentului sunt menite să reglementeze sistemele de IA, să le clasifice pe categorii de riscuri în vederea asigurării unei protecții sporite în utilizarea acestora.

5.2. Inteligența artificială generativă. Problema ChatGPT

Un alt aspect de noutate în reglementarea europeană este problematica IA generativă. Acest domeniu specializat al IA este concentrat pe construirea unor modele ce pot genera un conținut nou realist, precum imagini, text, videoclipuri, pe baza unor date deja existente. Una dintre cele mai răsunătoare sisteme de IA generativă este reprezentată de ChatGBT, lansat de OpenAI.

Amendamentele adoptate de Parlamentul European²⁵ propunerii de regulament privind inteligența artificială ating și problema IA generative, stabilind în amendamentul 399 următoarele obligații ale furnizorului de modele de bază folosite în sistemele de IA destinate expres să genereze, cu diferite niveluri de autonomie, conținut precum texte, imagini, materiale audio sau video complexe și ale furnizorului care specializează un model de bază într-un sistem de IA generativ, trebuie, în plus: ”să respecte obligațiile de transparență prevăzute la articolul 52 alineatul (1), să antreneze și, după caz, să proiecteze și să dezvolte modelul de bază astfel încât să ofere garanții adecvate că nu produce conținut care încalcă dreptul Uniunii, în conformitate cu stadiul actual al tehnologiei general recunoscut și fără a aduce atingere drepturilor fundamentale, inclusiv libertății de exprimare și fără a aduce atingere legislației unionale sau naționale privind drepturile de autor, documentează și pun la dispoziția publicului un rezumat suficient de detaliat al modului în care sunt utilizate datele de antrenament protejate în virtutea legislației privind drepturile de autor”.

Când se pune problema utilizării sistemelor de IA generativă, trebuie analizate riscurile asociate cu folosirea acestora, printre aceste riscuri putând să existe și următoarele: lipsa transparenței, lipsa de acuratețe, subiectivism, riscurile legate de dreptul de proprietate intelectuală.

Deși ChatGBT este o metodă rapidă de a obține anumite informații, s-a concluzionat că utilizarea cel puțin a unei variante gratuite, nu oferă o acuratețe a informațiilor furnizate. Cercetătorii de la Universitatea Long Island²⁶ au adresat o serie de întrebări acestui sistem de IA generativă,

²⁵ Amendamentele au fost adoptate de Parlamentul European în data de 14 iunie 2023 prin documentul P9_TA (2023) 0236, disponibil la adresa web https://www.europarl.europa.eu/doceo/document/TA-9-2023-0236_RO.html.

²⁶ <https://www.euronews.ro/articole/chatgpt-nu-este-o-sursa-sigura-pentru-a-afla-raspunsuri-la-problemele-medicale-co>.

răspunsurile primite de la software au fost ulterior comparate cu afirmațiile scrise și revizuite de către farmaciști instruiți. Conform studiului realizat²⁷, ChatGBT a oferit răspunsuri precise doar la 10 întrebări, în privința celorlalte 29 întrebări, răspunsurile au fost inexacte, incomplete sau nu au fost furnizate răspunsuri.

În momentul în care ChatGBT a fost întrebat care sunt referințele științifice pe care se bazează, chatbot-ul a oferit cercetătorilor citate fictive. La o primă vedere, citările oferite de sistemul de IA generativă păreau legitime: erau adesea formatate corespunzător, furnizau adrese URL și erau listate în reviste științifice legitime. Problema a intervenit în momentul în care echipa a încercat să găsească articolele la care se face referire deoarece s-a concluzionat că ChatGPT le-a oferit citate fictive care doar în aparență erau legitime, în realitate acestea nu existau.

Din punctul nostru de vedere, utilizarea acestui chatbot nu reprezintă o variantă sigură de a obține informații având în vedere cel puțin următoarele aspecte: este acest sistem apt să ofere o acuratețe informațiilor furnizate? Indică acest sistem sursele avute în vedere la emiterea unui răspuns sau rezolvarea unei probleme? Care este "creierul" din spatele acestui chatbot? Doar oferind răspunsuri la aceste minime întrebări putem concluziona faptul că chatbot-ul ar trebui să fie folosit doar în vederea înțelegerii funcționalității lui și pentru a înțelege principiile care stau la baza sistemelor de IA generativă iar nu pentru a folosi informațiile primite drept surse credibile sau cu scopul redactării unei lucrări științifice sau altele asemenea.

La finalul anului 2023, New York Times a chemat în judecată OpenAI, compania care a dezvoltat ChatGBT, pentru încălcarea drepturilor de proprietate intelectuală generate de folosirea articolelor fără indicarea sursei și fără obținerea unui acord prealabil pentru folosirea acestora. Având în vedere că la acest moment cel puțin există un vid de reglementare, apreciem că pe viitor aceste litigii vor fi din ce în ce mai răspândite, în condițiile în care, într-adevăr, furnizarea unor informații colectate pe baza unei programări, fără a indica sursele citate, constituie încălcarea drepturilor de autor și a drepturilor conexe.

În contextul în care la nivel mondial se acordă o mare atenție acestor sisteme de IA generativă, este interesant de urmărit modalitatea în care se va stabili răspunderea pentru prejudiciile cauzate de aceste sisteme având în vedere că spre deosebire de sistemele de IA tradiționale, în cazul sistemelor de IA generativă acestea sunt antrenate folosind învățarea nesupravegheată, astfel încât software-ul nu primește nicio îndrumare explicită.

Din punctul nostru de vedere, conținutul creat prin sistemele de IA generativă ar trebui să aibă un caracter original, însă nu trebuie neglijat faptul că în definitiv informațiile care duc la crearea conținutului au la bază date cu care au fost antrenate, astfel încât originalitatea poate fi pusă sub semnul întrebării.

Din punct de vedere juridic, din perspectiva protecției drepturilor civile, utilizarea acestor sisteme de IA generativă va ridica foarte multe probleme având în vedere considerentele expuse anterior. Astfel, cum putem limita eventualele prejudicii pe care sistemele de IA le pot cauza? Care este modalitatea de protecție a dreptului de autor? Oare este exclusă posibilitatea verificării unui conținut cu scopul de a stabili dacă acel conținut este generat de IA? Ne punem aceste întrebări în contextul în care la acest moment nu este conturat întregul ansamblu normativ

²⁷ <https://edition.cnn.com/2023/12/10/health/chatgpt-medical-questions/index.html>.

aplicabil iar aceste întrebări sunt subsumate ideii unei folosiri în scopuri legitime a sistemelor de IA implementate. În eventualitatea programării acestor sisteme în scopuri ilegite, contrare actelor normative în vigoare, apreciem că legiuitorul european și statele membre se vor asigura de norme care să pedepsească astfel de comportamente.

5.3. Practicile interzise prin Regulamentul privind IA

Astfel cum precizam și anterior, la nivelul UE, în domeniul IA s-a încercat o demarcare clară între ceea ce reprezintă practică interzisă în domeniul analizat și ce reprezintă sistemul de IA cu grad ridicat de risc.

În conformitate cu dispozițiile art. 5 din Regulament, reprezintă practici interzise în domeniul IA:

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

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

(c) introducerea pe piață, punerea în funcțiune sau utilizarea unor sisteme de IA pentru evaluarea sau clasificarea persoanelor fizice sau a grupurilor de persoane pe o anumită perioadă de timp, pe baza comportamentului lor social sau a caracteristicilor personale sau de personalitate cunoscute, deduse sau preconizate, cu un punctaj social care conduce la una dintre următoarele situații sau la ambele:

(i)

tratamentul prejudiciabil sau nefavorabil aplicat anumitor persoane fizice sau unor grupuri de persoane în contexte sociale care nu au legătură cu contextele în care datele au fost generate sau colectate inițial;

(ii)

tratamentul prejudiciabil sau nefavorabil aplicat anumitor persoane fizice sau unor grupuri de persoane, care este nejustificat sau disproporționat în raport cu comportamentul social al acestora sau cu gravitatea acestuia;

(d) introducerea pe piață, punerea în funcțiune în acest scop specific sau utilizarea unui sistem de IA pentru efectuarea de evaluări ale riscurilor persoanelor fizice cu scopul de a evalua sau de a

prevedea riscul ca o persoană fizică să comită o infracțiune, exclusiv pe baza creării profilului unei persoane fizice sau pe baza evaluării trăsăturilor și caracteristicilor sale de personalitate; această interdicție nu se aplică sistemelor de IA utilizate pentru a sprijini evaluarea umană a implicării unei persoane într-o activitate infracțională, care se bazează deja pe fapte obiective și verificabile legate direct de o activitate infracțională;

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

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

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

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

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

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

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

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

Ca și precizare suplimentară, infracțiunile menționate în lit. h) a art. 5 din Regulament sunt cele prevăzute în Anexa a Regulamentului, respectiv:

- terorism;
- trafic de ființe umane;
- exploatare sexuală a copiilor și pornografie infantilă;

- trafic ilicit de stupefiante sau de substanțe psihotrope;
- trafic ilicit de arme, muniții sau substanțe explozive;
- omor, vătămare corporală gravă;
- trafic ilicit de organe sau țesuturi umane;
- trafic ilicit de materiale nucleare sau radioactive;
- răpire, lipsire de libertate în mod ilegal sau luare de ostatici;
- infracțiuni de competența Curții Penale Internaționale;
- sechestrare ilicită de aeronave sau de nave;
- viol;
- infracțiuni împotriva mediului;
- jaf organizat sau armat;
- sabotaj;
- participare la o organizație criminală implicată în una sau mai multe dintre infracțiunile enumerate mai sus.

Astfel cum rezultă din enumerarea infracțiunilor din Anexa 2 la Regulament, folosirea datelor biometrice nu este una întâmplătoare, utilizarea acestor date fiind permisă în cazul unor infracțiuni de o gravitate mare care trebuie să aibă o limită de pedeapsă, astfel cum se prevede în art. 5 lit. h) pct. iii), privativă de libertate sau o măsură de siguranță privativă de libertate pentru o perioadă de cel puțin 4 ani.

Totodată, în cazul în care sistemele de identificare biometrică la distanță sunt utilizate, conform art. 5 alin. (2) din Regulament, doar pentru confirmarea identității persoanei vizate în mod specific, cu luarea în considerare a următoarelor elemente: (a) natura situației care determină posibila utilizare, în special gravitatea, probabilitatea și amploarea prejudiciului care ar fi cauzat dacă sistemul nu ar fi utilizat; (b) consecințele utilizării sistemului asupra drepturilor și libertăților tuturor persoanelor vizate, în special gravitatea, probabilitatea și amploarea acestor consecințe.

Ca și condiții suplimentare pentru utilizarea sistemelor de identificare biometrică la distanță în timp real, se impune a preciza inclusiv reglementarea art. 5 alin. (3) din Regulament conform căreia utilizarea acestor sisteme se poate dispune dacă utilizarea face obiectul unei autorizații prealabile acordate de o autoritate judiciară sau de o autoritate administrativă independentă a cărei decizie are efect obligatoriu din statul membru în care urmează să aibă loc utilizarea; autorizația respectivă este emisă pe baza unei cereri motivate și în conformitate cu normele detaliate de drept intern menționate la alineatul (5). Cu toate acestea, într-o situație de urgență justificată în mod corespunzător, utilizarea sistemului poate începe fără autorizație, cu condiția ca autorizația respectivă să fie solicitată fără întârzieri nejustificate, cel târziu în termen de 24 de ore. În cazul în care o astfel de autorizație este refuzată, utilizarea sistemului este oprită cu efect

imediat și toate datele, precum și rezultatele și produsele obținute în cadrul utilizării respective sunt înlăturate și șterse imediat.

Altfel spus, utilizarea sistemelor de identificare biometrică la distanță trebuie să aibă în vedere procedura instituită de Regulament, la care vom face referire în cele ce urmează și doar în situații excepționale utilizarea sistemului de identificare va începe fără autorizație, cu condiția ca autorizarea să fie cerută în termen de cel mult 24 ore. Regulamentul prevede și consecința refuzului emiterii autorizației de utilizare a sistemelor de identificare biometrică, respectiv oprirea utilizării sistemului și înlăturarea și ștergerea tuturor datelor, rezultatelor sau a produselor obținute ca urmare a respectivei utilizări neautorizate.

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

În consecință, utilizarea sistemelor de identificare biometrică la distanță nu se va putea face fără o justificare și urmează a fi autorizată doar după finalizarea unei evaluări a impactului asupra drepturilor fundamentale, realizată în conformitate cu prevederile art. 27 din Regulament și în urma înregistrării în baza de date a UE conform art. 49 din Regulament. Astfel, din punctul nostru de vedere, art. 5 din Regulament, dincolo de posibilitatea dată autorităților de a utiliza sistemele de identificare biometrică la distanță, sunt de natură a insera și garanții puternice care să impună autorităților anumite obligații, în conformitate cu dispozițiile actului normativ european nou aprobat. Astfel cum rezultă din dispozițiile legale la care am făcut referire anterior, garantarea respectării drepturilor fundamentale este un deziderat la care Regulamentul face referire în nenumărate rânduri, semn că la nivelul UE problematica drepturilor fundamentale este una arzătoare, prin maniera de reglementare nefiind permise erori în accesarea acestor sisteme de identificare în orice condiții.

În vederea garantării drepturilor fundamentale și totodată pentru siguranța că aceste sisteme nu vor fi utilizate decât în scopul aplicării legii, astfel cum rezultă din prevederile aceluiași articol, art. 5 alin. (3) din Regulament stabilește așa cum precizam anterior necesitatea obținerii unei autorizații în mod prealabil accesării sistemului și numai în situații excepționale sistemul va putea fi accesat fără autorizare însă cu îndeplinirea cerințelor expuse anterior. Regulamentul stabilește în continuare faptul că autoritatea judiciară competentă sau o autoritate administrativă independentă a cărei decizie are efect obligatoriu acordă autorizația numai dacă este convinsă, pe baza unor dovezi obiective sau a unor indicii clare care i-au fost prezentate, că utilizarea sistemului de identificare biometrică la distanță în timp real în cauză este necesară și

proporțională pentru realizarea unuia dintre obiectivele menționate la alineatul (1) primul paragraf litera (h), astfel cum a fost identificat în cerere și, în special, rămâne limitată la ceea ce este strict necesar din punctul de vedere al perioadei de timp, precum și al sferei de aplicare geografică și personală. Atunci când ia o decizie cu privire la cerere, autoritatea respectivă ia în considerare elementele menționate la alineatul (2). Nicio decizie care produce un efect juridic negativ asupra unei persoane nu poate fi luată exclusiv pe baza unui rezultat al sistemului de identificare biometrică la distanță în timp real.

Deși utilizarea sistemelor de identificare biometrică la distanță sunt menite a veni în sprijinul autorităților din statele membre în vederea identificării persoanelor suspecte că ar fi săvârșit una din infracțiunile prevăzute în Anexa 2 la Regulament, totuși procedura instituită de art. 5 din Regulament prevede că fiecare utilizare a unui sistem de identificare biometrică la distanță în timp real în spațiile accesibile publicului în scopul aplicării legii va fi notificată autorității naționale pentru protecția datelor iar statul membru care autorizează utilizarea sistemelor va stabili în dreptul intern norme detaliate care vor fi necesare pentru solicitarea, eliberarea, exercitarea și totodată pentru supravegherea autorizațiilor pentru utilizarea sistemelor de identificare biometrică la distanță în timp real. Normele care se vor adopta la nivelul statelor membre vor include, de asemenea, care obiective prevăzute în art. 5 vor fi supuse autorizării și pentru care dintre infracțiunile prevăzute în art. 5, lit. h) pct. iii) autorizarea se va face în scopul aplicării legii. Statele membre au posibilitatea reglementării unor legi mai restrictive privind utilizarea sistemelor de identificare biometrică la distanță, tocmai în vederea oferirii unor garanții suplimentare.

Tot pentru asigurarea unei trasabilități în privința utilizării sistemelor de identificare biometrică la distanță în timp real, potrivit dispozițiilor art. 5 alin. (6) din Regulament, autoritățile naționale de supraveghere a pieței și autoritățile naționale de protecție a datelor din statele membre care au fost notificate cu privire la utilizarea sistemelor de identificare biometrică la distanță în timp real în spațiile accesibile publicului în scopul aplicării legii în temeiul alineatului (4) prezintă Comisiei rapoarte anuale cu privire la utilizarea respectivă. În acest scop, Comisia furnizează statelor membre și autorităților naționale de supraveghere a pieței și de protecție a datelor un model, inclusiv informații privind numărul deciziilor luate de autoritățile judiciare competente sau de o autoritate administrativă independentă a cărei decizie are efect obligatoriu, în ceea ce privește cererile de autorizare în conformitate cu alineatul (3), precum și rezultatul cererilor respective.

În modalitatea de reglementare se observă o reală preocupare față de garantarea utilizării sistemelor de IA doar în vederea aplicării legii. Dincolo de condițiile restrictive în care sistemele de identificare biometrică la distanță în timp real vor putea fi utilizate, se impune a menționa și obligațiile de raportare impuse de prevederile Regulamentului, obligații care asigură, din punctul nostru de vedere, o reală posibilitate de gestionare și control a accesării acestor sisteme de identificare la distanță doar pentru scopurile arătate în Regulament.

5.4. Sisteme de IA cu grad ridicat de risc

Regulamentul reglementează și acele sisteme de IA care prezintă un grad ridicat de risc, articolul 6 din Regulament stabilind normele de clasificare pentru aceste sisteme de IA.

Potrivit art. 6 alin. (1) din Regulament, sistemul de IA este considerat ca prezentând un grad ridicat de risc în cazul în care sunt îndeplinite cumulativ următoarele condiții: (a) sistemul de IA este destinat a fi utilizat ca o componentă de siguranță a unui produs sau sistemul de IA este el însuși un produs care face obiectul legislației de armonizare a Uniunii care figurează în anexa I; (b) produsul a cărui componentă de siguranță în temeiul literei (a) este sistemul de IA sau sistemul de IA în sine ca produs trebuie să fie supus unei evaluări a conformității de către o terță parte, în vederea introducerii pe piață sau a punerii în funcțiune a produsului respectiv în temeiul legislației de armonizare a Uniunii care figurează în anexa I.

Pe lângă aceste sisteme menționate în alin. (1) al art. 6 din Regulament, trebuie analizate și sistemele de IA enumerate în Anexa 3 la Regulament care, potrivit art. 6 alin. (2), sunt considerate ca reprezentând un grad ridicat de risc.

Pentru acuratețe, vom reda în cele ce urmează sistemele de IA cu grad ridicat de risc reglementate în Anexa 3 la Regulament. Drept urmare, Sistemele de IA cu grad ridicat de risc conform art. 6 alin. (2) sunt sistemele de IA care aparțin unuia dintre următoarele domenii:

1. Biometrie, în măsura în care utilizarea acesteia este permisă în temeiul dreptului Uniunii sau intern relevant:

(a) sisteme de identificare biometrică la distanță. Acestea nu includ sistemele de IA destinate a fi utilizate pentru verificarea biometrică al cărei unic scop este de a confirma că o anumită persoană fizică este persoana care susține că este;

(b) sisteme de IA destinate a fi utilizate pentru clasificarea biometrică, în funcție de atribute sau caracteristici sensibile ori protejate, pe baza deducerii acestor atribute sau caracteristici;

(c) sisteme de IA destinate a fi utilizate pentru recunoașterea emoțiilor.

2. Infrastructură critică: sisteme de IA destinate a fi utilizate drept componente de siguranță în gestionarea și exploatarea infrastructurii digitale critice, a traficului rutier sau a aprovizionării cu apă, gaz, încălzire ori energie electrică.

3. Educație și formare profesională:

(a) sisteme de IA destinate a fi utilizate pentru a stabili accesul ori admisia sau pentru a repartiza persoane fizice la instituțiile de învățământ și formare profesională la toate nivelurile;

(b) sisteme de IA destinate a fi utilizate pentru a evalua rezultatele învățării, inclusiv atunci când acestea sunt utilizate pentru a orienta procesul de învățare al persoanelor fizice în instituțiile de învățământ și formare profesională la toate nivelurile;

(c) sisteme de IA destinate a fi utilizate în scopul evaluării nivelului adecvat de educație pe care o persoană îl va primi sau îl va putea accesa, în contextul sau în cadrul instituțiilor de învățământ și formare profesională la toate nivelurile;

(d) sisteme de IA destinate a fi utilizate pentru monitorizarea și detectarea comportamentului interzis al elevilor și studenților în timpul testelor, în contextul sau în cadrul instituțiilor de educație și formare profesională la toate nivelurile.

4. Ocuparea forței de muncă, gestionarea lucrătorilor și accesul la activități independente:

- (a) sisteme de IA destinate a fi utilizate pentru recrutarea sau selectarea persoanelor fizice, în special pentru a plasa anunțuri de angajare direcționate în mod specific, pentru a analiza și a filtra candidaturile pentru locuri de muncă și pentru a evalua candidații;
- (b) sisteme de IA destinate a fi utilizate pentru a lua decizii care afectează termenii relațiilor legate de muncă, promovarea și încetarea relațiilor contractuale legate de muncă, pentru a alocă sarcini pe baza comportamentului individual sau a trăsăturilor ori caracteristicilor personale sau pentru a monitoriza și evalua performanța și comportamentul persoanelor aflate în astfel de relații.

5. Accesul la servicii private esențiale și la servicii și beneficii publice esențiale, precum și posibilitatea de a beneficia de acestea:

- (a) sisteme de IA destinate a fi utilizate de autoritățile publice sau în numele autorităților publice pentru a evalua eligibilitatea persoanelor fizice pentru prestații și servicii de asistență publică esențiale, inclusiv servicii de îngrijiri de sănătate, precum și pentru a acorda, a reduce, a revoca sau a recupera astfel de prestații și servicii;
- (b) sisteme de IA destinate a fi utilizate pentru a evalua bonitatea persoanelor fizice sau pentru a stabili punctajul lor de credit, cu excepția sistemelor de IA utilizate în scopul detectării fraudelor financiare;
- (c) sisteme de IA destinate a fi utilizate pentru evaluarea riscurilor și stabilirea prețurilor în ceea ce privește persoanele fizice în cazul asigurărilor de viață și de sănătate;
- (d) sisteme de IA destinate pentru a evalua și a clasifica apelurile de urgență efectuate de persoane fizice sau pentru a distribui ori pentru a stabili prioritatea în distribuirea serviciilor de primă intervenție de urgență, inclusiv de către poliție, pompieri și asistența medicală, precum și în cadrul sistemelor de triaj de urgență pentru pacienți.

6. Aplicarea legii, în măsura în care utilizarea lor este permisă în temeiul dreptului Uniunii sau intern relevant:

- (a) sisteme de IA destinate a fi utilizate de către sau în numele autorităților de aplicare a legii sau de către instituțiile, organele, oficiile ori agențiile Uniunii în sprijinul autorităților de aplicare a legii sau în numele acestora pentru a evalua riscul ca o persoană fizică să devină victima unor infracțiuni;
- (b) sisteme de IA destinate a fi utilizate de către sau în numele autorităților de aplicare a legii ca poligrafe sau instrumente similare sau de către instituțiile, organele, oficiile ori agențiile Uniunii în sprijinul autorităților de aplicare a legii;
- (c) sisteme de IA destinate a fi utilizate de către sau în numele autorităților de aplicare a legii sau de instituțiile, organele, oficiile ori agențiile Uniunii în sprijinul autorităților de aplicare a legii pentru a evalua fiabilitatea probelor în cursul investigării sau al urmăririi penale a infracțiunilor;
- (d) sisteme de IA destinate a fi utilizate de către autoritățile de aplicare a legii sau în numele acestora de către instituțiile, organele, oficiile sau agențiile Uniunii în sprijinul autorităților de aplicare a legii pentru evaluarea riscului ca o persoană fizică să comită infracțiuni sau să

recidiveze, nu doar pe baza creării de profiluri ale persoanelor fizice, astfel cum se menționează la articolul 3 alineatul (4) din Directiva (UE) 2016/680, sau pentru a evalua trăsături și caracteristici de personalitate ori comportamentul infracțional anterior al unor persoane fizice sau grupuri;

(e) sisteme de IA destinate a fi utilizate de către sau în numele autorităților de aplicare a legii sau de către instituțiile, organele, oficiile ori agențiile Uniunii în sprijinul autorităților de aplicare a legii pentru crearea de profiluri ale persoanelor fizice, astfel cum se menționează la articolul 3 alineatul (4) din Directiva (UE) 2016/680, în cursul depistării, investigării sau urmăririi penale a infracțiunilor.

7. Migrație, azil și gestionare a controlului la frontiere, în măsura în care utilizarea lor este permisă în temeiul dreptului Uniunii sau intern relevant:

(a) sisteme de IA destinate a fi utilizate de către sau în numele autorităților publice competente sau de către instituțiile, organele, oficiile ori agențiile Uniunii drept poligrafe sau instrumente similare;

(b) sisteme de IA destinate a fi utilizate de către sau în numele autorităților publice competente sau de către instituțiile, organele, oficiile ori agențiile Uniunii pentru evaluarea unui risc, inclusiv a unui risc de securitate, a unui risc de migrație ilegală sau a unui risc pentru sănătate din partea unei persoane fizice care intenționează să intre sau care a intrat pe teritoriul unui stat membru;

(c) sisteme de IA destinate a fi utilizate de către sau în numele autorităților publice competente sau de către instituțiile, organele, oficiile ori agențiile Uniunii pentru a asista autoritățile publice competente în examinarea cererilor de azil, de viză sau de permise de ședere și a plângerilor aferente în ceea ce privește eligibilitatea persoanelor fizice care solicită un statut, inclusiv în evaluările conexe ale fiabilității probelor;

(d) sisteme de IA destinate a fi utilizate de către sau în numele autorităților publice competente sau de către instituțiile, organele, oficiile sau agențiile Uniunii, în contextul migrației, azilului sau gestionării controlului la frontiere, în scopul detectării, recunoașterii sau identificării persoanelor fizice, cu excepția verificării documentelor de călătorie.

8. Administrarea justiției și procesele democratice:

(a) sisteme de IA destinate a fi utilizate de către sau în numele unei autorități judiciare pentru a asista o autoritate judiciară în cercetarea și interpretarea faptelor sau a legii, precum și în aplicarea legii la un set concret de fapte sau destinate a fi utilizate în mod similar în soluționarea alternativă a litigiilor;

(b) sisteme de IA destinate a fi utilizate pentru a influența rezultatul unei alegeri sau al unui referendum ori comportamentul de vot al persoanelor fizice în exercitarea votului lor la alegeri sau referendumuri. Acestea nu includ sistemele de IA la ale căror rezultate nu sunt expuse direct persoane fizice, cum ar fi instrumentele utilizate pentru organizarea, optimizarea sau structurarea campaniilor politice din punct de vedere administrativ sau logistic.

Cu toate că art. 6 alin. (2) stabilește că sistemele de IA menționate în Anexa 3 sunt considerate sisteme care prezintă risc ridicat, totuși art. 6 alin. (3) stabilește anumite excepții potrivit cărora sistemul de IA menționat în Anexa 3 la Regulament nu va fi considerat că prezintă un grad

ridicat de risc dacă nu prezintă un risc semnificativ de a prejudicia sănătatea, siguranța sau drepturile fundamentale ale persoanelor fizice, inclusiv prin faptul că nu influențează în mod semnificativ rezultatul procesului decizional. Aceste dispoziții derogatorii se aplică dacă una din următoarele condiții este îndeplinită:

- (a) sistemul de IA este destinat să îndeplinească o sarcină procedurală restrânsă;
- (b) sistemul de IA este destinat să îmbunătățească rezultatul unei activități umane finalizate anterior;
- (c) sistemul de IA este destinat să depisteze modelele decizionale sau abaterile de la modelele decizionale anterioare și nu este menit să înlocuiască sau să influențeze evaluarea umană finalizată anterior, fără o revizuire umană adecvată; sau
- (d) sistemul de IA este destinat să îndeplinească o sarcină pregătitoare pentru o evaluare relevantă în scopul cazurilor de utilizare enumerate în anexa III.

În pofida primului paragraf, un sistem de IA menționat în anexa III este întotdeauna considerat ca prezentând un grad ridicat de risc dacă creează profiluri ale persoanelor fizice, altfel spus în această ipoteză în care printr-un sistem de IA sunt create profiluri ale persoanelor fizice, nu mai este aplicabilă excepția prevăzută mai sus.

În privința sistemelor de IA care sunt prezumate, în baza prevederilor Regulamentului, furnizorii acestor sisteme care consideră că un sistem de IA enumerat în anexa 3 la Regulament nu prezintă un grad ridicat de risc, trebuie să documenteze evaluarea înainte ca sistemul respectiv să fie introdus pe piață sau pus în funcțiune. Totodată, potrivit art. 6 alin. (4) din Regulament, furnizorul este supus obligației de înregistrare prevăzute la art. 49 alin. (2) din același regulament. Dispozițiile art. 49 alin. (2) stabilesc faptul că înainte de a introduce pe piață sau de a pune în funcțiune un sistem de IA pentru care furnizorul a concluzionat că nu prezintă un grad ridicat de risc în conformitate cu articolul 6 alineatul (3), furnizorul respectiv sau, după caz, reprezentantul autorizat se înregistrează pe sine, alături de sistemul respectiv în baza de date a UE menționată la articolul 71.

Din punctul nostru de vedere, această obligație prealabilă a furnizorului este de natură a garanta că documentarea pe care o face în sensul arătării că sistemul de IA nu prezintă un grad ridicat de risc nu este una formală, iar furnizorul urmează să fie înregistrat, împreună cu sistemul, în baza de date a UE.

Dincolo de posibilitatea criticabilă a unui furnizor de a face o documentație care să excepteze sistemul de IA de la aplicabilitatea regulilor stabilite de Regulament în privința sistemelor care prezintă un grad ridicat de risc, totuși admitem că există posibilitatea ca un sistem de IA, deși este menționat în Anexa 3, totuși să nu prezinte un risc ridicat; în această situație, pentru ca în baza dreptului UE totuși să se țină evidența acestor excepții prevăzute de Regulament, se impune o obligație suplimentară de raportare prealabilă conform celor arătate anterior.

5.5. Aspecte privind problematica răspunderii pentru prejudiciile cauzate de sistemele de IA.

Ceea ce este deosebit de important în această reglementare, dincolo de aspectele discutabile precizate mai sus, este că atât furnizorul sistemului de IA cât și sistemul de IA vor fi înregistrați în

baza de date a UE, lucru care este pe deplin justificat în condițiile în care în literatura de specialitate s-a analizat problematica răspunderii pentru prejudiciile cauzate de IA²⁸, într-un articol de specialitate publicat anterior adoptării Regulamentului privind IA.

În acest articol s-a analizat, raportat la prevederile Codului civil român, ce formă a răspunderii ar putea fi incidentă în situația în care prejudiciul ar fi generat de un sistem de IA, precizându-se faptul că pentru stabilirea formei de răspundere ce urmează să fie aplicabilă în cazul în care un sistem de IA ar produce un prejudiciu, astfel încât trebuie analizate cu prioritate formele de răspundere civilă deja existente pentru a stabili în ce măsură cadrul legislativ actual este suficient de bine dezvoltat pentru a acoperi și această nouă formă de răspundere ce se dorește a fi reglementată.

În Codul civil român este reglementat ca izvor al obligațiilor civile și faptul juridic ilicit care, în condițiile reglementate de lege, poate da naștere răspunderii civile delictuale. Această formă a răspunderii civile devine incidentă ori de câte ori o persoană își încalcă îndatorirea de a respecta regulile de conduită pe care legea sau obiceiul locului le impune, aducând atingere, prin acțiunile sau inacțiunile sale, drepturilor sau intereselor legitime ale altor persoane. Art. 1349 alin. (3) C. civ. stabilește că „în cazurile anume prevăzute de lege, o persoană este obligată să repare prejudiciul cauzat de fapta altuia, de lucrurile ori animalele aflate sub paza sa, precum și de ruina edificiului”. Totodată, alin. (4) al aceluiași articol stabilește că „răspunderea pentru prejudiciile cauzate de produsele cu defecte se stabilește prin lege specială”.

Răspunderea civilă delictuală care se angajează pentru fapta altuia, pentru prejudiciile cauzate lucruri, pentru prejudiciile cauzate de animale sau pentru prejudiciile cauzate prin ruina edificiului are un caracter obiectiv, spre deosebire de răspunderea civilă delictuală pentru fapta proprie care presupune și analiza condiției vinovăției pentru angajarea răspunderii.

Pentru a stabili un punct de plecare în analiza conceptului de răspundere pentru prejudiciile cauzate de un sistem de IA, trebuie analizate formele de răspundere cu care se pot stabili similitudini. Răspunderea pentru prejudiciile cauzate de lucruri și răspunderea pentru produsele cu defecte sunt formele de răspundere civilă delictuală care ar putea contura regimul juridic al răspunderii pentru prejudiciile cauzate de IA. Încă de la acel moment autorii au resimțit necesitatea abordării acestui subiect, ținând seama preponderent de gradul de noutate al acestor sisteme de IA pe de o parte iar pe de altă parte ținând cont de faptul cauzării prejudiciului de către un sistem de IA pentru care cineva trebuie să fie răspunzător.

Într-o comunicare a Comisiei Europene²⁹, s-a reținut faptul că în Cartea albă privind IA din 19 februarie 2020³⁰, Comisia s-a angajat să promoveze adoptarea IA și să abordeze riscurile asociate cu unele dintre utilizările sale prin promovarea excelenței și a încrederii. În Raportul

²⁸ În acest sens, a se vedea Ispas Gabriel-Liviu, Ispas Petruța-Elena, *Răspunderea civilă pentru prejudiciile cauzate de Inteligența Artificială. Nevoia unei reglementări europene*, articol publicat în revista Curierul Judiciar nr. 2/2022, paginile 84-89

²⁹ COM(2022) 496 final, disponibilă la adresa web <https://eur-lex.europa.eu/legal-content/RO/TXT/HTML/?uri=CELEX:52022PC0496>.

³⁰ Cartea albă „Inteligența artificială – O abordare europeană axată pe excelență și încredere”, 19.2.2020, COM(2020) 65 final.

referitor la răspunderea privind IA³¹ care însoțește Cartea albă, Comisia a identificat provocările specifice pe care le prezintă IA pentru normele existente în materie de răspundere. În concluziile sale din 9 iunie 2020 privind conturarea viitorului digital al Europei, Consiliul a salutat consultarea privind propunerile de politică din Cartea albă privind IA și a invitat Comisia să prezinte propuneri concrete. La 20 octombrie 2020, Parlamentul European a adoptat o rezoluție legislativă din proprie inițiativă în temeiul articolului 225 din TFUE, solicitând Comisiei să adopte o propunere privind un regim de răspundere civilă pentru IA în temeiul articolului 114 din Tratatul privind funcționarea Uniunii Europene (TFUE)³².

Normele naționale actuale în materie de răspundere, în special cele bazate pe culpă, nu sunt adecvate pentru soluționarea acțiunilor în răspundere pentru prejudiciile cauzate de produsele și serviciile bazate pe IA. În temeiul acestor norme, victimele trebuie să dovedească o faptă ilicită sau o omisiune din partea unei persoane care a cauzat prejudiciul. Caracteristicile specifice ale IA, inclusiv complexitatea, autonomia și opacitatea (așa-numitul efect al „cutiei negre”) fac ca identificarea persoanei responsabile și furnizarea de elemente de probă pentru îndeplinirea cerințelor pentru soluționarea cu succes a acțiunii în răspundere să fie dificile sau excesiv de costisitoare pentru victime. În special, atunci când solicită despăgubiri, victimele ar putea suporta costuri inițiale foarte ridicate și s-ar putea confrunta cu proceduri judiciare cu o durată semnificativ mai lungă, în comparație cu cauzele care nu implică IA. Prin urmare, victimele ar putea să fie descurajate să mai solicite despăgubiri. Aceste preocupări au fost, de asemenea, subliniate de Parlamentul European (PE) în rezoluția sa din 3 mai 2022 referitoare la inteligența artificială în era digitală³³.

În cazul în care o victimă introduce o acțiune, instanțele naționale, confruntate cu caracteristicile specifice ale IA, pot adapta modul în care aplică normele existente în mod ad-hoc pentru a ajunge la un rezultat just pentru victimă. Acest lucru va genera insecuritate juridică. Întreprinderile vor întâmpina dificultăți în a prevedea modul în care vor fi aplicate normele existente în materie de răspundere și, astfel, în a evalua și a asigura expunerea lor la riscul de răspundere. Efectul va fi amplificat pentru întreprinderile care desfășoară activități comerciale transfrontaliere, deoarece incertitudinea va acoperi diferite jurisdicții. Aceasta va afecta în special întreprinderile mici și mijlocii (IMM-urile), care nu se pot baza pe expertiza juridică internă sau pe rezerve de capital.

Strategiile naționale privind IA arată că mai multe state membre au în vedere sau chiar planifică în mod concret acțiuni legislative privind răspunderea civilă pentru IA. Prin urmare, se preconizează că, dacă UE nu va lua măsuri, statele membre își vor adapta normele naționale în materie de răspundere la provocările prezentate de IA. Acest lucru va duce la o fragmentare și

³¹ Raportul Comisiei către Parlamentul European, Consiliu și Comitetul Economic și Social European privind implicațiile în materie de siguranță și răspundere ale inteligenței artificiale, ale internetului obiectelor și ale roboticii, 19.2.2020, COM(2020) 64 final.

³² Rezoluția Parlamentului European din 20 octombrie 2020 conținând recomandări adresate Comisiei privind regimul de răspundere civilă pentru inteligența artificială (2020/2014(INL)).

³³ Rezoluția Parlamentului European din 3 mai 2022 referitoare la inteligența artificială în era digitală (2020/2266(INI)).

mai mare și la o creștere a costurilor pentru întreprinderile care își desfășoară activitatea pe întregul teritoriu al UE.

În contextul analizat, este deosebit de importantă abordarea răspunderii pentru prejudiciile generate de sisteme de IA și deși din punctul nostru de vedere, un regulament ar fi fost o variantă legislativă mai bună deoarece s-ar fi asigurat un cadru al răspunderii uniform, totuși în comunicarea Comisiei s-a precizat faptul că o directivă este instrumentul cel mai adecvat pentru prezenta propunere, deoarece asigură efectul de armonizare și securitatea juridică dorite, oferind în același timp flexibilitatea necesară pentru a permite statelor membre să integreze măsurile armonizate fără obstacole în regimurile lor naționale de răspundere.

Un instrument obligatoriu ar preveni lacunele în materie de protecție care decurg din punerea în aplicare parțială sau inexistentă. Deși un instrument fără caracter obligatoriu ar fi mai puțin invaziv, este puțin probabil ca acesta să abordeze problemele identificate în mod eficace. Rata de punere în aplicare a instrumentelor fără caracter obligatoriu este dificil de prevăzut și nu există suficiente indicii că efectul de persuasiune al unei recomandări ar fi suficient de puternic pentru a produce o adaptare coerentă a legislațiilor naționale.

Acest efect este și mai puțin probabil în cazul măsurilor de drept privat, din care fac parte normele în materie de răspundere extracontractuală. Acest domeniu este caracterizat de tradiții juridice de lungă durată, ceea ce face ca statele membre să fie reticente în a urmări o reformă coordonată, cu excepția cazului în care aceasta este determinată de perspectiva clară a beneficiilor pentru piața internă în cadrul unui instrument obligatoriu al UE sau de necesitatea de a se adapta la noile tehnologii din economia digitală.

Divergențele semnificative existente între cadrele de răspundere ale statelor membre reprezintă un alt motiv pentru care este puțin probabil ca o recomandare să fie pusă în aplicare în mod coerent.

În conformitate cu politica sa privind o mai bună legiferare, Comisia a efectuat o evaluare a impactului pentru propunerea la care am făcut referire anterior, propunere care a fost examinată de Comitetul de control normativ al Comisiei. Reuniunea Comitetului de control normativ din 6 aprilie 2022 a condus la un aviz pozitiv cu observații.

Au fost evaluate trei opțiuni de politică:

Opțiunea de politică 1: trei măsuri pentru a reduce sarcina probei pentru victimele care încearcă să își susțină cu dovezi cererea de despăgubire.

Opțiunea de politică 2: măsurile din cadrul opțiunii 1 + armonizarea normelor în materie de răspundere obiectivă pentru cazurile de utilizare a IA cu un anumit profil de risc, împreună cu o asigurare obligatorie.

Opțiunea de politică 3: o abordare etapizată constând în: o primă etapă: măsurile din cadrul opțiunii 1; o a doua etapă: un mecanism de revizuire pentru a reevalua, în special, necesitatea armonizării răspunderii obiective pentru cazurile de utilizare a IA cu un anumit profil de risc (eventual însoțită de o asigurare obligatorie).

Aceste opțiuni au fost comparate de către Comisie prin intermediul unei analize bazate pe criterii multiple, ținând seama de eficacitatea, eficiența, coerența și proporționalitatea acestora.

Rezultatele analizei bazate pe criterii multiple și a sensibilității arată că opțiunea de politică 3, care reduce sarcina probei pentru cererile de despăgubire legate de IA plus revizuirea specifică în ceea ce privește răspunderea obiectivă, eventual combinată cu asigurarea obligatorie, se situează pe primul loc și, prin urmare, este opțiunea de politică preferată pentru prezenta propunere.

Opțiunea de politică preferată ar asigura faptul că victimele produselor și serviciilor bazate pe IA (persoane fizice, întreprinderi și alte entități publice sau private) sunt protejate în aceeași măsură ca și victimele tehnologiilor tradiționale. Aceasta ar spori nivelul de încredere în IA și ar promova adoptarea acesteia.

În plus, ar reduce incertitudinea juridică și ar preveni fragmentarea, ajutând astfel întreprinderile, și mai ales IMM-urile, care doresc să valorifice întregul potențial al pieței unice a UE prin introducerea produselor și serviciilor bazate pe IA la nivel transfrontalier. Opțiunea de politică preferată creează, de asemenea, condiții mai bune pentru ca asigurătorii să ofere acoperire activităților legate de IA, ceea ce este esențial pentru gestionarea riscurilor de către întreprinderi, în special IMM-uri. Și anume, se estimează că opțiunea de politică preferată ar genera o creștere a valorii de piață a IA în UE-27 între aproximativ 500 de milioane EUR și aproximativ 1,1 miliarde EUR în 2025.

Comisia nu a neglijat în comunicarea sa nici problema drepturilor fundamentale, aceasta arătând că intenția sa este să se asigure că victimele prejudiciilor cauzate de IA beneficiază de un nivel de protecție echivalent în temeiul normelor în materie de răspundere civilă cu cel al victimelor prejudiciilor cauzate fără implicarea IA. Propunerea va permite asigurarea efectivă la nivel privat a respectării drepturilor fundamentale și va menține dreptul la o cale de atac eficientă în cazul în care riscurile specifice IA s-au materializat. În special, propunerea va contribui la protejarea drepturilor fundamentale, cum ar fi dreptul la viață (articolul 2 din cartă), dreptul la integritate fizică și psihică (articolul 3) și dreptul de proprietate (articolul 17). În plus, în funcție de tradițiile și de sistemul de drept civil ale fiecărui stat membru, victimele vor putea solicita despăgubiri pentru prejudiciile aduse altor interese juridice, cum ar fi încălcarea demnității personale (articolele 1 și 4 din cartă), respectarea vieții private și de familie (articolul 7), dreptul la egalitate (articolul 20) și nediscriminarea (articolul 21).

În plus, prezenta propunere completează alte componente ale politicii Comisiei privind IA, bazate pe cerințe preventive de reglementare și de supraveghere care vizează în mod direct evitarea încălcărilor drepturilor fundamentale (cum ar fi discriminarea). Acestea sunt Legea privind IA, Regulamentul general privind protecția datelor, Actul legislativ privind serviciile digitale și legislația UE privind nediscriminarea și egalitatea de tratament. În același timp, prezenta propunere nu creează și nu armonizează obligațiile de diligență sau răspunderea diferitelor entități a căror activitate este reglementată de actele juridice respective și, prin urmare, nu creează noi acțiuni în răspundere și nu afectează exonerările de răspundere în temeiul acestor alte acte juridice. S-a intenționat, prin comunicarea Comisiei, să se aducă reduceri ale sarcinii probei pentru victimele prejudiciilor cauzate de sistemele de IA în cadrul cererilor care se pot baza pe dreptul intern sau pe aceste alte acte legislative ale UE. Prin completarea acestor alte componente, prezenta propunere protejează dreptul victimei la despăgubiri în temeiul dreptului privat, inclusiv la despăgubiri pentru încălcări ale drepturilor fundamentale.

Astfel cum rezultă din comunicarea Comisiei europene, se intenționează adoptarea unui pachet legislativ coerent, directiva împreună cu Regulamentul privind IA fiind de natură să contureze un

cadru legislativ complex care să asigure inclusiv modalitatea de reparare a prejudiciilor cauzate de sistemele de IA. Cu toate că Regulamentul stabilește în mod neechivoc care sunt acele practici interzise în domeniul IA, nu se poate exclude în mod absolut că practicile nu vor fi totuși folosite, cu consecința creării unor prejudicii. În aceste condiții, la nivelul UE și la nivelul fiecărui stat membru trebuie să existe instrumente juridice care să dea încredere în sistemele de IA iar această încredere poate lua naștere inclusiv prin legiferarea unei forme de răspundere clară, neechivocă, ce nu împovărează victima unui prejudiciu cu o probațiune imposibil de îndeplinit.

Astfel cum s-a reținut în expunerea de motive a propunerii de directivă, aceasta abordează obstacolele care decurg din faptul că întreprinderile care doresc să producă, să disemineze și să exploateze produse și servicii bazate pe IA la nivel transfrontalier nu știu dacă și în ce mod se aplică regimurile de răspundere existente în cazul prejudiciilor cauzate de IA. Această incertitudine se referă în special la statele membre în care întreprinderile vor exporta sau își vor exploata produsele și serviciile. Într-un context transfrontalier, legea aplicabilă răspunderii extracontractuale care decurge dintr-o faptă ilicită este, în mod implicit, legea țării în care s-a produs prejudiciul. Pentru aceste întreprinderi, este esențial să cunoască riscurile relevante în materie de răspundere și să poată încheia asigurări împotriva acestora. În consecință, ia naștere și preocuparea pentru domeniul asigurărilor în acest domeniu complex, un alt semnal că sistemele de IA sunt analizate din toate punctele de vedere tocmai în vederea garantării că implementarea acestora va oferi un nivel de siguranță optim iar în cazul în care se cauzează prejudicii prin aceste sisteme, să existe posibilitatea pentru victimă de a se îndrepta fie împotriva persoanei care gestionează sistemul, fie împotriva asigurătorului acestui sistem.

Propunerea de directivă urmează a fi analizată într-un alt capitol aferent prezentei lucrări, la acest moment fiind analizată doar succint această problemă prin raportare la sistemele de IA care prezintă un grad ridicat de risc și implicit pot cauza prejudicii.

5.6. Posibilitatea modificării anexei 3 de către Comisie

Anexa 3 la Regulament, redată anterior, care cuprinde enumerarea sistemelor de IA care prezintă un grad ridicat de risc va putea fi revizuită de Comisie, aceasta fiind imputernicită prin art. 7 din Regulament, fie prin adăugarea unor cazuri de utilizare a sistemelor de IA cu grad ridicat de risc, fie prin modificarea unor cazuri de utilizare a sistemelor de IA, dacă sunt îndeplinite în mod cumulativ următoarele condiții:

- (a) sistemele de IA sunt destinate a fi utilizate în oricare dintre domeniile enumerate în anexa III;
- (b) sistemele de IA prezintă un risc de a aduce prejudicii sănătății și siguranței sau un risc de impact negativ asupra drepturilor fundamentale, iar riscul respectiv este echivalent sau mai mare în raport cu riscul de a aduce prejudicii sau de a provoca un impact negativ prezentat de sistemele de IA cu grad ridicat de risc deja menționate în anexa III.

Pentru evaluarea condiției prevăzute la lit. b), Comisia va analiza și va lua în considerare criteriile enumerate în art. 7, respectiv:

- (a) scopul preconizat al sistemului de IA;
- (b) măsura în care a fost utilizat sau este probabil să fie utilizat un sistem de IA;

(c) natura și volumul datelor prelucrate și utilizate de sistemul de IA, în special dacă sunt prelucrate categorii speciale de date cu caracter personal;

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

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

(f) amploarea potențială a unor astfel de prejudicii sau a unui astfel de impact negativ, în special în ceea ce privește intensitatea și capacitatea sa de a afecta numeroase persoane sau de a afecta în mod disproporționat un anumit grup de persoane;

(g) măsura în care persoanele care sunt potențial prejudiciate sau afectate de un impact negativ depind de rezultatul produs cu ajutorul unui sistem de IA, în special deoarece, din motive practice sau juridice, nu este posibil în mod rezonabil să se renunțe la rezultatul respectiv;

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

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

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

(k) măsura în care dreptul existent al Uniunii prevede:

(i) măsuri reparatorii eficace în legătură cu riscurile prezentate de un sistem de IA, cu excepția cererilor de despăgubiri;

(ii) măsuri eficace de prevenire sau de reducere substanțială a acestor riscuri.

Comisia are, totodată, și prerogativa de a adopta acte în vederea modificării listei din anexa 3 prin eliminarea sistemelor de IA cu grad ridicat de risc în situația în care sunt îndeplinite în mod cumulativ două condiții enumerate de art. 7 alin. (3) din Regulament, respectiv:

(a) sistemul de IA cu grad ridicat de risc în cauză nu mai prezintă riscuri semnificative pentru drepturile fundamentale, sănătate sau siguranță, ținând seama de criteriile enumerate la alineatul (2);

(b) eliminarea nu reduce nivelul general de protecție a sănătății, siguranței și drepturilor fundamentale în temeiul dreptului Uniunii.

Din punctul nostru se vede, Comisia va decide, pe baza analizei realizate în conformitate cu prevederile art. 7 din Regulament dacă sistemele de IA reglementate în anexa 3 ca fiind sisteme cu grad ridicat de risc prezintă într-adevăr caracteristicile cerute de Regulament pentru a avea acest caracter. În cazul în care Comisia, pe baza unor analize care considerăm că vor fi temeinic analizate și justificate, va constata că totuși fie anexa 3 trebuie modificată, fie că anumite sisteme de IA nu prezintă grad ridicat de risc și va aprecia că se impune eliminarea acestora din cuprinsul Anexei 3 la Regulament, este împuternicită, în baza dispozițiilor legale anterior citate, să procedeze la adoptarea actelor delegate în conformitate cu art. 97 în vederea modificării listei sistemelor de IA din anexa 3, în oricare dintre modalitățile prevăzute de art. 7 din Regulament.

5.7. Sistemele de IA cu grad ridicat de risc. Cerințe și sistem de gestionare a riscurilor

Astfel cum am analizat anterior, prevederile Regulamentului sunt întemeiate pe un sistem de gestionare a riscurilor care ar putea fi generate de utilizarea sistemelor de IA, art. 8 din Regulament stabilind că sistemele de IA care prezintă un grad ridicat de risc trebuie să respecte cerințele stabilite în secțiunea 2 din Regulament, cu luarea în considerare a scopului preconizat al acestor sisteme și a stadiului de avansare recunoscut IA și tehnologiilor conexe IA.

În privința sistemului de gestionare a riscurilor, potrivit art. 9 din Regulament, ca efect al acestui act normativ european, este instituit, pus în aplicare, documentat și menținut un sistem de gestionare a riscurilor în legătură sistemele de IA cu grad ridicat de risc.

Sistemul de gestionare a riscurilor reprezintă acel proces iterativ continuu planificat și derulat pe parcursul întregului ciclu de viață al unui sistem de IA cu grad ridicat de risc, care necesită periodic actualizarea și revizuirea sistematică și care conține următoarele etape prevăzute de art. 9 alin. (2) din Regulament:

- (a) identificarea și analiza riscurilor cunoscute și previzibile în mod rezonabil pe care sistemul de IA cu grad ridicat de risc le poate prezenta pentru sănătate, siguranță sau drepturile fundamentale atunci când sistemul de IA cu grad ridicat de risc este utilizat în conformitate cu scopul preconizat;
- (b) estimarea și evaluarea riscurilor care pot apărea atunci când sistemul de IA cu grad ridicat de risc este utilizat în conformitate cu scopul său preconizat și în condiții de utilizare necorespunzătoare previzibilă în mod rezonabil;
- (c) evaluarea altor riscuri care ar putea apărea pe baza analizei datelor colectate din sistemul de monitorizare ulterioară introducerii pe piață menționat la articolul 72;
- (d) adoptarea unor măsuri adecvate și specifice de gestionare a riscurilor, concepute pentru a combate riscurile identificate în temeiul literei (a).

Art. 9 din Regulament se referă exclusiv la acele riscuri care pot fi atenuate sau eliminate în mod rezonabil prin dezvoltarea sau proiectarea sistemului de IA cu grad ridicat de risc sau prin furnizarea de informații tehnice adecvate.

În vederea identificării celor mai adecvate măsuri de gestionare a riscurilor urmează a se asigura îndeplinirea unor cerințe, după cum urmează:

(a) eliminarea sau reducerea riscurilor identificate și evaluate în temeiul alineatului (2), în măsura în care acest lucru este fezabil din punct de vedere tehnic prin proiectarea și dezvoltarea adecvată a sistemului de IA cu grad ridicat de risc;

(b) după caz, punerea în aplicare a unor măsuri adecvate de atenuare și control pentru combaterea riscurilor care nu pot fi eliminate;

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

Art. 9 alin. (5) paragraful final din Regulament stabilește că pentru eliminarea sau reducerea riscurilor legate de utilizarea sistemelor de IA cu grad ridicat de risc se acordă o atenție sporită cunoștințelor tehnice, experienței, educației și formării preconizate din partea implementatorului, precum și contextului prezumtiv în care urmează să fie utilizat sistemul.

În vederea determinării riscurilor asociate care pot fi generate ca urmare a utilizării unor sisteme de IA, este necesară testarea în scopul identificării celor mai adecvate măsuri de gestionare a riscurilor, testarea urmând a fi realizată în condiții reale, în conformitate cu prevederile Regulamentului, pentru a se asigura că sistemele de IA cu grad ridicat de risc funcționează în mod coerent cu scopul preconizat și că acestea sunt conforme cu cerințele stabilite în Regulament referitoare la gestionarea riscurilor.

O prevedere importantă a Regulamentului este conținută în art. 9 alin. (8), această dispoziție stabilește că testarea se realizează în orice moment pe parcursul procesului de dezvoltare dar în toate cazurile înainte de introducerea pe piață sau înainte de punerea în funcțiune a acestora. Testarea se va efectua, conform prevederilor Regulamentului, pe baza unor indicatori și a unor praguri de probabilitate definite în prealabil, conforme cu scopul preconizat al sistemului de IA cu grad ridicat de risc.

5.8. Datele și guvernanta datelor

În privința sistemelor de IA cu grad ridicat de risc care utilizează tehnici care implică antrenarea unor modele de IA cu date, potrivit art. 10 din Regulament, acestea se dezvoltă pe baza unor seturi de date de antrenament, de validare și de testare care îndeplinesc criteriile de calitate la care ne vom referi în cele ce urmează și care sunt enumerate de art. 10 alin. (2)-(5) din Regulament.

Seturile de date de antrenament, de validare și de testare pe baza cărora se testează sistemele de IA cu grad ridicat de risc fac obiectul unor practici de guvernanta și de gestionare a datelor adecvate scopului preconizat al sistemului de IA cu grad ridicat de risc, aceste practici referindu-se în special la următoarele aspecte:

(a) opțiunile de proiectare relevante;

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

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

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

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

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

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

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

Seturile de date de antrenament, validare și testare trebuie să prezinte relevanță pentru sistemul de IA cu grad ridicat de risc, să fie reprezentative, fără erori și complete, conforme cu scopul preconizat. În categoria proprietăților statistice corespunzătoare se regăsesc în art. 10 alin. (3) din Regulament referiri inclusiv la persoanele sau grupurile de persoane în legătură cu care se intenționează să se utilizeze sistemul de IA cu grad ridicat de risc, iar caracteristicile seturilor de date se pot îndeplini la nivelul unor seturi de date individuale sau la nivelul unor combinații a acestora.

Potrivit art. 10 alin. (4) din Regulament, seturile de date se vor lua în considerare în funcție de scopul preconizat, caracteristicile sau elementele specifice, cadrul geografic, contextual, comportamental sau funcțional specific în care sistemul de IA cu grad ridicat de risc va fi utilizat.

Prelucrarea datelor cu caracter personal va putea fi realizată de furnizorii de sisteme de IA în mod excepțional, sub rezerva unor garanții adecvate pentru drepturile și libertățile fundamentale ale persoanelor fizice, fiind necesar ca în mod suplimentar față de Regulamentele (UE) 2016/679 și (UE) 2018/1725 și de Directiva (UE) 2016/680, pentru ca o astfel de prelucrare să aibă loc, trebuie să fie respectate în mod cumulativ următoarele condiții:

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

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

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

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

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

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

În consecință, deși se permite ca în mod excepțional și pentru respectarea prevederilor Regulamentului, furnizorii sistemelor de IA cu grad ridicat de risc să poată prelucra date cu caracter personal sensibile, este necesar a se asigura că drepturile fundamentale ale persoanelor fizice sunt apărute în mod corespunzător iar o asemenea prelucrare nu este de natură a aduce atingere drepturilor și libertăților fundamentale ale persoanelor fizice.

Încă o dată, prevederile Regulamentului tind spre a institui o protecție sporită în privința persoanelor fizice care ar putea suferi prejudicii ca urmare a utilizării sistemelor de IA cu grad ridicat de risc, aspect care ne conduce din nou spre ideea răspunderii pentru prejudiciile cauzate de aceste sisteme. Nu trebuie neglijat faptul că utilizarea sistemelor de IA în justiție poate fi de natură a prejudicia aceste drepturi și libertăți care sunt strâns legate de protecția datelor cu caracter personal. Trebuie avut în vedere că instanțele de judecată sunt operatori de date cu caracter personal, astfel încât implementarea și utilizarea acestor sisteme în justiție trebuie corelată cu măsurile de protecție instituite prin Regulament, tocmai pentru a se evita prejudicierea persoanelor fizice beneficiare ale acestor dispoziții legale.

5.9. Transparența

Art. 13 din Regulament stabilește regulile de transparență și furnizarea de informații implementatorilor.

Astfel cum precizam și anterior, întreaga reglementare adoptată prin Regulament are ca principal obiectiv asigurarea unui nivel ridicat al utilizării sistemelor de IA, siguranța implicând și transparența, în condițiile art. 13 din Regulament.

Potrivit acestui articol, în privința sistemelor de IA cu grad ridicat de risc trebuie urmărit ca proiectarea și dezvoltarea acestor sisteme să se facă astfel încât să se asigure că funcționarea lor este suficient de transparentă, astfel încât să se asigure implementatorilor interpretarea rezultatelor sistemului și utilizarea acestuia într-un mod corespunzător. Se reiterează asigurarea unui grad adecvat de transparență, pentru a se asigura respectarea obligațiilor relevante ale furnizorului și ale implementatorului sistemului de IA cu grad ridicat de risc.

Sistemele de IA cu grad ridicat de risc sunt însoțite de instrucțiuni de utilizare care conțin informații concise, complete, corecte și clare, informații care sunt relevante, accesibile și ușor de înțeles pentru implementatori, instrucțiunile urmând să conțină cel puțin următoarele informații enumerate în art. 13 alin. (3) din Regulament:

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

(b) caracteristicile, capacitățile și limitările performanței sistemului de IA cu grad ridicat de risc, inclusiv: (i) scopul său preconizat; (ii) nivelul de acuratețe, inclusiv indicatorii săi, de robustețe și de securitate cibernetică menționat la articolul 15 în raport cu care sistemul de IA cu grad ridicat de risc a fost testat și validat și care poate fi preconizat, precum și orice circumstanță cunoscută și previzibilă care ar putea avea un impact asupra nivelului preconizat de acuratețe, robustețe și securitate cibernetică; (iii) orice circumstanță cunoscută sau previzibilă legată de utilizarea sistemului de IA cu grad ridicat de risc în conformitate cu scopul său preconizat sau în condiții de utilizare necorespunzătoare previzibilă în mod rezonabil, care poate conduce la riscurile pentru sănătate și siguranță sau pentru drepturile fundamentale menționate la articolul 9 alineatul (2); (iv) după caz, capacitățile și caracteristicile tehnice ale sistemului de IA cu grad ridicat de risc de a furniza informații relevante pentru explicarea rezultatelor sale; (v) după caz, performanțele sale în ceea ce privește anumite persoane sau grupuri de persoane în legătură cu care este destinat să fie utilizat sistemul; (vi) după caz, specificațiile pentru datele de intrare sau orice altă informație relevantă în ceea ce privește seturile de date de antrenament, de validare și de testare utilizate, ținând seama de scopul preconizat al sistemului de IA cu grad ridicat de risc; (vii) după caz, informații care să le permită implementatorilor să interpreteze rezultatele sistemului de IA cu grad ridicat de risc și să le utilizeze în mod corespunzător;

(c) modificările aduse sistemului de IA cu grad ridicat de risc și performanței acestuia care au fost predeterminate de către furnizor la momentul evaluării inițiale a conformității, dacă este cazul;

(d) măsurile de supraveghere umană menționate la articolul 14, inclusiv măsurile tehnice instituite pentru a facilita interpretarea rezultatelor sistemelor de IA cu grad ridicat de risc de către implementatori;

(e) resursele de calcul și resursele hardware necesare, durata de viață preconizată a sistemului de IA cu grad ridicat de risc și orice măsuri de întreținere și de îngrijire, inclusiv frecvența lor, necesare pentru a asigura funcționarea corespunzătoare a sistemului de IA respectiv, inclusiv în ceea ce privește actualizările software-ului;

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

5.10. Obligațiile furnizorilor de sisteme de IA

În vederea îndeplinirii cerințelor de siguranță și transparență, dar și pentru a asigura garantarea drepturilor și libertățile fundamentale, Regulamentul introduce anumite obligații stabilite în sarcina furnizorilor de sisteme de IA cu grad ridicat de risc, aceștia urmând a respecta următoarele cerințe:

(a) se asigură că sistemele lor de IA cu grad ridicat de risc respectă cerințele prevăzute în secțiunea 2;

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

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

- (d) păstrează documentația menționată la articolul 18;
- (e) atunci când acestea se află sub controlul lor, păstrează fișierele de jurnalizare generate automat de sistemele lor de IA cu grad ridicat de risc menționate la articolul 19;
- (f) se asigură că sistemul de IA cu grad ridicat de risc este supus procedurii relevante de evaluare a conformității menționată la articolul 43, înainte de introducerea sa pe piață sau de punerea sa în funcțiune;
- (g) elaborează o declarație de conformitate UE în conformitate cu articolul 47;
- (h) aplică marcajul CE pe sistemul de IA cu grad ridicat de risc sau, în cazul în care acest lucru nu este posibil, pe ambalajul sau în documentația sa însoțitoare, pentru a indica conformitatea cu prezentul regulament, în conformitate cu articolul 48;
- (i) respectă obligațiile de înregistrare menționate la articolul 49 alineatul (1);
- (j) iau măsurile corective necesare și furnizează informațiile prevăzute la articolul 20;
- (k) la cererea motivată a unei autorități naționale competente, demonstrează conformitatea sistemului de IA cu grad ridicat de risc cu cerințele prevăzute în secțiunea 2;
- (l) se asigură că sistemul de IA cu grad ridicat de risc respectă cerințele de accesibilitate, în conformitate cu Directivele (UE) 2016/2102 și (UE) 2019/882.

După cum reiese din prevederile Regulamentului anterior citate, este evidentă preocuparea la nivelul UE de a stabili o trasabilitate a sistemului de IA, de a se asigura de conformitatea sistemelor de IA cu grad ridicat de risc cu cerințele existente la nivelul UE, de existența marcajului CE, de a respecta obligațiile de înregistrare prevăzute de Regulament, de a demonstra conformitatea sistemului de IA cu grad ridicat de risc cu cerințele prevăzute în secțiunea 2 din același Regulament.

În consecință, din punctul nostru de vedere, corolarul în jurul căruia a fost construit Regulamentul urmează a se bucura de o corectă aplicare deoarece acesta este bazat pe protecția drepturilor fundamentale, pe un sistem bazat pe o siguranță și o trasabilitate sporită care este de natură să crească încrederea persoanelor în utilizarea sistemelor de IA chiar dacă acestea prezintă un grad ridicat de risc. Toate măsurile stabilite în Regulament sunt, din punctul nostru de vedere, menite să introducă aspectul de noutate al sistemelor de IA la un nivel de siguranță cu care cetățenii europeni sunt deja obișnuiți, astfel încât noutatea se îmbină în mod armonios cu clasicele drepturi fundamentale, de la care Regulamentul nu face rabat.

5.11. Obligațiile distribuitorilor de sisteme de IA

Pe lângă furnizorii sistemelor de IA cu grad ridicat de risc, este deosebit de important de importantă și stabilirea unor obligații în sarcina distribuitorilor de sisteme de IA cu grad ridicat de risc. Regulamentul a dedicat art. 24 acestor obligații, obligații care trebuie îndeplinite înainte de a pune la dispoziție pe piață un astfel de sistem de IA.

Astfel, înainte de introducerea pe piață a unui sistem de IA distribuitorul verifică dacă sistemul poartă marcajul CE necesar, dacă este însoțit de o copie a declarației de conformitate UE și de

instrucțiunile de utilizare. Totodată, distribuitorul este obligat să verifice dacă furnizorul și importatorul sistemului respectiv au respectat obligațiile prevăzute în sarcina lor în Regulament.

În eventualitatea în care distribuitorul apreciază că nu sunt îndeplinite cerințele din secțiunea 2 cu privire la sistemul de IA cu grad ridicat de risc, acesta nu va pune pe piață sistemul respectiv înainte ca acesta să fie adus în conformitate cu cerințele respective. În cazul sistemelor de IA prezintă un risc în sensul art. 79 alin. (1) din Regulament, respectiv acele sisteme care prezintă riscuri pentru sănătatea, siguranța sau pentru drepturile fundamentale ale persoanelor, distribuitorii au obligația să informeze furnizorul sau implementatorul sistemului în acest sens.

O altă obligație stabilită în sarcina distribuitorilor se referă la condițiile pe care sistemul de IA aflat în responsabilitatea lor trebuie să le îndeplinească, urmând ca distribuitorul să se asigure pe toată această perioadă de timp condițiile de depozitare sau transport nu periclitizează conformitatea sistemului cu cerințele prevăzute în secțiunea 2 din Regulament.

În cazul în care un distribuitor al unui sistem de IA cu grad ridicat de risc consideră sau are motive suficiente să aprecieze, pe baza informațiilor pe care le are, că un sistem de IA cu grad ridicat de risc pe care l-a introdus pe piață nu este conform cu secțiunea 2 din Regulament, trebuie să ia toate măsurile de corecție necesare pentru a asigura conformitatea sistemului cu prevederile și cerințele Regulamentului, pentru a retrage sistemul de pe piața pe care a fost introdus, pentru a rechema sistemul sau pentru a se asigura că furnizorul, importatorul sau orice operator relevant ia măsurile corective care se impun pentru a se asigura de conformitatea sistemului de IA cu grad ridicat de risc cu cerințele la care am făcut referire anterior. Dacă sistemul de IA prezintă riscuri pentru sănătatea, siguranța sau pentru drepturile fundamentale ale persoanelor, distribuitorul trebuie să informeze de îndată furnizorul sau importatorul sistemului și autoritățile competente pentru sistemul de IA cu grad ridicat de risc respectiv, oferind informații detaliate, preponderent despre neconformitate și orice măsură corectivă întreprinsă până la acel moment.

Distribuitorii au obligația de cooperare cu autoritățile cu competențe în domeniu cu privire la orice acțiune întreprinsă de autorități în legătură cu un sistem de IA cu grad ridicat de risc pus la dispoziție pe piață de distribuitori, preponderent pentru a reduce sau a atenua riscul prezentat de acesta.

5.12. Inteligența artificială în justiție. Cazuri posibile

Deși în urmă cu câțiva ani ni se părea ireal să fim operați cu ajutorul unui robot, nu puteam concepe că vom circula cu o mașină autonomă care nu este condusă de un șofer, nu ne puteam imagina cum este să fim judecați de un judecător-robot, acum, odată cu dezvoltarea tehnologiei și investițiile foarte mari făcute în cercetare, aceste probleme nu mai apar ca fiind atipice, ci începem să le privim ca pe situații normale³⁴.

Incidența sistemelor de IA va fi din ce în ce mai răspândită, urmând a vedea în ce domenii aceste sisteme își vor găsi o utilitate mai mare.

Spre exemplu, din punctul nostru de vedere, în privința litigiilor civile de o dificultate redusă, care pot fi soluționate într-un mod automatizat, considerăm că un sistem de IA poate soluționa un

³⁴ Pentru o analiză în extenso, a se vedea P. Ispas, *op. Cit.*

astfel de litigiu. Cu toate că cel puțin în mod aparent se poate presupune că această idee nu poate fi pusă în aplicare, la nivel mondial roboții, deci sistemele de IA au luat locul mediatorilor, avocaților, judecătorilor, procurorilor, polițiștilor³⁵. Potrivit unor articole identificate în presa din România, în Estonia există deja un robot care soluționează dosare cu o valoare de cel mult 6400 EUR, litigii care nu presupun un probatoriu complex care pot avea ca obiect: divorțuri, datorii neachitate, contracte care nu au fost respectate de părți. În Estonia există un grad impresionant de digitalizare, aspect care ușurează inclusiv intentarea acestor litigii care să fie soluționate de judecătorul.... robot. Decizia robotului poate fi contestată, moment în care litigiul va fi soluționat de judecătorul.... om. Din datele existente în articolul citat, dacă judecătorul robot va da dovadă de acuratețe, filtrând în mod corect datele care îi sunt puse la dispoziție, acesta ar putea judeca și litigii care să ajungă la o valoare de 15.000 EUR.

O testare asupra unui jurist robot s-a realizat și în Statele Unite ale Americii, unde societatea Law Geex a organizat un concurs între om și robot, fiind selectate 30 întrebări de către un juriu format din trei experți de la Stanford și Harvard, întrebările fiind referitoare la 5 contracte. Concursul s-a desfășurat între un robot și cei mai buni practicieni din Statele Unite ale Americii, specializați în contractele selectate. Conform datelor puse la dispoziție de experții din juriu, acuratețea răspunsurilor roboților a fost de 90% iar cea a oamenilor juriști a fost de 85%. Roboții au răspuns în 26 secunde la 20 probleme ridicate, în timp ce oamenii juriști au răspuns în aproximativ 80-90 minute. Având în vedere că în această perioadă doar se pot face anumite testări în acuratețea acestor sisteme de IA, nu vedem ca fiind imposibil ca în câțiva ani să vedem o concurență între oameni și roboți în sălile de judecată.

În China a fost testat și un robot procuror care, potrivit detaliilor existente în presă³⁶, face cercetări pe infracțiuni precum: furt, conducere periculoasă, fraudă cu carduri de credit, fiind programat printr-un sistem de IA. Este adevărat că în China cercetarea este una evoluată, fără a putea emite aceleași pretenții cu privire la statul român care, dincolo de adoptarea unei strategii privind IA, nu observăm niciun studiu publicat, nicio aplecare a autorităților spre a cunoaște și înțelege cât mai bine cum funcționează sistemele de IA. În capitolele care urmează, vom analiza *in concreto* utilizarea IA în justiție, cu precădere în justiția penală, urmând a ne referi inclusiv la identificarea biometrică în timp real.

Este adevărat că scepticii se vor feri în a face aprecieri asupra oportunității introducerii unor sisteme de IA în actul de justiție, însă pe lângă dezavantajele pe care aceste sisteme le prezintă, nu sunt de neglijat multiplele avantaje care, pe de o parte, pot degreva magistrații sau grefierii de activități care pot fi realizate prin procese automatizate, pot ajuta avocații în litigiile în care se impune căutarea practicii judiciare, pot ajuta polițiștii în strângerea dovezilor pentru clarificarea unor cauze etc.

Spre deosebire de om, care poate da dovadă de slăbiciune, de corupție, de subiectivism în adoptarea anumitor soluții, roboții pot fi vulnerabili doar în fața unei programări defectuoase, făcute cu intenția de a folosi un sistem de IA într-un mod neconform prevederilor legale care se

³⁵ <https://mediaflux.ro/judecatorii-roboti-inteligenta-artificiala-da-verdicte-in-procese-civile-cu-mize-mic/>; https://www.dcbusiness.ro/ultima-inventie-a-chinezilor-te-infioara-omul-judecat-de-robot_638626.html;

³⁶ <https://www.express.co.uk/news/science/1542035/china-news-robot-prosecutor-public-crimes-robot-police-dissent>.

vor aplica. Însă dacă ajungem în această ipoteză, prevederile Regulamentului sunt suficiente cât să se instituie un sistem de răspundere, așa cum analiza mai în detaliu într-un capitol dedicat acestei forme de răspundere.

Faptul că anumite soluții pot fi pronunțate în baza unor procese automatizate, ar trebui să se implementeze și mijloace tehnice care să sprijine activitatea magistraților, care să faciliteze adoptarea anumitor soluții. Este adevărat că roboții pot fi testați în primul rând, cel puțin în litigiile civile din România, în procedura prealabilă judecătii, în care instanța analizează regularitatea cererii de chemare în judecată cu dispozițiile legale.

În procedura regularizării, în consecință, roboții ar putea fi programați să verifice conformitatea cererii de chemare în judecată cu dispozițiile legale, deoarece această activitate este una nu foarte complexă și se poate realiza pe bază de proceduri automate. Câtă vreme în prezent regularizarea cererii de chemare în judecată poate dura și 1 an, utilizarea unor asemenea sisteme de IA ar fi de natură să degreveze activitatea desfășurată de instanțele de judecată anterior stabilirii termenelor de judecată în ședință publică.

Totodată, o altă aplicabilitate posibilă ar fi în materie necontencioasă, unde un robot care nu trebuie să conducă o ședință de judecată ar avea toate atuurile necesare pentru soluționarea unor cereri. Chiar dacă în aparență cel puțin utilizarea în sistemele de justiție din statele membre va necesita un timp pentru adaptarea sistemelor, legislației aplicabile, programării sistemelor astfel încât acestea să fie utilizate, apreciem că progresiv se poate ajunge la o corectă îmbinare a sistemelor de IA în justiție. Cu titlu de exemplu și fiind mai degrabă o aplicabilitate a digitalizării în servicii conexe justiției, însă se pune și problema implementării unui sistem bazat pe inteligența artificială, câtă vreme prin platforma creată în Spania s-au pus bazele unui sistem de încheiere contractelor de asistență juridică pe cale digitală, soluția adoptată permițând urmărirea contractului încheiat, efectuează identificarea părților semnatare, înregistrează orice demers pentru obținerea trasabilității tranzacției și este integrat unui sistem bancar, care certifică realizarea plății.³⁷ Prin această platformă creată, munca administrativă a avocatului este mult ușurată atât prin prisma încheierii contractului, cât și prin prisma onorariilor care se plătesc exclusiv online, fiind o cerință pentru nașterea valabilă a contractului. În situația în care onorariul nu este plătit în termenul convenit în contractul de asistență juridică, acesta nu mai produce efecte juridice, avocatul nefiind ținut să respecte obligațiile asumate la încheierea contractului.

³⁷ În acest sens, a se vedea confilegal.com.

Capitolul 6

Răspunderea pentru prejudiciile cauzate de inteligența artificială. Riscuri ale utilizării IA în activitatea judiciară

Așa cum s-a descris în literatura de specialitate³⁸, problematica răspunderii pentru prejudiciile cauzate de sistemele de IA este una de mare actualitate, având în vedere caracterul de noutate al reglementării instituite prin Regulament și totodată retinerea sistemelor de justiție existente în statele membre ale UE. Astfel cum s-a reținut în lucrarea citată, nu se poate discuta juridic decât cu precauțiile de rigoare și în circumstanțele cuvenite dacă reglementarea în vigoare a răspunderii civile poate ori trebuie să fie adaptată la situațiile ce implică utilizările inteligenței artificiale. Miza e mai ales aceea de a prezerva caracterul universal al regulilor existente, favorizând totodată emergența IA într-un spațiu securizat din punct de vedere juridic. Din această perspectivă, stabilirea răspunderii pentru daune cauzate de IA este mult mai complexă decât situația clasică reglementată de codurile civile moderne. Utilizarea sistemelor de IA presupune și anumite riscuri, unul dintre riscurile principale fiind acela al suferirii unui prejudiciu.

În momentul în care prejudiciul se produce, se pune întrebarea modalității în care acesta va fi supus reparației.

Este adevărat că sistemul de IA, asemeni animalelor sau lucrurilor, nu se bucură de aceeași capacitate delictuală cerută pentru angajarea acestei forme de răspundere, însă trebuie analizat, în vederea stabilirii propunerii existente la nivelul UE, dacă formele de răspundere reglementate în Codul civil român sunt apte a acoperi și sistemele de IA care pot cauza prejudicii. În toate cazurile, forma de răspundere va fi, din punctul nostru de vedere, o formă de răspundere obiectivă, independentă de condiția vinovăției, în oricare formă a sa.

La nivelul UE a fost inițiată propunerea de Directivă a Parlamentului European și a Consiliului 2022/0303 privitoare la adaptarea normelor în materie de răspundere civilă extracontractuală la inteligența artificială, în preambul fiind reținut că în momentul în care o persoană prejudiciată solicită despăgubiri pentru prejudiciul suferit, normele generale ale statelor membre în materie de răspundere obiectivă impun, de obicei, ca persoana respectivă să dovedească că a avut loc o acțiune sau o omisiune prejudiciabilă din neglijență sau intenționată („culpă”) a persoanei potențial răspunzătoare pentru prejudiciul respectiv, precum și o cauzalitate între culpa respectivă și prejudiciul relevant. Cu toate acestea, atunci când IA este interpusă între acțiunea sau omisiunea unei persoane și prejudiciu, caracteristicile specifice ale anumitor sisteme de IA, cum ar fi opacitatea, comportamentul autonom și complexitatea, pot face excesiv de dificil, dacă nu imposibil, pentru persoana prejudiciată să îndeplinească această sarcină a probei. În special, poate fi excesiv de dificil să se demonstreze că o anumită contribuție pentru care persoana potențial responsabilă este răspunzătoare a generat un rezultat specific al sistemului de IA care a condus la prejudiciul în cauză.

³⁸ Mircea Duțu, *Inteligența artificială și răspunderea civilă*, articol disponibil la <https://www.wolterskluwer.com/ro-ro/expert-insights/inteligena-artificiala-si-raspunderea-civila>.

Totodată, s-a reținut că pentru a se profita de beneficiile economice și societale ale IA și pentru a promova tranziția către economia digitală, este necesar ca anumite norme naționale în materie de răspundere civilă să fie adaptate în mod specific la aceste caracteristici specifice ale anumitor sisteme de IA. Astfel de adaptări ar trebui să contribuie la sporirea încrederii societății și a consumatorilor și, prin urmare, să promoveze introducerea IA. De asemenea, astfel de adaptări ar trebui să mențină încrederea în sistemul judiciar, prin asigurarea faptului că victimele prejudiciilor cauzate cu implicarea IA primesc aceleași despăgubiri efective ca și victimele prejudiciilor cauzate de alte tehnologii.

S-a mai reținut în expunerea de motive a propunerii că scopul inițiativei legislative este de a contribui la buna funcționare a pieței interne prin armonizarea anumitor norme naționale în materie de răspundere extracontractuală bazată pe culpă, astfel încât să se asigure că persoanele care solicită despăgubiri pentru prejudiciile care le-au fost cauzate de un sistem de IA beneficiază de un nivel de protecție echivalent celui de care beneficiază persoanele care solicită despăgubiri pentru prejudiciile cauzate fără implicarea unui sistem de IA. Acest obiectiv nu poate fi realizat în mod satisfăcător de către statele membre, deoarece obstacolele relevante de pe piața internă sunt legate de riscul unor măsuri de reglementare unilaterale și fragmentate la nivel național. Având în vedere caracterul digital al produselor și serviciilor care intră în domeniul de aplicare al propunerii de directivă, aceasta din urmă este deosebit de relevantă într-un context transfrontalier.

Tot în expunerea de motive a propunerii de directivă, s-a reținut că legislația statelor membre privind răspunderea producătorilor pentru prejudiciile cauzate de defectele produselor lor este deja armonizată la nivelul Uniunii prin Directiva 85/374/CEE a Consiliului. Totuși, aceste acte legislative nu aduc atingere normelor statelor membre privind răspunderea contractuală sau extracontractuală, cum ar fi garanția, culpa sau răspunderea obiectivă, întemeiate pe alte motive decât defectul produsului. Deși, în același timp, revizuirea Directivei 85/374/CEE a Consiliului urmărește să clarifice și să asigure faptul că persoana prejudiciată poate solicita despăgubiri pentru prejudiciile cauzate de produsele bazate pe IA defecte, ar trebui, prin urmare, clarificat faptul că dispozițiile prezentei directive nu afectează niciunul dintre drepturile pe care o persoană prejudiciată le-ar putea avea în temeiul normelor naționale de punere în aplicare a Directivei 85/374/CEE.

Pentru a se asigura conformitatea propunerii de directivă cu prevederile Regulamentului, instanțele naționale ar trebui să poată dispune divulgarea sau păstrarea elementelor de probă relevante legate de prejudiciile cauzate de sistemele de IA cu grad ridicat de risc din partea persoanelor care au obligația de a documenta sau de a înregistra informații în temeiul Regulamentului deja adoptat, indiferent de calitatea acestor persoane, dacă sunt furnizori, persoane supuse aceluiași obligații ca și furnizorii sau utilizatorii unui sistem de IA.

Propunerea de directivă este pe deplin alineată cu prevederile Regulamentului, ținând seama că inclusiv definițiile fac trimitere la dispozițiile celui din urmă act, în vederea unei coerențe juridice în lipsa căreia aplicabilitatea, respectiv transpunerea directivei după momentul adoptării, la nivelul statelor membre s-ar face într-un mod defectuos.

Prin articolul 3 din propunerea de directivă se propune ca reglementare divulgarea elementelor de probă și prezumția legală relativă la neconformitate. Conform propunerii arătate, statele membre urmează să se asigure, la transpunerea directivei (s.n.), că instanțele naționale vor fi îndreptățite, fie la cererea unui reclamant potențial care a solicitat anterior acest lucru unui furnizor, fie a unui utilizator, să divulge elementele de probă relevante aflate la dispoziția sa cu

privire la un sistem de IA cu grad ridicat de risc care ar fi produs prejudicii. Pentru a-și susține o atare cerere, reclamantul potențial trebuie să prezinte fapte și elemente de probă suficiente pentru a avea întemeiată o cerere în despăgubiri.

Pentru a se primi o cerere în despăgubiri, instanța va dispune divulgarea probelor numai dacă reclamantul dovedește că a întreprins toate încercările de a strânge elementele de probă de la pârât. La momentul transpunerii prevederilor directivei, statele membre se vor asigura că instanțele naționale sunt abilitate, la cererea unui reclamant, să dispună măsuri specifice pentru păstrarea elementelor de probă.

Instanțele de judecată se vor asigura și vor limita divulgarea elementelor de probă doar la aspectele necesare și proporționale pentru a susține o asemenea cerere sau o acțiune în despăgubiri.

Nu este de neglijat că aceste informații solicitate a fi divulgate vor avea un caracter sensibil, nefiind publice, aspect care se regăsește și în propunerea de directivă, respectiv în art. 3 alin. 4 unde se propune spre reglementare că în vederea stabilirii aspectului dacă un ordin de divulgare sau de păstrare a elementelor de probă este proporțional, instanțele naționale iau în considerare interesele legitime ale tuturor părților, inclusiv ale terților în cauză, în special în ceea ce privește protecția secretelor comerciale în sensul articolului 2 alineatul (1) din Directiva (UE) 2016/943 și a informațiilor confidențiale, ca de exemplu informațiile legate de siguranța publică sau securitatea națională.

Totodată, statele membre se asigură că, în cazul în care se dispune divulgarea unui secret comercial sau a unui presupus secret comercial pe care instanța l-a identificat drept confidențial în sensul articolului 9 alineatul (1) din Directiva (UE) 2016/943, instanțele naționale sunt abilitate, la cererea motivată corespunzător a unei părți sau din proprie inițiativă, să ia măsurile specifice necesare pentru a păstra confidențialitatea atunci când elementele de probă respective sunt utilizate sau menționate în cadrul procedurilor judiciare.

Statele membre se asigură, de asemenea, că persoana obligată să divulge sau să păstreze elementele de probă menționate la alineatul (1) sau (2) dispune de căi de atac procedurale adecvate ca răspuns la astfel de ordonanțe.

Astfel cum rezultă din propunerea de mai sus, informațiile pe care reclamantii le pot solicita se bucură de un caracter privilegiat, astfel încât ca urmare a procedurii de transpunere, statele membre vor stabili un echilibru între drepturile reclamantului la a folosi informațiile protejate în vederea întemeierii pretenției sale deduse judecății și caracterul informațiilor care, potrivit directivei, se bucură de protecție sporită, fiind informații nepublice.

În toate cazurile, statele membre vor modifica legislația aplicabilă unor astfel de proceduri judiciare, astfel încât persoana obligată la divulgarea unor astfel de informații să aibă o cale de atac procedurală față de hotărârea prin care va fi obligat la divulgare.

Aceste situații trebuie foarte bine echilibrate din punct de vedere legislativ, deoarece legislația recunoaște deopotrivă dreptul reclamantului de a solicita ”declasificarea” acestor informații în vederea dovedirii unei acțiuni în răspundere pentru prejudiciul cauzat de un sistem de IA cu grad ridicat de risc, însă trebuie analizată și sensibilitatea informațiilor care urmează să fie puse la dispoziția reclamantului deși au un caracter protejat, confidențial.

Din punctul nostru de vedere, provocarea dată de propunerea de directivă va trebui să fie atent analizată la nivel legislativ de statele membre deoarece trebuie stabilit un echilibru între drepturile părților din litigiu. Din punctul nostru de vedere, prejudiciul ar trebui să fie unul neechivoc pentru ca reclamantul să poată face o asemenea solicitare în fața instanței de judecată în vederea înlăturării caracterului confidențial al acestor informații confidențiale.

Este adevărat că putem analiza critic și situația în care, bazându-se tocmai pe protecția caracterului confidențial al acestor informații, pârâtul să poată ascunde anumite caracteristici sau informații din care rezultă în mod evident că sistemul de IA care a cauzat prejudiciul nu este conform cu Regulamentul, aspect care ar putea atrage răspunderea pecuniară în temeiul acestui din urmă act.

Până la momentul la care directiva va fi adoptată, putem doar exprima probleme potențiale care pot apărea în actuala propunere cu aplicabilitate directă asupra posibilității unui reclamant de a putea folosi informațiile pe care pârâtii le vor proteja ca fiind confidențiale și care nu sunt de natură să fie divulgate.

Potrivit art. 3 alin. (5) din propunerea de directivă, în situația în care pârâtul nu se conformează unei ordonanțe emise de o instanță națională în cadrul unei cereri pentru acordarea de despăgubiri de a divulga sau de a păstra elementele de probă aflate la dispoziția sa în temeiul alineatului (1) sau (2), o instanță națională prezumă nerespectarea de către pârât a unei obligații de diligență relevante, în special în circumstanțele menționate la articolul 4 alineatul (2) sau (3), și că elementele de probă solicitate au fost menite să ofere dovezi în sensul cererii relevante pentru acordarea de despăgubiri.

În consecință, refuzul pârâtului de a se conforma dispozițiilor judecătorești instituie o prezumție simplă că acesta nu a respectat o obligație de diligență, prezumție care poate fi răsturnată de pârât.

În toate cazurile, apreciem în continuare că există posibilitatea ca persoanele obligate să divulge astfel de informații confidențiale vor opune o mare rezistență, însă din punctul nostru de vedere, propunerea de directivă trasează pentru statele membre suficiente linii directoare, astfel încât să se garanteze persoanelor prejudiciate de sistemele de IA cu grad ridicat de risc posibilitatea de a se adresa instanței de judecată, posibilitatea de a proba prejudiciul, asigurându-se totodată și dreptul pârâtului de a ataca o hotărâre prin care a fost obligat să dezvăluie informații confidențiale, în vederea păstrării unei poziții de egalitate juridică între părțile implicate în litigiu.

În continuare, propunerea de directivă propune reglementarea unei prezumții relative a cauzalității în caz de culpă, în art. 4. Conform prevederilor propunerii de directivă, instanțele naționale prezumă, în cazul unei cereri de despăgubire, cauzalitatea dintre culpa pârâtului și rezultatul produs de sistemul de IA sau incapacitatea sistemului de IA de a produce un rezultat, în cazul în care vor fi îndeplinite în mod cumulativ cerințele stabilite în art. 4 alin. (1) lit. a)- c), respectiv:

a) reclamantul a demonstrat sau instanța a prezumat, în temeiul articolului 3 alineatul (5), culpa pârâtului sau a unei persoane pentru al cărei comportament este responsabil pârâtul, constând în nerespectarea unei obligații de diligență prevăzute în dreptul Uniunii sau în dreptul intern, menite în mod direct să protejeze împotriva prejudiciului produs;

(b) se poate considera în mod rezonabil că este probabil, pe baza circumstanțelor cazului, ca culpa să fi influențat rezultatul produs de sistemul de IA sau incapacitatea sistemului de IA de a produce un rezultat;

(c) reclamantul a demonstrat că rezultatul produs de sistemul de IA sau incapacitatea sistemului de IA de a produce un rezultat a generat prejudiciul.

În situația în care se formulează o cerere în despăgubiri împotriva unui furnizor de IA cu grad ridicat de risc, conform cerințelor art. 4 alin. (2) sau împotriva unei persoane care are obligațiile unui furnizor, în condițiile stabilite de Regulament, cerința de la art. 4 alin. (1) lit. a) este îndeplinită doar dacă reclamantul poate demonstra că furnizorul sau persoana care are obligațiile

furnizorului nu a respectat una dintre cerințele prevăzute în Regulament (în accepțiunea propunerii de directivă Legea privind IA, s.n.), cu luarea în considerare a măsurilor întreprinse în cadrul sistemului de gestionare a riscurilor și de rezultatele acestuia realizate în conformitate cu Regulamentul. Astfel, pentru ca acest alineat să fie aplicabil, trebuie îndeplinită una din următoarele cerințe:

(a) sistemul de IA este un sistem care utilizează tehnici ce implică antrenarea de modele cu date și care nu a fost elaborat pe baza unor seturi de date de antrenament, de validare și de testare care îndeplinesc criteriile de calitate menționate la [articolul 10 alineatele (2)-(4) din Legea privind IA];

(b) sistemul de IA nu a fost conceput și dezvoltat într-un mod care să îndeplinească cerințele de transparență prevăzute la [articolul 13 din Legea privind IA];

(c) sistemul de IA nu a fost conceput și dezvoltat într-un mod care să permită o supraveghere eficientă de către persoane fizice în perioada în care sistemul de IA este utilizat în temeiul [articolului 14 din Legea privind IA];

(d) sistemul de IA nu a fost conceput și dezvoltat astfel încât să atingă, având în vedere scopul său preconizat, un nivel adecvat de acuratețe, robustețe și securitate cibernetică în temeiul [articolului 15 și al articolului 16 litera (a) din Legea privind IA] sau

(e) acțiunile corective necesare nu au fost luate imediat pentru a aduce sistemul de IA în conformitate cu obligațiile prevăzute în [titlul III capitolul 2 din Legea privind IA] sau pentru a retrage sau a rechema sistemul, după caz, în temeiul [articolului 16 litera (g) și al articolului 21 din Legea privind IA].

Dacă cererea care are ca obiect acordarea de despăgubiri, cererea fiind îndreptată împotriva unui utilizator de sistem de IA cu grad ridicat de risc care face obiectul cerințelor prevăzute în capitolele 2 și 3 de la titlul III din Regulament, cerința prevăzută de art. 4 alin. (1) lit. a din propunerea de directivă este îndeplinită dacă reclamantul face dovada faptului că utilizatorul:

(a) nu și-a respectat obligațiile de a utiliza sau de a monitoriza sistemul de IA în conformitate cu instrucțiunile de utilizare însoțitoare sau, după caz, de a suspenda sau de a întrerupe utilizarea acestuia (în temeiul [articolului 29 din Legea privind IA]) sau

(b) a expus sistemul de IA la date de intrare aflate sub controlul său care nu sunt relevante având în vedere scopul preconizat al sistemului (în conformitate cu [articolul 29 alineatul (3) din lege]). În cazul în care pârâțul demonstrează că reclamantul are acces în mod rezonabil la suficiente elemente de probă, prezumția instituită în art. 4 alin. (1) din propunerea de directivă nu va putea fi aplicată de către instanțele naționale.

Propunerea de directivă mai analizează două ipoteze în legătură cu cererile de despăgubiri introduse în fața instanțelor naționale cu referire la prejudicii cauzate de sisteme de IA care nu prezintă grad ridicat de risc, în această ipoteză prezumția reglementată de art. 4 alin. (1) din propunere urmând a putea fi aplicată doar dacă instanța națională consideră că dovedirea de către reclamant a cauzalității menționate în alin. (1) este excesivă. În cazul în care proba poate fi făcută de către reclamant într-un mod facil, aplicabilitatea prezumției nu poate opera.

O ultimă ipoteză reglementată de propunerea de directivă se referă la situația în care cererea pentru acordarea de despăgubiri este îndreptată împotriva unei persoane care a utilizat sistemul de IA ca activitate personală, neprofesională, în această situație prezumția se poate aplica doar dacă persoana împotriva căreia este îndreptată cererea a intervenit în mod semnificativ în condițiile de funcționare a sistemului de IA sau în cazul în care acestei persoane i s-a cerut să

stabilească în ce condiții poate funcționa sistemul și deși era în măsură să dea curs solicitării reclamantului, nu a făcut-o.

Astfel cum rezultă din propunerea de directivă ale cărei prevederi le-am amintit, documentul instituie o protecție sporită în privința unei persoane prejudiciate ca urmare a prejudiciului cauzat de un sistem de IA cu grad ridicat de risc. De remarcat este și faptul că propunerea de directivă acoperă și prejudiciile cauzate de un sistem de IA care nu prezintă un grad ridicat de risc, dar și situația în care o persoană acționează în interes personal, particular, utilizează un sistem de IA și cauzează altuia un prejudiciu.

În momentul în care propunerea de directivă se va concretiza și va fi adoptată la nivel european, va reveni în sarcina fiecărui stat membru obligația de a transpune în legislația națională prevederile acestei directive, în vederea unei reglementări a acestei forme de răspundere civilă delictuală. Cu toate că nu face obiectul prezentei lucrări, nu excludem ca punct de plecare instituirea unui sistem al răspunderii apropiat cu răspunderea pentru produsele defectuoase, ca formă obiectivă a răspunderii civile extracontractuale.

Capitolul 7

Sancțiuni pentru nerespectarea prevederilor regulamentului

Art. 99 din Regulament stabilește că în conformitate cu dispozițiile actului normativ european, statele membre stabilesc normele privind sancțiunile și alte măsuri de aplicare a legii care pot include și avertismente și sancțiuni nemonetare. Totodată, statele membre iau toate măsurile necesare pentru a se asigura că aceste sancțiuni și măsuri sunt puse în aplicare într-un mod corespunzător și efectiv, cu luarea în considerare a orientărilor emise de Comisie în conformitate cu dispozițiile art. 96 din Regulament.

Sancțiunile trebuie să fie efective, proporționale și cu efect de descurajare. Statele membre notifică Comisiei normele privind sancțiunile și orice alte măsuri de aplicare a legii menționate în art. 99 alin. (10) din Regulament și comunică totodată orice modificare ulterioară care intervine în legătură cu aceste sancțiuni.

Astfel cum vom vedea în cele ce urmează, sancțiunile stabilite în Regulament sunt stabilite având în vedere gravitatea încălcărilor prevederilor legale conținute în actul normativ european, aspect care este previzibil având în vedere faptul că în Regulament sunt reglementate și practicile interzise în domeniul inteligenței artificiale, sistemele de IA cu grad ridicat de risc dar și sistemele de IA de uz general care, cel puțin în teorie, nu sunt de natură să genereze încălcări ale prevederilor analizate și implicit nici să atragă aplicarea unor sancțiuni în temeiul Regulamentului.

În conformitate cu art. 99 alin. (3), nerespectarea oricăreia dintre interdicțiile privind practicile în domeniul IA menționate la articolul 5 din Regulament³⁹ face obiectul unei amenzi administrative de până la 35.000.000 EUR sau, în cazul în care sancțiunea se aplică unei întreprinderi, sancțiunea poate ajunge până la 7% din cifra sa de afaceri pentru exercițiul financiar precedent, cu luarea în considerare a celei mai mari valori dintre aceste 2 criterii.

Tot cu titlul de sancțiune, art. 99 alin. (4) impune o serie de sancțiuni, în funcție de modul în care încălcarea prevederilor Regulamentului intervine, fiind stabilit că neconformitatea cu oricare dintre dispozițiile referitoare la operatori sau la organisme notificate, altele decât cele prevăzute la art. 5 din Regulament, atrage aplicarea unor amenzi administrative de până la 15.000.000 EUR sau, în cazul în care sancțiunea se aplică unei întreprinderi, de până la 3% din cifra de afaceri pentru exercițiul financiar precedent, cu luarea în considerare a valorii celei mai mari dintre acestea. Prevederile art. 99 alin. (4) se vor aplica în caz de:

- (a) obligațiile furnizorilor în temeiul articolului 16⁴⁰;
- (b) obligațiile reprezentanților autorizați în temeiul articolului 22⁴¹;
- (c) obligațiile importatorilor în temeiul articolului 23⁴²;
- (d) obligațiile distribuitorilor în temeiul articolului 24⁴³;
- (e) obligațiile implementatorilor în temeiul articolului 26⁴⁴;

³⁹ Practicile interzise în domeniul inteligenței artificiale.

⁴⁰ Obligațiile furnizorilor de sisteme de IA cu grad ridicat de risc.

⁴¹ Reprezentanții autorizați ai furnizorilor de sisteme de IA cu grad ridicat de risc.

⁴² Obligațiile importatorilor.

⁴³ Obligațiile distribuitorilor.

(f) cerințele și obligațiile organismelor notificate în temeiul articolului 31⁴⁵, al articolului 33⁴⁶ alineatele (1), (3) și (4) sau al articolului 34⁴⁷;

(g) obligațiile de transparență pentru furnizori și implementatori în temeiul articolului 50⁴⁸.

În situația în care se furnizează informații incorecte, incomplete sau înșelătoare organismelor notificate instituite prin prevederile Regulamentului sau autorităților naționale competente ca răspuns la o cerere face obiectul unor amenzi administrative de până la 7.500.000 EUR sau, în cazul în care sancțiunea se aplică unei întreprinderi, o sancțiune de până la 1% din cifra sa de afaceri pentru exercițiul financiar precedent, cu luarea în considerare a celei mai mari valori dintre acestea. În cazul în care sancțiunea se aplică unor IMM-uri sau unor întreprinderi nou înființate, fiecare amendă stabilită în baza Regulamentului nu depășește procente arătate mai sus sau cuantumul menționat, cu luarea în considerare a valorii celei mai mici dintre acestea.

La stabilirea cuantumului amenzii sau la stabilirea deciziei de a aplica o sancțiune în temeiul Regulamentului, se va acorda o atenție deosebită următoarelor aspecte prevăzute în art. 99 alin.

(7) din actul normativ analizat:

a) natura, gravitatea și durata încălcării și a consecințelor acesteia, ținându-se seama de scopul sistemului de IA în cauză, precum și, după caz, de numărul de persoane afectate și de nivelul prejudiciilor suferite de acestea;

(b) dacă alte autorități de supraveghere a pieței au aplicat deja amenzi administrative aceluiasi operator pentru aceeași încălcare;

(c) dacă alte autorități au aplicat deja amenzi administrative aceluiasi operator pentru încălcări ale altor acte din dreptul Uniunii sau de drept intern, în cazul în care astfel de încălcări rezultă din aceeași activitate sau omisiune care constituie o încălcare relevantă a prezentului regulament;

(d) dimensiunile, cifra de afaceri anuală și cota de piață ale operatorului care a săvârșit încălcarea;

(e) orice alt factor agravant sau atenuant aplicabil circumstanțelor cazului, cum ar fi beneficiile financiare dobândite sau pierderile evitate în mod direct sau indirect ca urmare a încălcării;

(f) gradul de cooperare cu autoritățile naționale competente, pentru a remedia încălcarea și a atenua efectele negative posibile ale încălcării;

(g) gradul de responsabilitate al operatorului, ținându-se seama de măsurile tehnice și organizatorice puse în aplicare de acesta;

(h) modul în care încălcarea a fost adusă la cunoștința autorităților naționale competente, în special dacă și, în caz afirmativ, în ce măsură operatorul a notificat încălcarea;

(i) dacă încălcarea a fost comisă cu intenție sau din culpă;

(j) orice măsură luată de operator pentru a atenua dauna suferită de persoanele afectate.

⁴⁴ Obligațiile implementatorilor de sisteme de IA cu grad ridicat de risc.

⁴⁵ Cerințe cu privire la organismele notificate.

⁴⁶ Filiale ale organismelor notificate și subcontractare.

⁴⁷ Obligații operaționale ale organismelor notificate.

⁴⁸ Obligații de transparență pentru furnizorii și implementatorii anumitor sisteme de IA.

Stabilirea cuantumului amenzilor și decizia de sancționare în temeiul prevederilor Regulamentului trebuie să fie însoțite de garanții procedurale adecvate, inclusiv căi de atac judiciare eficiente și dreptul la un proces echitabil.

Cu alte cuvinte, în implementarea dispozițiilor referitoare la sancțiunile care se vor aplica în baza Regulamentului privind IA, trebuie să se asigure oricărui subiect de drept care poate primi o asemenea sancțiune, garantarea dreptului la un proces echitabil dar și posibilitatea efectivă de a ataca o asemenea decizie de sancționare.

În întregul său ansamblu, Regulamentul tinde să acorde, așa cum am arătat și mai sus, o înaltă protecție a drepturilor utilizatorilor sistemelor de IA dar totodată creează un echilibru și în privința celor care introduc pe piață sistemele de IA și care pot încălca prevederile actului normativ, cu consecința unei sancționări în temeiul aceluiași act. Cu toate acestea, dreptul la un proces echitabil trebuie să fie asigurat de statele membre, astfel încât subiectul de drept sancționat pentru încălcarea prevederilor Regulamentului să aibă posibilitatea să conteste aplicarea sancțiunii, să aibă o cale de atac efectivă împotriva sancțiunii primite.

Va reveni fiecărui stat membru în parte obligația de a-și stabili măsurile, regulile, de a-și conforma legislația internă cu prevederile Regulamentului, de a stabili măsurile procedurale care se impun în vederea asigurării unei protecții a dreptului la un proces echitabil.

Astfel cum rezultă din aspectele prezentate și în capitolul referitor la răspundere prin prisma analizării propunerii de directivă dar și în acest capitol în care am parcurs sancțiunile stabilite pentru nerespectarea prevederilor Regulamentului, nu excludem *ab initio* nici posibilitatea cumulului celor două forme de răspundere deoarece propunerea de directivă analizează situația în care un subiect de drept a suferit un prejudiciu ca urmare a utilizării unui sistem de IA, în timp ce sancțiunile reglementate în Regulament se adresează celor care nu respectă prevederile acestui act normativ, independent de cauzarea unui prejudiciu.

Urmează să analizăm, pe măsură ce prevederile Regulamentului vor fi puse în aplicare și în momentul în care directiva va fi adoptată, care au fost măsurile concrete adoptate la nivelul României și modalitatea în care actele normative europene sunt aplicate.

Capitolul 8

Utilizarea IA în sistemul de justiție. Perspective privind IA și justiția. Justiția asistată de IA. IA în proceduri judiciare

8.1. Utilizarea IA în procedurile judiciare penale este un subiect de actualitate și deja analizat în articole de specialitate⁴⁹. Ca și subdomenii în care IA poate fi folosită, autoarea menționează poliția predictivă, depistarea infracțiunilor, probe generate de sisteme, integrarea inteligenței artificiale în evaluarea riscului și în privința recidivei etc. Dincolo de schimbarea care se produce în modul de investigare tradițional, utilizarea inteligenței artificiale extinde puterile de investigație pentru organele de cercetare penală.

Cu ajutorul IA se pot analiza, prin programe anume programate în acest sens, date referitoare la infracțiuni anterioare și persoane sau locuri asociate cu aceste infracțiuni; utilizarea sistemelor de IA poate fi făcută pentru a face anumite predicții cu privire la locul în care este posibil ca o infracțiune să fie comisă sau chiar cu privire la persoanele care pot comite asemenea infracțiuni. Autoarea lucrării citate apreciază pe bună dreptate că în aceste situații în care pot fi identificate aceste vulnerabilități pe baza utilizării unor sisteme de IA dau posibilitatea autorităților să aloce resurse și să dispună mai multe controale în zonele care prezintă un grad ridicat al infracționalității.

În aspecte care țin de detectarea infracțiunilor, sistemele de IA pot fi folosite pentru identificarea folosirii armelor, dacă senzorii sunt conectați la infrastructura publică și la un computer programat să identifice tragerea cu o armă. În acest fel, poate fi identificat momentul la care s-a tras cu o armă și sunetul acesteia, astfel încât, ca urmare a implementării unui asemenea sistem, nu mai este nevoie de prezența poliției care să identifice aceste aspecte.

Totodată, în lucrarea citată se precizează că utilizarea sistemelor de IA poate fi realizată și pentru a veni în ajutorul judecătorilor care, cu ajutorul IA ar putea determina sentințe corespunzătoare dar și probabilitatea recidivismului.

Se cuvine a menționa că sistemele de IA pot ajuta atât procurorii cât și avocații apărării, deoarece utilizarea unor asemenea sisteme este de natură să ușureze activitățile procurorilor, să ajute la strângerea probelor, la analiza acestora, la o investigare mai rapidă a infracțiunilor săvârșite în mediul online.

Trebuie totuși avut în vedere că implementarea unor astfel de sisteme de IA este costisitoare iar folosirea sistemelor de IA poate fi riscantă în momentul în care o investigație este bazată exclusiv pe baza interpretărilor sau concluziilor unei asemenea tehnologii.

⁴⁹ Use of AI in criminal justice, Dr. Angelika Hellweger, articol disponibil la următoarea adresă web:

https://signin.lexisnexis.com/lnaccess/app/signin?back=https%3A%2F%2Fplus.lexis.com%3A443%2Fuk%2Fdocument%2F%3Fpdmfid%3D1001073%26crd%3D9b0c88b6-d36f-432a-b8d3-adb8111471aa%26pdocfullpath%3D%252Fshared%252Fdocument%252Fnews-uk%252Furn%253AcontentItem%253A68WP-XRH3-RRMG-90WG-00000-00%26pdcontentcomponentid%3D184200%26pdteaserkey%3D%26pdislpamode%3Dfalse%26pddocumentnumber%3D1%26pdworkfolderlocatorid%3DNOT_SAVED_IN_WORKFOLDER%26ecomp%3Dft5k%26earg%3Ds0r%26prid%3D0c80e449-0f1d-4edf-9484-78134979089b&aci=uk

Totodată, trebuie avut în vedere faptul că cel puțin la acest moment, un sistem de IA nu poate înlocui un judecător, însă în activitatea desfășurată în instanțele penale, judecătorii pot fi ajutați de anumite sisteme de IA, însă acestea trebuie îndelung testate și programate astfel încât algoritmi folosiți să nu încalce, spre exemplu, drepturile fundamentale ale persoanei suspecte de săvârșirea unei fapte prevăzute de legea penală. În egală măsură, programarea unui sistem de IA care să aibă suficiente informații cu privire la circumstanțele, agravante sau atenuante, în care fapta a fost săvârșită, dacă persoana a mai săvârșit anterior fapte de natură penală, fiind recidivist, dar și alte asemenea ipoteze care pot conduce la o sporire la micșorare a pedepsei aplicate într-o cauză determinată.

Într-o altă lucrare de specialitate⁵⁰ se subliniază potențialele beneficii și provocări care pot interveni ca urmare a utilizării sistemelor de IA în investigațiile aferente procedurilor penale. Pe de o parte, se apreciază că utilizarea sistemelor de IA poate îmbunătăți eficiența și efectivitatea cercetărilor, conducând la o identificare mai rapidă a conduitei infracționale. Sistemele de IA pot asista în managementul și analiza unui volum mare de date și informații, permițând organelor de cercetare penală să se concentreze pe aspecte mai complexe care necesită discernământ uman și proces de luare a deciziilor.

Astfel, conform lucrării citate, sistemele de IA își pot găsi cu succes aplicabilitatea în cercetarea penală, însă autorul atrage atenția, în mod corect, și asupra provocărilor care însoțesc sistemele de IA. Nu trebuie neglijată situația eticii care trebuie să fie respectată în utilizarea noilor tehnologii, la fel cum trebuie avut în vedere ca utilizarea acestor sisteme să se facă în concordanță deplină cu normele de drept aplicabile. Este adevărat că, așa cum am arătat pe parcursul acestei lucrări, nu puține sunt provocările utilizării sistemelor de IA, în special a acelor sisteme care au un grad ridicat de risc.

Pentru o aplicare eficientă și în conformitate cu dispozițiile legale, este necesar ca programarea sistemelor de IA să se facă în mod progresiv și, cel puțin la început, sub o atentă supraveghere umană. Acest lucru este important din punctul nostru de vedere ținând seama însăși definiția dată de Regulament acestor sisteme de IA care reprezintă un sistem bazat pe o mașină care este conceput să funcționeze cu diferite niveluri de autonomie și care poate prezenta adaptabilitate după implementare, și care, urmărind obiective explicite sau implicite, deduce, din datele de intrare pe care le primește, modul de generare a unor rezultate precum previziuni, conținut, recomandări sau decizii care pot influența mediile fizice sau virtuale.

În consecință, pentru succesul implementării acestor sisteme de IA, procedura de implementare trebuie să fie făcută treptat, pentru a putea vedea rezultatele pe care sistemul le are, modalitatea în care erorile pot fi corectate în vederea obținerii unui rezultat cât mai precis. Utilizarea în justiție trebuie făcută cu și mai mare atenție, având în vedere garanțiile care trebuie oferite de sistemul de justiție pe parcursul procedurilor judiciare, civile sau penale. Implementarea fără respectarea eticii sau fără bază legală solidă, poate genera probleme în utilizarea acestor sisteme bazate pe IA. Mai mult decât atât, nu trebuie neglijat că puterea potențială a sistemelor de IA implică și riscuri. Viteza, complexitatea și scalabilitatea inteligenței artificiale înseamnă că depășește cu mult ființele umane la anumite sarcini. Potențiala inscrutabilitate a algoritmilor

⁵⁰ Gulyamov Said Saidakhrovich *The role of artificial intelligence in investigation*, articol publicat în *Journal of Law and artificial intelligence*, vol. 2, issue 1, iunie 2023, E-ISSN: 2584-1661, pp. 16-22.

auto-generați înseamnă că metoda și raționamentul folosit pentru a produce o anumită ieșire pot fi de necunoscut, chiar și pentru dezvoltatorul AI.

Utilizarea sistemelor de IA în justiție trebuie însoțită de reguli clare de etică prin care să se stabilească reguli privind procesele, procedurile și valorile care sunt menite să asigure cel mai înalt standard de comportament. Totodată, trebuie identificate principii ale eticii, fiind identificate următoarele principii directoare care trebuie avute în vedere: principiul transparenței, principiul responsabilității, principiul siguranței și securității, principiul confidențialității⁵¹.

În același raport, s-a analizat drept caz practic de utilizare a unui sistem de IA, cazul PredPol, o companie din California care a luat naștere dintr-un proiect între UCLA și Departamentul de Poliție din Los Angeles, definește „poliția predictivă [ca] practica de a identifica orele și locațiile în care anumite crime sunt cel mai probabil să se producă, apoi patrularea în acele zone. pentru a preveni producerea acestor crime.” PredPol folosește datele istorice ale unui departament de poliție client pentru o perioadă de doi până la cinci ani pentru a antrena un algoritm de învățare automată, care este ulterior actualizat zilnic. Sunt utilizate doar trei puncte de date: tipul infracțiunii, locația și data/ora. Potrivit PredPol, „Nu se utilizează niciodată informații demografice, etnice sau socio-economice. Acest lucru elimină posibilitatea de încălcare a vieții private sau a drepturilor civile observate cu alte modele de poliție bazate pe informații sau predictive.” Această tehnologie nu este ieftină, ci presupune costuri semnificative, câtă vreme Poliția Kent din Regatul Unit a folosit PredPol din decembrie 2012 până în martie 2018, la un cost de 100.000 de lire sterline pe an. S-a raportat că, în timpul unui proces inițial de patru luni, utilizarea PredPol a dus la o scădere cu 6% a criminalității stradale.

8.2. Inteligența artificială generativă și sistemul de justiție

Inteligența artificială generativă este de bun augur pentru oportunități în ceea ce privește economisirea de timp, productivitatea, accesul îmbunătățit la lege și predictibilitatea justiției. Adaptarea rapidă a companiilor de tehnologie legală și a editorilor juridici demonstrează acest lucru.

Profesioniștii din domeniul juridic trebuie, așadar, să se adapteze la dezvoltarea instrumentelor de inteligență artificială generativă, respectând în același timp principiile lor etice și cadrul de reglementare. Într-un raport al senatului francez⁵², raportorii au remarcat însă decalajul tehnologic tot mai mare dintre profesiile reglementate, care folosesc deja aceste instrumente și elaborează coduri de bună practică specifice acestei tehnologii pentru a limita riscurile pe care le generează utilizarea acesteia, și magistrații și personalul instanțelor, care suferă de subinvestiții majore și de durată în echipamentele lor IT și digitale, care trebuie remediate urgent.

Difuzarea corectă a acestei tehnologii în sectorul juridic necesită, pentru ca aceasta să fie virtuoasă, să se asigure adaptarea formării inițiale și continue a profesioniștilor din domeniul juridic. Software-ul de inteligență artificială generativă este, de fapt, destinat să fie utilizat chiar de profesioniștii din domeniul juridic.

⁵¹ În acest sens, a se vedea Committee on Legal Affairs and Human Rights, Justice by algorithm- the role of artificial intelligence in policing and criminal justice systems, 9 septembrie 2020.

⁵² Raport de informare nr. 216, M. Christophe-André FRASSA et Mme Marie-Pierre de LA GONTRIE,

IA generativă poate avea ca rezultat o efectivă transformare a profesiilor juridice. Utilizarea sistemelor de IA generativă presupune în continuare o acțiune umană ținând cont că această formă de inteligență artificială se bazează pe un model probabilistic ce presupune un risc de eroare ridicat, astfel încât este necesară implicarea profesionistului jurist.

Inteligența artificială generativă nu va putea înlocui oamenii în toate procedurile care necesită interacțiuni interpersonale care, în ciuda locului în creștere pe care tehnologia digitală îl ocupă în societate, rămân centrale. Spre exemplu, consultanța juridică, asistența juridică din partea avocatului nu va putea fi substituită prin utilizarea inteligenței artificiale.

Pentru a discuta despre utilizarea inteligenței artificiale în sistemul de justiție, este necesar în primul rând ca sistemul judiciar să se bucure de o reformă digitală. Aceste discuții sunt, cel puțin la nivelul țării noastre, pur teoretice câtă vreme digitalizarea este destul de puțin dezvoltată și implementată.

Inteligența artificială poate fi extrem de utilă în domeniul sistemului de justiție, pentru prelucrarea datelor sau efectuarea de sarcini repetitive și automatizate, care nu necesită capacitate creativă. Așa cum subliniam pe parcursul acestei lucrări, nu excludem ca procedura regularizării în litigiile civile să se poată face prin intermediul unor sisteme de inteligență artificială. În egală măsură, repartizarea dosarelor pe secții specializate se poate face prin intermediul acestor sisteme de IA care, pe baza unor algoritmi prestabiliți, pot înlocui o persoană care face repartizarea dosarelor.

Nu în ultimul rând, vedem ca oportună implementarea unui sistem de IA care să ajute instanțele de judecată în redactarea hotărârilor judecătorești, exceptând raționamentul instanței care conduce la soluția pronunțată; având în vedere că în România digitalizarea nu este suficient dezvoltată, astfel încât lipsește o infrastructură pe care să fie dezvoltate sistemele de IA, cel mai probabil aceste întârzieri în aplicarea tehnologiei se vor resimți și asupra unei implementări a sistemelor de IA în justiție.

Cu toate acestea, observăm să în alte state membre, precum Franța, problema utilizării sistemelor de inteligență artificială în profesiile juridice a fost și este un subiect de o actualitate covârșitoare cât la nivelul Senatului se întocmesc rapoarte ce au în vedere toate profesiile juridice și implicațiile utilizării inteligenței artificiale asupra acestora. Astfel cum s-a reținut în raportul realizat asupra implicațiilor utilizării acestor sisteme în justiție, s-a reținut că instrumentele de inteligență artificială generativă și-au găsit un ecou favorabil în rândul profesiilor juridice reglementate și a avocaților corporativi, care par mult mai sensibili la acestea decât magistrații și grefierii

Din moment ce companiile legaltech și editorii juridici oferă servicii bazate pe inteligență artificială generativă, în mai puțin de optsprezece luni, profesiile juridice din sectorul privat au început să adopte aceste instrumente la o scară masivă greu de cuantificat cu precizie, dar care totuși par semnificative ținând seama de audierile desfășurate de raportori și de contribuțiile scrise transmise acestora. Conform raportului prezentat Senatului francez, avocații sunt cei mai implicați în adoptarea acestor instrumente, în special în firmele mari de avocatură. Firme de avocatură au confirmat faptul că zilnic folosesc instrumente de inteligență artificială generativă pentru cercetarea juridică și că utilizarea acestor instrumente reprezintă un avantaj față de firmele de avocatură care nu folosesc inteligența artificială.

În același raport se precizează că și consultanții în proprietate industrială testează instrumente de inteligență artificială generativă, pentru a răspunde la întrebări juridice, pentru a redacta răspunsuri sau pentru a efectua cercetări. În egală măsură, comisarii de justiție francezi utilizează inteligența artificială generativă dar și notarii publici.

Dincolo de posibilitățile reale și efective de utilizare a instrumentelor, sistemelor de inteligență artificială în profesiile juridice, apreciem că la nivelul țării noastre, fiecare profesie ar trebui să adopte reguli care să permită practicienilor ajutorului inteligenței artificiale generative. Totodată, transparența utilizării acestor sisteme este un alt subiect care trebuie analizat și suficient reglementat deoarece, spre exemplu, dacă un avocat acordă consultanță juridică întemeindu-se pe un sistem de inteligență artificială, acest lucru ar trebui să fie adus la cunoștința clientului. La fel și în situația în care s-ar ajunge la redactarea hotărârilor judecătorești cu ajutorul noilor tehnologii, implicarea acestor sisteme trebuie să fie una transparentă, realizată în baza unor reguli clare și neechivoce, cu luarea în considerare a tuturor regulilor care trebuie respectate pe baza legislației existente în prezent la nivel european.

Stabilirea unor coordonate logice, transparente și predictibile sunt de natură a contura implementarea unui sistem care să vină în ajutorul celor care îndeplinesc profesii juridice, cu unicul scop al aplicării legii.

Trebuie avut în vedere că relația dintre protejarea drepturilor fundamentale și acțiunile polițienești eficiente trebuie să fie întotdeauna un element esențial în discuțiile despre caracterul oportun și modalitatea de utilizare a IA de către sectorul de aplicare a legii, unde deciziile pot avea consecințe de durată asupra vieții și libertății oamenilor; acest aspect este foarte important, deoarece IA ar putea deveni un element permanent al ecosistemului de justiție penală, oferind analize și asistență în anchete, stabilirea unui probatoriu, reducerea infracționalității etc.

Nu trebuie neglijat că IA este utilizată de autoritățile de aplicare a legii în aplicații cum ar fi tehnologiile de recunoaștere facială, de exemplu, căutarea în baze de date de suspecți și identificarea victimelor traficului de persoane sau ale exploatării și abuzurilor sexuale asupra copiilor, recunoașterea automată a numărului de înmatriculare, identificarea vorbitorului, identificarea vocală, tehnologii de lectură labială, supraveghere sonoră (adică algoritmi de detectare a focurilor de armă), cercetare și analiză autonomă a bazelor de date identificate, prognoză (activități polițienești predictive și de analiză a focarelor infracționale), instrumente de detectare a comportamentului, instrumente avansate de autopsie virtuală care să contribuie la stabilirea cauzei decesului, instrumente autonome de identificare a fraudelor financiare și a finanțării terorismului, monitorizarea platformelor de comunicare socială (extragere și recoltare de date în vederea explorării conexiunilor) și sisteme automate de supraveghere care includ diferite capacități de detectare (cum ar fi detectarea bătailor inimii și camerele cu termoviziune). Aplicațiile menționate mai sus, alături de alte aplicații potențiale sau viitoare ale tehnologiei IA în domeniul aplicării legii, pot prezenta grade diferite de fiabilitate și acuratețe și afectează protejarea drepturilor fundamentale și dinamica sistemului justiției penale; întrucât multe dintre aceste instrumente sunt utilizate în țări din afara UE, dar ar fi ilegale în baza cadrului legislativ și al jurisprudenței Uniunii privind protecția datelor; întrucât utilizarea de rutină a algoritmilor, chiar și cu o rată mică de rezultate fals pozitive, poate face ca numărul de alerte corecte să fie cu mult depășit de numărul celor false;

Trebuie ținut totodată cont că instrumentele și aplicațiile din domeniul IA sunt utilizate și de sistemele judiciare din câteva țări din lume, inclusiv la fundamentarea hotărârilor de detenție preventivă, la stabilirea pedepselor, la calcularea probabilităților de recidivă și la determinarea perioadei de probațiune, la soluționarea online a litigiilor, la gestionarea jurisprudenței și la oferirea unui acces mai facil la legislație; întrucât aceasta a condus la afectarea și diminuarea șanselor pentru persoanele de culoare și alte minorități; întrucât în prezent în UE, cu excepția unor state membre, utilizarea acestora este limitată în principal la cauze civile.

Utilizarea IA în aplicarea legii implică o serie de riscuri potențiale mari și, în anumite cazuri, inacceptabile pentru protejarea drepturilor fundamentale ale persoanelor, cum ar fi opacitate în luarea deciziilor, diferite tipuri de discriminare și erori inerente în algoritmul de bază care pot fi consolidate prin bucle de feedback, precum și riscuri pentru protejarea vieții private și a datelor cu caracter personal, a libertății de exprimare și de informare, a prezumției de nevinovăție, a dreptului la o cale de atac și la un proces corect, precum și pentru libertatea și securitatea persoanelor;

Sistemele bazate pe IA utilizate de autoritățile de aplicare a legii și de cele judiciare pot fi, la rândul lor, vulnerabile la atacuri comise cu folosirea IA împotriva sistemelor informatice sau la practica „otrăvirii datelor” (data poisoning), prin care se introduce un set greșit de date cu scopul de a produce rezultate lipsite de neutralitate, în aceste situații daunele rezultate pot fi chiar mai mari și pot duce la creșterea exponențială a nivelului de nocivitate la adresa persoanelor și grupurilor,

Implementarea IA în domeniul aplicării legii și al sistemului judiciar nu trebuie considerată o simplă chestiune de fezabilitate tehnică, ci o decizie politică privind structura și obiectivele sistemelor de aplicare a legii și de justiție penală; întrucât dreptul penal modern se bazează pe ideea că autoritățile reacționează la o infracțiune după ce aceasta fost comisă, fără a presupune că oamenii sunt periculoși și că trebuie monitorizați constant pentru a preveni eventuale infracțiuni. Tehnicile de supraveghere bazate pe IA pun serios în discuție această abordare și fac urgent necesar ca legiuitorii din întreaga lume să evalueze temeinic consecințele perimiterii utilizării tehnologiilor care diminuează rolul ființelor umane în aplicarea legii și în deciziile justiției.

IA se bazează pe prelucrarea unor cantități mari de date cu caracter personal, dreptul la protecția vieții private și a datelor cu caracter personal se aplică tuturor domeniilor IA și că trebuie respectat pe deplin cadrul juridic al Uniunii privind protecția datelor și a vieții private. La nivelul UE s-au stabilit deja standarde de protecție a datelor pentru autoritățile de aplicare a legii, care constituie baza pentru orice reglementare viitoare în domeniul IA pentru utilizări în aplicarea legii și în sistemul judiciar.

Prelucrarea datelor cu caracter personal ar trebui să fie legală și corectă, scopurile prelucrării ar trebui specificate, explicite și legitime, prelucrarea ar trebui să fie adecvată, relevantă și neexcesivă în raport cu scopul în care sunt prelucrate, ar trebui să fie exactă, actualizată, iar datele inexacte ar trebui corectate sau șterse dacă nu se aplică restricții, datele nu ar trebui păstrate mai mult decât este necesar, ar trebui stabilite termene clare și adecvate pentru ștergere sau pentru analiza periodică a necesității stocării acestor date și ar trebui să fie prelucrate într-

un mod sigur; mai subliniază că ar trebui împiedicată posibila identificare a persoanelor prin intermediul unei aplicații bazate pe IA care a utilizat date anonimizate anterior.

Soluțiile bazate pe IA folosite în asigurarea respectării legii și în sistemul judiciar trebuie, de asemenea, să respecte pe deplin principiile demnității umane, nediscriminării, libertății de circulație, prezumția de nevinovăție și dreptul la apărare, inclusiv dreptul la tăcere, libertatea de exprimare și de informare, libertatea de întrunire și de asociere, egalitatea în fața legii, egalitatea forțelor și dreptul la o cale de atac efectivă și la un proces corect, în conformitate cu Carta și cu Convenția europeană a drepturilor omului.

Pentru a ne asigura că implementarea sistemelor de IA se va face într-un mod conform legii, toate aceste chestiuni trebuie atent analizate la nivelul statelor membre iar acestea trebuie ca, pe baza politicii adoptate la nivel statal să găsească un just echilibru între provocările noilor tehnologii și sistemul de drept împământenit.

8.3. Inteligența artificială generative și profesiile juridice

8.3.1. Utilizarea IA generativă în avocatură

Profesia de avocat poate suferi multiple schimbări ca urmare a utilizării inteligenței artificiale generative.

Ca și beneficii, pot fi menționate speranța economisirii timpului și creșterea productivității. Dacă sunt utilizate în mod corespunzător, instrumentele de IA reprezintă o oportunitate de necontestat deoarece prin intermediul acestora care preiau mare parte din activitățile avocaților, le dau acestora posibilitatea să se concentreze asupra unor aspect și sarcini cu valoare adăugată ridicată.

Ca și sarcini ce pot fi transmise de profesionistul avocat către sistemul de IA generative se pot număra următoarele:

- sarcini administrative, corespondență și traduceri;
- cercetare juridică personalizată pe un subiect determinat în detrimentul utilizării motoarelor de căutare clasice;
- analiza, sinteza și rezumarea documentelor voluminoase, a hotărârilor judecătorești;
- redactarea unor documente standardizate;
- detectarea nerespectării unor proceduri în cadrul dosarelor aflate pe rolul instanțelor de judecată, în special în momentul în care nerespectarea procedurilor ar atrage sancțiunea nulității.

Pentru a obține rezultate optime, este esențial ca sistemul de IA generativ ”să fi fost antrenat” în mod corespunzător, astfel încât sarcinile care îi sunt date să fie îndeplinite în mod corespunzător. Dacă instrumentul de IA generativă, acesta poate prelua sarcini ale unui avocat, sarcini care nu presupun un contact uman și implicit acordă posibilitatea avocatului să dedice mai mult timp unei gândiri analitice, pe care instrumentul de IA i-o facilitează prin căutarea soluțiilor în vederea ușurării muncii avocatului.

Trebuie însă precizat că sistemele de IA nu vor putea înlocui omul în orice acțiune ce trebuie întreprinsă în exercitarea profesiei de avocat chiar dacă, astfel cum am precizat în prezenta lucrare, în SUA a avut loc o testare asupra unui jurist robot, unde societatea Law Geex a organizat un concurs între om și robot, fiind selectate 30 întrebări de către un juriu format din trei experți de la Stanford și Harvard, întrebările fiind referitoare la 5 contracte. Concursul s-a desfășurat între un robot și cei mai buni practicieni din Statele Unite ale Americii, specializați în contractele selectate. Conform datelor puse la dispoziție de experții din juriu, acuratețea răspunsurilor roboților a fost de 90% iar cea a oamenilor juriști a fost de 85%. Roboții au răspuns în 26 secunde la 20 probleme ridicate, în timp ce oamenii juriști au răspuns în aproximativ 80-90 minute. Având în vedere că în această perioadă doar se pot face anumite testări în acuratețea acestor sisteme de IA, nu vedem ca fiind imposibil ca în câțiva ani să vedem o concurență între oameni și roboți în sălile de judecată.

Este adevărat că dacă privim această situație cu un optimism excesiv, putem aprecia că într-o perioadă de timp va exista posibilitatea antrenării unor roboți care inclusiv să pledeze, însă informația transmisă acestora trebuie să se bucure de o mare acuratețe astfel încât robotul să fie suficient de bine antrenat cât să asigure o apărare efectivă. Până la acel moment, sistemele de IA generativă trebuie să fie "hrănite" cu informație corectă, completă și complexă, pentru a-și găsi utilitatea într-o profesie juridică provocatoare cum este profesia de avocat.

8.3.2. Utilizarea IA generativă în activitatea instanțelor de judecată

În raportul întocmit în Senatul francez, anterior citat, s-a reținut faptul că acest concept de justiție predictivă acoperă o varietate de realități pe care este important să le distingem, deoarece acestea nu implică aceleași riscuri și, prin urmare, nu necesită aplicarea aceluiași cadru juridic. Forma de actualitate a justiției predictive este înlocuirea unei decizii judiciare cu un algoritm. Profilarea este legată de aceasta din urmă, deoarece echivalează cu abandonarea către un algoritm a analizei personalității unui individ sau a unui judecător. Aceste prime două forme de justiție predictivă par să fie unanim respinse de cei implicați în drept - și fac obiectul unor interdicții legislative. Cu toate acestea, există forme mai puțin controversate de justiție predictivă, care pot fi asimilate jurimetriei; exemplu, identificarea celei mai probabile decizii, această abordare urmărește obiectivul de transparență și previzibilitate a legii - ca să nu mai vorbim de faptul că nu interferează a priori cu procesul decizional al judecătorului.

Prin urmare, anumite forme de justiție predictivă interzise atât de legislația franceză, cât și de cea europeană. În primul rând, legislația franceză interzice toate tehnicile de profilare în materie judiciară. Articolul 47 din Legea franceză nr. 78-17 din 6 ianuarie 1978 privind prelucrarea datelor, fișierele de date și libertățile individuale interzice unui judecător să întemeieze o hotărâre judecătorească pe o evaluare a personalității unei persoane rezultată din prelucrarea automată a datelor cu caracter personal. De asemenea, articolul interzice ca deciziile care au efecte juridice asupra unei persoane să fie luate doar pe această bază - ceea ce nu se aplică doar deciziilor judiciare.

În consecință, astfel cum este previzibil, sistemul decizional caracteristic activității magistraților judecătorești nu poate suferi o schimbare radicală într-un timp atât de scurt.

Este adevărat că justițiabililor le sunt garantate drepturile fundamentale legate de accesul la instanțele de judecată, dar am văzut exemplul Estoniei unde cererile de valoare redusă sunt ”judecate” de roboți. Astfel cum am precizat și anterior, există dosare de o complexitate foarte mare care nu pot fi soluționate pe baza unor algoritmi sau ai antrenării unui sistem în acest sens iar în această ipoteză utilizarea sistemelor de IA va fi foarte greoaie, însă în activitățile administrative care au loc în cadrul instanțelor de judecată, considerăm că aceste sisteme de IA pot fi implementate cu succes, pentru a facilita activitățile administrative.

Într-un articol recent⁵³, s-a analizat problematica incidenței inteligenței artificiale în justiție și s-a reținut că preocuparea pentru acest subiect a fost reflectată concret și în demersurile Asociației Internaționale a Judecătorilor (IAJ-UIM), prin tema abordată de Comisia de Studii nr. 1 în anul 2024, și anume „Efectele inteligenței artificiale asupra sistemului judiciar”, discutată la cea de-a 66-a Reuniune Anuală a IAJ-UIM, desfășurată la Cape Town, în perioada 17-22 octombrie 2024. Aspectele esențiale ce trebuiau tratate de asociațiile membre au vizat modalitățile efective de utilizare a IA în sistemele judiciare, argumentele pro și contra folosirii IA, posibilele efecte asupra independenței justiției, precum și dacă este sau nu necesară limitarea utilizării IA de către judecători. Concluziile dezbaterilor, scrise și orale, au fost cuprinse în Raportul general al Comisiei de Studii nr. 1 a Asociației Internaționale a Judecătorilor (IAJ-UIM). Printre asociațiile membre care au participat activ la dezbateri s-a aflat, la fel ca în fiecare an, și Asociația Magistratilor din România (AMR).

În articolul citat se enumeră câteva riscuri care sunt inerente utilizării oricărui sistem bazat pe inteligența artificială, după cum urmează:

1. Încrederea excesivă în IA, care ar putea submina judecata umană și înțelegerea nuanțată pe care judecătorii o aduc cauzelor, iar acestea ar putea duce la un sistem judiciar mai puțin uman, erodând încrederea publicului în instanțe. Dependența excesivă de IA ar putea, de asemenea, să facă procesele mentale ale judecătorilor mai pasive, ceea ce ar putea conduce la erori, deoarece instrumentele AI au capacitatea de a „halucina”, adică de a oferi răspunsuri false sau eronate.
2. Prejudecățile din sistemele IA: dacă un sistem are prejudecăți în datele sale de formare, acesta poate reproduce sau chiar amplifica respectivele prejudecăți, conducând la decizii incorecte.
3. Lipsa transparenței sistemelor IA în privința modului de luare a anumitor decizii, fapt care ar putea să afecteze încrederea publicului în sistemul judiciar.
4. Confidențialitatea și securitatea datelor: utilizarea datelor personale ale justițiabililor de către sistemele IA ridică probleme legate de viața privată și confidențialitate, în condițiile în care, în general, instrumentele IA trebuie să colecteze cantități mari de date de la părți, ceea ce poate duce la dezvăluirea de informații personale sau private în mod nejustificat sau nepotrivit.

⁵³ Jud. Dr. Andreea Ciucă, *Justiția și inteligența artificială. Judecător sau judecător-robot?*, articol publicat în revista Universul Juridic, disponibil la adresa web: <https://www.universuljuridic.ro/justitia-si-inteligenta-artificiala-judecator-sau-judecator-robot/>

Este adevărat că am arătat la prezentarea reglementării regulamentului adoptat la nivelul UE în legătură cu inteligența artificială faptul că și la nivelul UE există această preocupare a protecției drepturilor fundamentale, oricând sunt utilizate sisteme de IA.

Dacă plecăm întotdeauna de la prezentarea riscurilor aferente oricărei evoluții, punctul nostru de vedere este că riscul stopează evoluția, aspect care nu este conform cu politicile dezvoltate la nivelul UE și totodată la nivel național.

Dorința de a păstra natura umană a sistemului de justiție este o expresie a clasicului care se opune progresului tehnologic. Admitem că în fază incipientă va fi destul de dificil să ajungem la a implementa judecătorul robot, însă un robot ar putea fi folosit pentru a căuta pentru judecător practică judiciară relevantă sau un sistem de IA ar putea, pe baza unor date preexistente, să ajute la redactarea hotărârilor judecătorești, în procedura regularizării, într-o gestionare mai eficientă a dosarului electronic, acest lucru presupunând și o digitalizare dezvoltată.

În concluzie, sistemul de justiție poate beneficia de mari progrese ca urmare a demarării implementării sistemelor de IA în activitățile conexe celei de judecată. Cu timpul, pe măsură ce aceste sisteme vor fi testate și antrenate în mod corespunzător, nu excludem posibilitatea ca roboții să depășească atribuțiile administrative și să înceapă să fie folosiți și în activitatea de judecare a cauzelor.

Bibliografie

Cursuri, monografii, articole de specialitate

Andreea Ciucă, *Justiția și inteligența artificială. Judecător sau judecător-robot?*, articol publicat în revista Universul Juridic, disponibil la adresa web: <https://www.universuljuridic.ro/justitia-si-inteligenta-artificiala-judecator-sau-judecator-robot/>

Mircea Duțu, *Inteligența artificială și răspunderea civilă*, articol disponibil la <https://www.wolterskluwer.com/ro-ro/expert-insights/inteligenta-artificiala-si-raspunderea-civila>.

Gabriel-Liviu Ispas, Daniela Panc, *Dreptul Instituțional al Uniunii Europene, ediția a II-a revizuită și adăugită*, ed. Hamangiu, București, 2021

Gabriel-Liviu Ispas, Petruța-Elena Ispas, *Răspunderea civilă pentru prejudiciile cauzate de Inteligența Artificială. Nevoia unei reglementări europene*, articol publicat în revista Curierul Judiciar nr. 2/2022

Petruța- Elena Ispas, *Artificial Intelligence. New Challenges*, articol publicat în Central And Eastern European Legal Studies (CEELS) nr. 2/2023, ISSN 2310-2705

Gabriel Manu, Open data în materia hotărârilor judecătorești, articol publicat în Revista Universul Juridic, Revistă lunară de doctrină și jurisprudență | ISSN 2393-3445, la data de 1 octombrie 2020, disponibil la adresa web: <https://revista.universuljuridic.ro/open-data-materia-hotararilor-judecatoresti/>.

Carmen Muñoz Garcia, *Regulacion de la inteligencia artificial en Europa*, ed. Tirant lo blanch, Valencia, 2023

Adrian Onacă, *Transparența justiției în era digitalizării*, articol publicat în revista Themis 1-2/2023, disponibil pe site-ul Institutului Superior al Magistraturii

Vangelis Papakonstantinou, Evangelos Zarkadoulas, *Remote Biometric and emotion recognition in the context of Law Enforcement*, articol disponibil la adresa web <https://eucrim.eu/articles/remote-biometric-identification-and-emotion-recognition-in-the-context-of-law-enforcement/>.

Gulyamov Said Saidakhrovichm *The role of artificial intelligence in investigation*, articol publicat în Journal of Law and artificial intelligence, vol. 2, issue 1, iunie 2023, E-ISSN: 2584-1661.

Legislație națională și europeană

Constituția României

Legea 304/2022

Legea 305/2022

Codul de procedură civilă

Codul de procedură penală

Regulamentul (UE) 2022/850 al Parlamentului European și al Consiliului din 30 mai 2022 privind un sistem informatizat pentru schimbul electronic transfrontalier de date în domeniul cooperării judiciare în materie civilă și penală

Regulamentul (UE) 2020/1784 al Parlamentului European și al Consiliului din 25 noiembrie 2020 privind notificarea sau comunicarea în statele membre a actelor judiciare și extrajudiciare în materie civilă sau comercială

Regulamentul (UE) 2020/1783 al Parlamentului European și al Consiliului din 25 noiembrie 2020 privind cooperarea între instanțele statelor membre în domeniul obținerii de probe în materie civilă sau comercială

Regulamentul (UE) 2023/1543 al Parlamentului European și al Consiliului din 12 iulie 2023 privind ordinele europene de divulgare a probelor electronice și ordinele europene de păstrare a probelor electronice în cadrul procedurilor penale și pentru executarea pedepselor privative de libertate în urma unor proceduri penale

Directiva (UE) 2023/2843 A PARLAMENTULUI EUROPEAN ȘI A CONSILIULUI din 13 decembrie 2023 de modificare a Directivelor 2011/99/UE și 2014/41/UE ale Parlamentului European și ale Consiliului, a Directivei 2003/8/CE a Consiliului și a Deciziilor-cadru 2002/584/JAI, 2003/577/JAI, 2005/214/JAI, 2006/783/JAI, 2008/909/JAI, 2008/947/JAI, 2009/829/JAI și 2009/948/JAI ale Consiliului, în ceea ce privește digitalizarea cooperării judiciare.

Cartea albă „Inteligența artificială – O abordare europeană axată pe excelență și încredere”, 19.2.2020, COM(2020) 65 final.

Jurisprudență

Decizia nr. [23/2022](#) pronunțată de Înalta Curte de Casație și Justiție în recurs în interesul legii

Decizia nr. [5/2022](#), pronunțată de Înalta Curte de Casație și Justiție în recurs în interesul legii

Decizia nr. [1/2023](#) pronunțată de Înalta Curte de Casație și Justiție în recurs în interesul legii

Decizia nr. 28/2021 pronunțată de Înalta Curte de Casație și Justiție în recurs în interesul legii

Site-uri web

<https://publications.parliament.uk/pa/ld5802/ldselect/ldjusthom/180/180.pdf>

<https://digital-strategy.ec.europa.eu/en/policies/european-approach-artificial-intelligence>

<https://www.consilium.europa.eu/ro/press/press-releases/2023/12/08/eu-takes-important-step-towards-digitalisation-of-justice-systems/>

<https://mediaflux.ro/judecatorii-roboti-inteligenta-artificiala-da-verdicte-in-procese-civile-cu-mize-mic/>; https://www.dcbusiness.ro/ultima-inventie-a-chinezilor-te-infioara-omul-judecat-de-robot_638626.html

<https://www.express.co.uk/news/science/1542035/china-news-robot-prosecutor-public-crimes-robot-police-dissent>.

<https://www.euronews.ro/articole/chatgpt-nu-este-o-sursa-sigura-pentru-a-afla-raspunsuri-la-problemele-medicale-co>.

<https://edition.cnn.com/2023/12/10/health/chatgpt-medical-questions/index.html>.

<https://eur-lex.europa.eu/legal-content/RO/TXT/HTML/?uri=CELEX:52022PC0496>.

https://signin.lexisnexis.com/laccess/app/signin?back=https%3A%2F%2Fplus.lexis.com%3A443%2Fuk%2Fdocument%2F%3Fpdmfid%3D1001073%26crd%3D9b0c88b6-d36f-432a-b8d3-adb8111471aa%26pddocfullpath%3D%252Fshared%252Fdocument%252Fnews-uk%252Furn%253AcontentItem%253A68WP-XRH3-RRMG-90WG-00000-00%26pdcontentcomponentid%3D184200%26pdteaserkey%3D%26pdislpamode%3Dfalse%26pddocumentnumber%3D1%26pdworkfolderlocatorid%3DNOT_SAVED_IN_WORKFOLDER%26ecomp%3Dft5k%26earg%3Dsr0%26prid%3D0c80e449-0f1d-4edf-9484-78134979089b&aci=uk