

Reglementarea Inteligenței Artificiale în Uniunea Europeană – respectarea drepturilor omului

Sorin BEJAN*

Abstract: *This article examines the regulation of artificial intelligence (AI) in the European Union, with a focus on respect for human rights. In the context of the rapid advancement of AI technologies, it is essential to ensure that their development and implementation respect the fundamental principles of human dignity, equality and justice. The study examines the existing legislative framework, including proposals for regulating AI, and assesses their impact on individual rights, such as the right to privacy, non-discrimination and access to justice. It also discusses the ethical and social challenges raised by the use of AI, as well as the need for collaboration between European institutions, Member States and civil society to promote a responsible and transparent approach. The conclusions underline the importance of proactive regulation that protects human rights in the digital age, thus ensuring a fair and sustainable future for all European citizens. Creating a positive image of artificial intelligence (AI) is essential, given that although the technology is often criticised, it brings many significant benefits. Thus, AI can help address global challenges such as climate change by optimizing resource consumption, developing sustainable solutions, and modeling data to predict trends. In addition, technologies based on this type of intelligence, such as virtual assistants and personalized recommendations, improve the user experience in various applications, from e-commerce to streaming platforms. AI can also help create solutions that support people with disabilities, such as voice recognition technologies or automatic translation applications, thus facilitating access to information and services.*

Keywords: *Artificial Intelligence, human rights, regulation, European Union*

* Facultatea de Jurnalism, Universitatea Hyperion din București

Parlamentul European a devenit primul legislativ din lume care a adoptat o lege privind inteligență artificială (Parlamentul European, 13 martie 2024). Documentul a fost ratificat în plenara de la Strasbourg, la începutul lunii martie a acestui an cu o majoritate covârșitoare, peste 520 de voturi „pentru” și doar 46 „împotriva”. Legea urmărește să protejeze drepturile fundamentale, democrația și statul de drept în fața sistemelor de inteligență artificială cu grad ridicat de risc. Totodată, actul normativ vizează și să încurajeze inovația și să asigure un rol de lider în domeniu pentru Uniunea Europeană.

Noile norme interzic anumite utilizări ale inteligenței artificiale care amenință drepturile cetățenilor, inclusiv sistemele biometrice de clasificare, bazate pe caracteristicile sensibile ale persoanelor.

Extragerea, fără scop precis, a imaginilor faciale de pe internet ori din înregistrările camerelor video cu circuit închis pentru a crea baze de date de recunoaștere facială se numără și ea printre utilizările interzise. Nu vor fi permise nici recunoașterea emoțiilor la locul de muncă și în școli, atribuirea unui punctaj social, sistemele de poliție predictivă¹. Când imaginile se bazează doar pe stabilirea profilului unei persoane sau pe analiza caracteristicilor sale, și inteligența artificială care manipulează comportamentul uman sau exploatează vulnerabilitățile oamenilor.

Folosirea sistemelor de identificare biometrică de către organele de aplicare a legii este în principiu interzisă, cu excepția unor situații enumerate clar și definite în mod strict în lege.

Astfel, sistemele de identificare biometrică, în timp real, pot fi instalate doar dacă se respectă garanții stricte, de exemplu, dacă folosirea lor este limitată în timp și geografic și este aprobată în prealabil de o autoritate judiciară sau de un organ administrativ. Ele pot fi folosite, de pildă, pentru a căuta o persoană dispărută sau pentru a preveni un atac terorist.

Așadar subiectul acestei lucrări este dedicat Inteligenței Artificiale și Legislației europene. Desigur, nu suntem un produs al

1 Noile norme interzic anumite utilizări ale inteligenței artificiale care amenință drepturile cetățenilor, inclusiv sistemele biometrice de clasificare bazate pe caracteristicile sensibile ale persoanelor. Extragerea fără scop precis a imaginilor faciale de pe internet ori din înregistrările camerelor video cu circuit închis pentru a crea baze de date de recunoaștere facială se numără și ea printre utilizările interzise. Nu vor fi permise nici recunoașterea emoțiilor la locul de muncă și în școli, atribuirea unui punctaj social, sistemele de poliție predictivă – când acestea se bazează doar pe stabilirea profilului unei persoane sau pe analiza caracteristicilor sale – și AI care manipulează comportamentul uman sau exploatează vulnerabilitățile oamenilor.

inteligenței artificiale, dar suntem beneficiarii unei inteligențe native, să spunem așa.

Ce aduce nou acest act normativ adoptat de Parlamentul European?

Acest act normativ este un regulament al Uniunii Europene, deci o să fie direct aplicabil din momentul în care se publică în Jurnalul Oficial², probabil în luna mai sau chiar iunie în acest an, aduce niște obligații pe zona civilă și administrativă pentru cei care fie creează sisteme de inteligență artificială sau cei care le pun în aplicare. În același timp, creează mai degrabă un cadru general în care creatorii de inteligență artificială trebuie să se gândească la sistemele create și să le raporteze la riscurile pe care acestea le pot avea pentru drepturile fundamentale.

Se naște, astfel o întrebare: Teritoriul Uniunii Europene este geografic și administrativ foarte clar delimitat, dar teritoriul virtual... al Uniunii Europene nu e chiar un vârf de lance în dezvoltarea inteligenței artificiale. Vedem roboți japonezi, chinezești, americani și așa mai departe... Cum va fi gestionată această relație în spațiul virtual, dacă există un teritoriu virtual al Uniunii Europene? Am putea spune că nu există un teritoriu virtual – depășirera granițelor terestre – și, evident, se vor naște o serie de probleme din acest punct de vedere³. Însă, pe de altă parte, suntem un public țintă. Adică,

2 Jurnalul Oficial al Uniunii Europene este publicația oficială (Monitorul Oficial) a instituțiilor, organelor, oficiilor și agențiilor UE pentru actele juridice, alte tipuri de acte și informații oficiale. Acesta este publicat de luni până vineri – și în cazuri urgente sâmbăta, duminica și în zilele de sărbătoare legală – în limbile oficiale ale UE la momentul publicării, în prezent 24. EUR-Lex conține versiunea electronică a tuturor Jurnalului Oficial începând de la 30 decembrie 1952, când a fost publicat prima ediție a Jurnalului Oficial al Comunității Europene a Cărbunelui și Oțelului.

3 Potrivit [art. 288](#) din Tratatul privind funcționarea Uniunii Europene (TFUE), pentru exercitarea competențelor Uniunii, instituțiile adoptă regulamente, directive, decizii, recomandări și avize, toate acestea constituind acte juridice. Regulamentul este actul juridic european cu aplicabilitate generală, obligatoriu în toate elementele sale și direct aplicabil în toate statele membre, de la data la care intră în vigoare. Decizia este obligatorie în toate elementele sale, iar în cazul în care se indică destinatarii, este obligatorie numai pentru aceștia, de la data intrării în vigoare. Directiva este obligatorie pentru fiecare stat membru destinat cu privire la rezultatul care trebuie atins, lăsând autorităților naționale competența în ceea ce privește forma și mijloacele. Recomandările și avizele nu au caracter obligatoriu. Actele juridice europene care au caracter obligatoriu (regulamentele, deciziile și directivele) sunt adoptate la nivelul Uniunii prin proceduri legislative (procesul decizional european).

sistemele care sunt accesibile cetățenilor europeni, inclusiv sistemele AI, sunt destul de clare.

O primă reglementare este cea din zona de GDPR și de prelucrare a datelor cu caracter personal, care pot aduce obligații inclusiv celor care nu se află pe teritoriul European, însă vând servicii și produse către cetățenii europeni.

Din acest punct de vedere, consider că acest regulament al AI este binevenit, pentru că scopul său este să protejeze cetățenii europeni de eventuale riscuri și pericole pe care soluțiile de tip AI le-ar putea avea.

Cât de dificil este să identificăm pe cineva care stă în spatele unui astfel de sistem AI?

Dacă vorbim de sisteme AI făcute cu bună credință, n-ar trebui să fie nici o problemă. La fel se întâmplă cu orice serviciu online sau cu orice serviciu digital, unde există obligație de transparență prin care creatorul aceluși sistem poate, trebuie, să spună cine îl creează și cine îl administrează. De obicei, în spatele unui astfel de sistem se află o firmă. Întrebarea este: Ce fel de firmă?

De fapt, răspunsul la această întrebare răspunde și se referă Regulamentul adoptat de Parlamentul European. Tocmai de aceea, acest document nu ar trebui să ridice probleme deosebite. Dacă vorbim, în schimb, de utilizarea malițioasă a unui sistem de AI, atunci e cu totul o altă discuție.

În România, vom observa chiar în Statutul Asociației pentru Tehnologie și Internet faptul că se dorește elaborarea unor anumite coduri de conduită în concordanță cu dispozițiile legii actuale privind comerțul electronic, de pildă.

Chiar dacă este menționat în statut, Asociația își propune să creioneze un astfel de cod. Așadar, e mai degrabă un deziderat de coreglementare, adică de reglementare în care nu doar statul vine să impună niște reguli, ci și zona de sector privat să vină cu niște norme pe care în mod voluntar să le accepte terții. Aici, din păcate, de la dorință la realitate este o cale lungă.

Nici pe legea privind comerțul electronic, mdeși e în vigoare de peste 20 de ani, nu s-a reușit crearea unor astfel de coduri de conduită, cu toate că ele sunt prevăzute și în alte legislații, și în GDPR, dar și în acest regulament privind Inteligența Artificială. Specialiștii sunt de părere că, momentan, e foarte greu ca să ajungi la o adoptare a unui astfel de cod de conduită aplicabil, de fapt, în unul sau mai multe state ale Uniunii Europene. Acest cod ar fi ori sub forma

unui act normativ, de exemplu o lege. Dar, s-ar putea merge și pe varianta unui cod sau document de bune practici în acest domeniu, dar care să implice și pedepse și/sau amenzi. Însă va fi mai greu de aplicat. Când vorbim de coduri de conduită, vorbim întotdeauna de documente care sunt asumate voluntar de cei care participă în astfel de sisteme.

Doar că, de la teorie la practică, este cale lungă și complicată din mai multe puncte de vedere. Putem aprecia faptul că avem în față un domeniu pe care lumea abia îl deslușește și, încet, încet, să-l înțeleagă, un domeniu, cel al tehnologiei informației, un domeniu cu o dezvoltare, însă, absolut explozivă și extrem de accelerată. Nici nu apuci bine să îți cumperi un telefon, căci, după două săptămâni sau o lună, poți spune că este deja vechi și, după alte două săptămâni, apare altul nou... și așa mai departe.

Dar, pe de altă parte, dacă ne uităm la cine controlează majoritatea aplicațiilor din telefon sau chiar pe telefon, observăm că majoritatea serviciilor digitale sunt controlate de un număr foarte mic de firme la nivel global. De aici apare și nevoia unui cod de conduită. Aici sunt alte reglementări ale Uniunii Europene, cele privind serviciile digitale, care au intrat în vigoare pe deplin în februarie, martie, în acest an, și care își propun mai mult decât codul de conduită.

Și aici e important să se înțeleagă faptul că aceste reguli trebuie să fie combinate cu cele din prezentul regulament privind inteligența artificială, care va intra gradual în vigoare. Adică, chiar dacă vorbim de un text adoptat de Parlamentul European, până la publicarea jurnalului oficial o să mai treacă una sau două luni, iar intrarea în vigoare se va face la 20 de zile de la publicare, dar aplicarea va fi treptată, în următorii 2 ani.

Unul dintre domeniile în care există cea mai mare temere pentru utilizarea inteligenței artificiale este cel al dezinformării și al știrilor false, evident. În primul rând, ele pot fi implicate în crearea unui conținut care dezinformează. Aici ne referim, în mod specific, la cele *deepfakes*, care sunt clipuri video sau audio, care sunt construite de la zero cu ajutorul inteligenței artificiale. Nu mai vorbim de o fotografie reală care este apoi retușată prin intermediul unor aplicații precum Photoshop, ci vorbim de o fotografie construită, efectiv, în baza unui șablon, deci a unei instrucțiuni, a unei cerințe, de la zero, sau unui clip video, sau unui clip audio. În prezent, aceste instrumente s-au rafinat, iar accesul la ele s-a simplificat. Uneori este gratuit, alteori e relativ puțin costisitor ca preț.

Ca să dăm un exemplu concret, pentru a falsifica acum vocea cuiva este suficient să ai sub un minut de înregistrare cu vocea acelei persoane și Inteligența Artificială „învață” să copieze inflexiunile, sigur, cu niște limite încă, în așa fel încât să poată păcăli urechea auditorului (Abhang et al., 2016).

Au fost folosite deja în contexte electorale, astfel de clipuri video sau audio, în care persoane politice erau făcute să spună lucruri care să afecteze opinia electoratului și, în cele din urmă, votul. Astfel, Directoratul Național pentru Securitate Cibernetică elaborat un ghid, menit să ofere atât presei, cât și publicului larg, informațiile specifice recunoașterii unor astfel de informații – audio și video (Directoratul Național de Securitate Cibernetică, n. d.).

Este obligatoriu, conform acestei legii, să se pună o etichetă la imaginile sau clipurile sau fotografiile produse de inteligență artificială?

Dacă s-ar putea pune un *watermark*, o astfel de etichetă, automat, asta, cel puțin pentru o persoană care este avizată asupra semnificației conținutului, să spunem, ar fi o măsură pozitivă. Mai ales că inteligența artificială poate fi folosită pentru a compensa o parte din munca de creație umană și atâta timp cât e un proces transparent nu ar fi neapărat o problemă, să spunem. O putem asocia unei creații artistice.

În România a fost un caz cu guvernatorul Băncii Naționale (imaginea de mai jos), când i s-au atribuit o serie de afirmații. Pe imaginile apărute în spațiul public, pe diverse site-uri de socializare, apare un mesaj clar, persoana este asemeni guvernatorului Isărescu, comunică ideile cu subiect și predicat, cum se spune, și o face într-un mod cât se poate de... real. Dar, din păcate, videoclipul prezentat este un produs al Inteligenței Artificiale, iar prezentarea este destul de convingătoare. Numai un ochi vigilent și format în spiritul detectării unor anumite probleme tehnice și a imaginilor care nu concordă cu realitatea, își poate da seama că în fața ochilor are un *fake*.



Sursa imaginii: www.profit.ro

Astfel, s-au înmulțit reclamele de tip *deepfake* pe platformele de socializare în care celebriți, mai ales din lumea financiară, „se oferă” să dea românilor secretul îmbogățirii rapide. Cu buze care se mișcă anapoda și voci care o iau razna, clipurile sunt vizibil trucate, dacă le urmărești cu puțină atenție. Totuși, mulți le iau de bune. Reclamațiile la Facebook și Google nu au însă niciun efect. Intrigant este răspunsul Facebook (și) pentru BNR conform căruia *deepfake*-ul propagat pe platformă, în diversele postări, „respectă standardele rețelei”.

În schimb, Banca Națională a României a reacționat prin intermediul unui comunicat remis presei:

În ultima perioadă, pe mai multe platforme și rețele de socializare, au apărut postări tip *deepfake* care îl implică pe guvernatorul Băncii Naționale a României, Mugur Isărescu. Videoclipurile folosesc fraudulos imaginea și vocea guvernatorului BNR pentru a convinge publicul să facă investiții financiare pe o platformă inexistentă. Reiterăm faptul că Banca Națională a României nu face recomandări și propuneri de investiții. În cazul în care ați dat curs unor astfel de anunțuri false, raportați imediat aceste situații autorităților competente. (Banca Națională a României, 2024)

Au existat astfel de situații, inclusiv în războiul din Ucraina, de pildă, în care surse de dezinformare au creat un fel de *fact-check*-uri, verificări factuale false, în care puneau diagnosticul, să spunem, de *fake* unor imagini reale din conflict, tot mai pentru a delegitima cauza Ucrainei și tentativele acesteia de a arăta amplitudinea distrugerilor din timpul războiului. Și, de asemenea, mai există practica în care materiale *fake* au fost asociate unor organizații internaționale de presă foarte cunoscute, pentru a obține efectul invers, pentru a legitima acel

fake. Deci, da, se poate și... așa. Dar asta nu este un argument să nu folosim aceste etichete.

Orice tehnologie pe care o avem la dispoziție poate fi folosită pentru a crea rău. Tocmai de aceea, există un sistem legal și de reglementare care să identifice și să sancționeze aceste derapaje.

Sigur, nu știu, sincer, dacă avem suficienți specialiști în informatică, specialiști care să fie consultați în aceste cazuri de infraționalitate. Există amenzi și pedepse pentru infraționalitatea cibernetică. Totuși, ce aduce nou această reglementare europeană, adoptată recent? Poate faptul că realizată această clasificare a aplicațiilor inteligenței artificiale, în funcție de gradul de risc și tocmai această clasificare a gravității utilizării AI este binevenită. La fel ca și în cazul dezinformării, există practici care intră, poate, în zona dreptului penal, dacă nu, intră sub incidența, depinde, a diferitelor legi naționale. Aici, pachetul legislativ pentru piețele și serviciile digitale are cel mai important rol în a stabili niște reglementări precise.

Acum, sigur, e la modă să vorbim despre dezinformare, pentru că este un an electoral, nu numai la noi ci și pe plan european. Sunt alegeri europarlamentare. Cam în fiecare an sunt alegeri într-o țară europeană și dezinformarea este o tehnică aplicată în multe cazuri la aceste alegeri.

Cum poate fi incriminată această practică? Cum ar trebui pedepsită?

Mai întâi, aceste practici ar trebui dovedite și apoi pedepsite. Dar, mai întâi de toate, am putea spune că este foarte periculos să intrăm pe panta cenzurii sau unor mecanisme punitive de acest tip. Este foarte delicată această problemă.

Indicat este să fie curățat acest mediul digital, acest „ecosistem”, de această poluare comunicațională. Acesta e primul pas. Este asemeni actului medical – cu cât organismul e mai slăbit, cu atât un virus se răspândește mai repede. Cu cât organismul este mai robust, virusul se răspândește mai greu. Astfel, trebuie lucrat la reconstruirea rezilienței sociale. Cu alte cuvinte, să facem cetățenii mai conștienți de ce înseamnă dezinformarea, să o recunoască, să respingă narațiunile înșelătoare, pentru că înțeleg contextul în care ele circulă și cum sunt lansate de exemplu de actori statali care vor să slăbească Uniunea Europeană.

Există o serie de actori care distribuie conținut, de la omul obișnuit care distribuie cu cele mai bune intenții, până la actori statali sofisticăți care se angajează în acțiuni de război informațional. Avem în față o situație complexă încât nu avem la dispoziție doar un singur tip de măsuri. Sunt măsuri care pornesc de la reglementările supranaționale până, într-adevăr, la anumite precizări de natură penală, dar care sunt limitate și foarte concrete, cum ar fi de exemplu scurgerile de date, pornografia (cea de răzbunare), fraudă de tipul furtului datelor cu ajutorul unor site-uri impoștore, care intră cumva sub incidența aceasta a dezinformării. Iar în rest, în special în Uniunea Europeană, aceste măsuri merg mai mult înspre însănătoșirea ecosistemului media-digital și stabilirea unor obligații suplimentare pentru platforme care au un rol sistemic în a oferi infra-structura de comunicare, mai mult decât măsurile unidirecționale axate pe conținut.

Cum ar fi mai util pentru a ajunge la cetățeni informația?

Există o categorie deja semnificativă de cetățeni și tendința e cu atât mai pronunțată, cu cât aceștia, mai tineri ca vârstă, se informează doar de pe rețelele sociale. Acest fapt îi obligă pe jurnaliști, dar și organizațiile media, să-și stabilească o prezență digitală pe rețelele sociale. În același timp, și oamenii politici, dar și instituțiile politice ar trebui să facă același lucru, pentru a ajunge la cetățeni.

Aici intervine și problema educației media care, în alte state acordă mai multă atenție acestei probleme și începe de la vârste fragede. Pentru că trebuie să învățăm, de pildă, cum să recunoaștem și să facem diferența între un cont fals și contul oficial al primului ministru, să spunem, sau al ministerului X sau paginile oficiale. Adică, trebuie să învățăm să navigăm și noi printre aceste pericole ca utilizatori și cel puțin la nivel universitar și cred că și în licee, într-o oarecare măsură, să se acorde tot mai multă atenție educației digitale și educației pentru media.

În ce măsură inteligența artificială poate să obțină o semnătură electronică, pentru a deveni o persoană?

Specialiștii sunt de părere că există, într-adevăr, un risc asociat cu o asemenea situație, în condițiile în care metodele de identificare de la distanță care sunt în momentul ăsta disponibile, sunt create tot de un sistem de inteligență artificială, dar... la alt nivel.

Utilizarea inteligenței artificiale într-un asemenea scenariu e mai mult în a ataca, de a exploata vulnerabilitățile platformei, care nu să execute acțiunile pe care le face un om. Când se vorbește de inteligență artificială, ne gândim repede la roboții care iau câte o cană de pe masă și o aduc ca să o bem. Dar, inteligența artificială e ceva cu mult mai mult, mai ales spațiul virtual.

Există mecanisme și autorități statale care se ocupă cu urmărirea și identificarea utilizatorilor, dar există și un procentaj foarte mare de utilizatori ai internetului care utilizează rețelele de anonimizare și care nu pot fi identificați. Astfel, până când nu se întâmplă o acțiune care să lege cumva zona fizică, deci existența fizică a unei persoane de o anumită activitate cibernetică, este destul de greu de identificat.

Ce este interesant, este că experții se concentrează mai degrabă asupra aspectelor riscante, iar oamenii obișnuiți se concentrează mai degrabă asupra beneficiilor. Pentru că, dacă ne uităm în acest moment, cred că se apropie de un miliard numărul persoanelor care deja utilizează tot felul de inteligențe artificiale și numărul este în creștere. Așadar, câtă vreme este folosită ca o unealtă pur și simplu, nu cred că e vreo problemă, dar ce ne facem când unealta vrea să ne înlocuiască? Da, acesta este principalul risc, într-adevăr, și anume impactul pe care îl vor avea inteligențele artificiale asupra lucrurilor de muncă. Deci asupra pieței forței de muncă și, pe mai departe, a reglementării acesteia de către legiuitor. În acest sens, sunt multe prognoze, care arată că vor înlocui foarte multe locuri de muncă. Chiar un raport al Forumului Economic Mondial, arată că Inteligența Artificială va crea aproape 100 de milioane de noi locuri de muncă până în 2025 (Russo, 2020).

Concluzii

Apreciem că pe de o parte, crearea unui cadru juridic coerent va facilita creșterea încrederii utilizatorilor, ceea ce va conduce la o creștere a solicitărilor de utilizare a inteligenței artificiale la nivel de companii private și de autorități publice. Pe de altă parte, prin creșterea securității juridice și armonizarea regulilor, furnizorii de AI vor accesa piețe mai mari, cu produse pe care utilizatorii și consumatorii le solicită, le apreciază și le cumpără.

Legea cu privire la inteligența artificială este parte a efortului Uniunii Europene de a fi un lider global în promovarea unei AI de încredere la nivel internațional. Inteligența artificială a devenit o zonă de importanță strategică la răscrucea dintre geopolitică, mize comerciale și preocupări de securitate.

Deși reglementările în domeniul AI sunt abia la început, Uniunea

Europeană și-a asumat deja rolul de lider mondial, sens în care și-a manifestat intenția explicită de a extinde parteneriatele, coalițiile și alianțele în domeniu cu diferiți parteneri globali, fie la nivel statal, fie la nivel instituțional (OCDE, G7 și G20).

Referințe

Articole

- Abhang, P. A., Gawali, B. W. & Mehrotra, S. C. (2016). Technical Aspects of Brain Rhythms and Speech Parameters. in *Introduction to EEG-and Speech-Based Emotion Recognition*. (pp. 51–79). Cambridge: Academic Press, Elsevier.
- Marcusohn, V. (13 decembrie 2022). Legea privind inteligența artificială (AI Act): tot mai aproape!. www.juridice.ro. Disponibil online la adresa: <https://www.juridice.ro/717781/legea-privind-inteligenta-artificiala-ai-act-tot-mai-aproape.html>.
- Russo, A. (20 Oct 2020). Recession and Automation Changes Our Future of Work, But There are Jobs Coming, Report Says. *World Economic Forum*. Disponibil online la adresa: <https://www.weforum.org/press/2020/10/recession-and-automation-changes-our-future-of-work-but-there-are-jobs-coming-report-says-52c5162fce/>.

Documente

- Jurnalul Oficial al Uniunii Europene. (7 iunie 2016). Tratatul privind funcționarea Uniunii Europene (Versiune consolidată). Disponibil online la adresa: <https://eur-lex.europa.eu/legal-content/RO/TXT/PDF/?uri=CELEX:12016E/TXT&from=EN>.
- Jurnalul Oficial al Uniunii Europene. (2022). *Regulamentul (UE) 2022/1925 al Parlamentului European și al Consiliului, din 14 septembrie 2022, privind piețe contestabile și echitabile în sectorul digital și de modificare a Directivelor (UE) 2019/1937 și (UE) 2020/1828 (Regulamentul privind piețele digitale)*. Disponibil online la adresa: <https://eur-lex.europa.eu/legal-content/RO/TXT/PDF/?uri=CELEX:32022R1925>.
- Jurnalul Oficial al Uniunii Europene. (2022). *Regulamentul (UE) 2022/2065 al Parlamentului European și al Consiliului din 19 octombrie 2022, privind o piață unică pentru serviciile digitale și de modificare a Directivei 2000/31/CE (Regulamentul privind serviciile digitale)*. Disponibil online la adresa: <https://eur-lex.europa.eu/legal-content/RO/TXT/HTML/?uri=CELEX:32022R2065>
- Comisia Europeană. (28 septembrie 2022). *Propunere de Directivă a Parlamentului European și a Consiliului privind adaptarea normelor în materie de răspundere civilă extracontractuală la inteligența artificială (Directiva privind răspunderea în materie de IA)*. Disponibil online la adresa: <https://eur-lex.europa.eu/legal-content/RO/TXT/HTML/?uri=CELEX:52022PC0496>.
- Asociația pentru Tehnologie și Internet. (n. d.). Statut. Disponibil online la adresa: <https://www.apti.ro/statut.html>.
- Directoratul Național de Securitate Cibernetică. (n. d.). *Deepfake*. Manipulat sau informat?. Disponibil online la adresa: <https://dnsc.ro/vezi/document/ghid-deepfake>.

Comunicate de presă

Banca Națională a României. (5 februarie 2024). Comunicat de presă: Tentativă de fraudă financiară tip *deepfake* care folosește imaginea guvernatorului BNR. Disponibil online la adresa: <https://www.bnro.ro/page.aspx?prid=23800>.

Parlamentul European. (13 martie 2024). Comunicat de presă: Legea privind inteligența artificială: PE adoptă un act de referință. Disponibil online la adresa: <https://www.europarl.europa.eu/news/ro/press-room/20240308IPR19015/legea-privind-inteligenta-artificiala-pe-adopta-un-act-de-referinta>.