THE NEED TO ADAPT THE LEGAL RESPONSE TO THE COMPLEXITY OF HYBRID AND ASYMMETRIC THREATS IN THE DIGITAL AGE

Viorel GHEORGHE[1]

Abstract

The current development of evolving threats, both to national and international security, the global security environment, in general, is witnessing a state of heightened instability, in fact, of hybrid, asymmetric threats as well as those hybrids with asymmetric element, have been able to produce changes at the level of concepts such as „war", „conflict" and „peace" at all levels, through or with the input of artificial intelligence. The highlighted criminogenic amalgam has become enshrined under the expression „gray zone", which has become a priority for preserving the state of global security, but also the rule of law, in a generic sense, proving the ability to transcend the known theories and concepts of the use of force, as well as the tools and methods of deterrence or control, including three theories that depend entirely on psychological, physical, and normative factors: the balance of power, the normative balance, the balance of terror, and that of deterrence. We observe, without fear of an error, that, within this criminogenic palette, the information factor (especially the digital one), gains constant growth in the interest of scientific research, at the same time generating a necessary modeling of the domestic and international legal framework. Society has become, on the one hand, the victim of increasingly frequent manipulation and disinformation operations, carried out by state actors and proxies of states interested in achieving various goals, and on the other hand, trying to compensate through resilience and assertiveness in the perception process of information. The criminogenic interest in „information dissemination in the online space", as a manifestation of the evolution of the security reality encountered in the proximity of Romania's borders, as well as in different „hot areas" of the world (e.g. the Near East, the Middle East, various regions of Africa and South America), calls for special attention in the management of hybrid threats and asymmetric threats, both forms of serious crime, generating controversies and discussions in the area of legal research, seen as a contributory factor of normative predictability, under the sole purpose of predictability, countering or eliminating any aggressive actions against national security or state defense, under the effect of the universal principles of law: legality, necessity and proportionality. The article is a scientific signal to the need to adapt the law, of all bodies with decision-making powers, in the face of hybrid and asymmetric threats, present, especially, in the digital space, at the same time, to significantly limit the implications and consequences for the fundamental attributes of any state, implicitly for the preservation of fundamental rights and freedoms.

Keywords: *international law; digital space; statehood; conflict; hybrid threat; asymmetric threat*

1. Introducere

Asistăm, în ultimă perioadă, la o tot mai diversificată instrumentalizare a mijloacelor și metodelor neconvenționale pentru purtarea diferitelor forme de agresiune; de asemenea, tot mai des, auzim despre utilizarea, pe scară extinsă, a diferitelor tipuri de tehnologii în satisfacerea îndreptată înspre satisfacerea unor scopuri exclusive ale unora din statele puternice din punct de vedere economic și militar. Această manieră acțională s-a extins și dezvoltat astfel că, în „filosofia actului criminal", tot mai frecvent sunt sesizate prezențe și întrebuințări ale instrumentelor de luptă de sau cu valență sau care incumbă element hibrid[2]

[1] Drd. Expert naţional TAIEX; e-mail: *viorelgheorghe@yahoo.com*.

[2] Conform accepțiunii Uniunii Europene, conceptul de amenințare hibridă urmărește să surprindă amestecul de acțiuni convenționale și neconvenționale, militare și nemilitare, deschise și ascunse care pot fi utilizate în mod coordonat de către actori statali sau nestatali pentru atingerea obiectivelor specifice, rămânând, concomitent, sub pragul intensității unui război declarat oficial. Acestea vizează vulnerabilitățile critice și caută să creeze ambiguitate pentru a împiedica luarea rapidă și eficientă a deciziilor. Gama de măsuri aplicate în cadrul unei campanii hibride poate fi foarte largă: de la atacuri cibernetice asupra sistemelor informaționale critice, prin întreruperea serviciilor critice, cum ar fi aprovizionarea cu energie sau serviciile financiare, până la subminarea încrederii publicului în instituțiile guvernamentale sau exploatarea vulnerabilităților sociale. Un prim pas și crucial pe drumul către obținerea unei mai bune protecție împotriva amenințărilor hibride este dobândirea unei cunoștințe adecvate a situației. Acesta este motivul pentru care informațiile și schimbul de informații devin atât de importante. Pentru a preveni și a răspunde eficient amenințărilor hibride, este esențial să se sporească rezistența

cât și asimetric[1], ori, ce este cel mai grav, depunem proprie mărturie la îmbinarea utilității celor două forme de amenințare, într-o unică realizare a unității infracționale, astfel că, putem spune, zona marțială a intrat într-o nouă eră: cea a amenințărilor mixte la adresa securității naționale și a celei internaționale, fapt care, îndeobște, reclamă o reacție a sistemelor juridice, încă o datăm spus, o reacție juridică proporțională - suntem forțați a o spune - de expresie hribridă și asimetrică, fără teama de a greși.

Inteligența artificială[2] poate avea - și are deja - un impact important asupra segmentelor de interes ale societății, de la sănătate, agricultură și industrie până la servicii financiare și educație. Cu toate acestea, secretarul general al Națiunilor Unite António Guterres a declarat, cu ocazia lansării Strategiei privind noile tehnologii (2018), faptul că „aceste tehnologii sunt foarte promițătoare, ele sunt nu fără riscuri, iar unele inspiră anxietate și chiar teamă. Ele pot fi folosite în scopuri rău intenționate sau pot avea consecințe negative neintenționate"[3]. Apreciez că este o frază elocventă, în legătură cu impactul și influența pe care inteligența artificială deja le are asupra vieții omului, prin dualitatea capacității de dezvoltare, multi-fațetată și superioară oricărei alte forme a tehnologiei emergente. Bunăoară, în timp ce-și poate sduce aportul la progresul multor sectoare (ex. industrie, știință, tehnică etc.), devine tot mai clar faptul că inteligența artificială are și va avea - un din ce în ce mai pregnant - potențial de a limitare sau chiar împiedicare a exercitării drepturilor și libertăților fundamentale ale omului, îndeosebi, spun eu, îndeosebi, a dreptului la nediscriminare, dar și la viață privată, respectiv la libertatea de gândire și de exprimare. Așa încât, orice introspecție a procesului de utilizare a inteligenței artificiale ar trebui să fie nemijlocit dependentă de circumspecție, etică și un permanent efort de prevenire a potențialelor încălcări a drepturilor omului.

---

societăților și a infrastructurii critice. Având în vedere natura amenințărilor hibride, este esențial să se lucreze peste granițele geografice și granițele agențiilor (*https://ec.europa.eu/commission/presscorner/detail/it/MEMO_16_1250*, accesare 01.12.2023).
Conform altei opinii, conceptul de „amenințare hibridă" sau „război hibrid" ridică mai multe întrebări. Comisia pentru afaceri juridice și drepturile omului consideră că, deși nu există o definiție universală pentru această terminologie, principala trăsătură a unui „război hibrid" este „asimetria juridică" a acestuia, întrucât adversarii hibrizi își neagă activitățile și operează chiar la marginea lege. În timp ce acțiunile militare sunt în desfășurare, se aplică dreptul internațional, în special dreptul la autoapărare și dreptul umanitar. În cazul acțiunilor non-militare, este mai presus de toate dreptul penal intern care intră în joc. În toate cazurile, drepturile omului trebuie respectate. Orice restrângere a acestor drepturi trebuie să respecte cerințele care rezultă din Convenția Europeană a Drepturilor Omului (*https://assembly.coe.int/nw/xml/XRef/Xref-XML2HTML-en.asp?fileid=24547&lang=en*).

[1] Una din accepțiuni evocă o posibilă soluție de luat în seamă la stabilirea definiției amenințării asimetrice: „evantaiul larg şi imprevizibil al operaţiilor militare, paramilitare şi de informaţie, conduse de naţiuni, organisme, indivizi sau de forţe indigene sau de plasare sub comanda lor, ce vizează în mod specific slăbiciuni şi vulnerabilităţi într-o guvernare inamică sau într-o forţă armată" (în Michael L. Kolodzie, „Commentary The Asymmetric Threat", *http://www.almc.army.mil/alog/issues/JulAug01/MS628.htm*, p. 1 apud Ghe. Văduva, „Ameninţări asimetrice sau ameninţări hibride: delimitări conceptuale pentru fundamentarea securităţii şi apărării naţionale", Universitatea Națională de Apărare „Carol I", 2013, p. 23-24, lucrare disponibilă la adresa electronică *https://cssas.unap.ro/ro/pdf_studii/amenintari_asimetrice_sau_amenintari_hibride.pdf*, accesare 02.12.2023).

[2] Potrivit unei definiții, inteligența artificială este domeniul informaticii care vizează dezvoltarea sistemelor informatice capabile să performeze sarcini care ar necesita în mod normal inteligența umană, cum ar fi percepția vizuală, recunoașterea vorbirii, traducerea între limbi, luarea deciziilor și rezolvarea problemelor. O mare parte din atractia inteligenței artificiale constă în capacitatea sa pentru a analiza cantități mari de date – denumite și „date mari" – mai rapid și cu mai multă ușurință decât un om analistul sau chiar o echipă de analiști poate face și, făcând acest lucru, să descopere tipare și corelații nevăzute pentru ochiul uman. În plus, inteligența artificială poate extrapola rezultatele probabile ale unui anumit scenariu pe baza datelor disponInteligența artificială este teoria și dezvoltarea sistemelor informatice care sunt capabile să îndeplinească sarcini care necesită în mod normal inteligența umană, cum ar fi percepția vizuală, recunoașterea vorbirii, luarea deciziilor și traducerea între limbi. Inteligența artificială face posibil ca mașinile să învețe din experiență, să se adapteze la noile intrări și să îndeplinească sarcini asemănătoare omului. Cele mai multe exemple de inteligență artificială despre care auziți astăzi, de la computere care joacă șah la mașini cu conducere autonomă, se bazează în mare măsură pe învățarea profundă și pe procesarea limbajului natural. Definiția este regăsită pe platforma *Science Direct* (*https://www.sciencedirect.com/topics/social-sciences/artificial-intelligence*, accesare 30.11.2023).

[3] Countering Terrorism online with Artificial Intelligence an overview for law enforcement and counter-terrorism agencies in South Asia and South-East Asia, articol, Oficiul pentru Combaterea Terorismului al ONU, 2021.

Ce este oarecum îmbucurător este faptul că, deja, lumea a sesizat potențialul de pericol atât al unei greșite întrebuințări, dar mai ales a riscurilor unei eronate interpretări a produselor sau disponibilităților inteligenței artificiale, astfel că o seamă de organizații internaționale și regionale, alături de autoritățile naționale și organizațiile societății civile, sunt sau devin implicate în diferite inițiative (inclusiv de ordin juridic) menite să pună în aplicare fundamentele etice ale unei juste și limitate utilizări a inteligenței artificiale, precum și permanenta apariție și îmbunătățire a cadrului „proto"-juridic nemijlocit asociat problematicii.

Problematica unei corecte întrebuințări a apărut în atenția publică inclusiv pe fondul proliferării amenințărilor de natură hibridă și a celor asimetrice, detectate în mediul online, unde creșterea activității infracționale, îndeosebi, a celei teroriste nu mai poate fi numită provocare ci o prealitate în creștere, devenită, în timp, formă a terorismului contemporan. În acest sens, pot oferi exemplul din anul 2020 când organizația Europol și alte 17 state membre ale Uniunii Europene au identificat și evaluat, pentru a fi eliminate, aproximativ 1906 URL-uri care trimiteau la conținut terorist, aflate pe un număr de 180 de platforme și site-uri web, doar într-o singură zi, proporțional, platforma de socializare Facebook reliefând faptul că, într-un interval de numai doi ani, a eliminat peste de 26 milioane de videclipuri cu conținut terorist sau de apologie a terorismului, menționând ca exemplu pe cele provenite de la entități teroriste organizate precum Daesh, respectiv, de la rețeaua de rețele teroriste Al-Qaeda. Concomitent, în cadrul contemporanului conflict ruso-ucrainean, Internetul și rețelele sociale se dovedesc a fi instrumente puternice în mâinile unor entități care, în mod concertat, propun publicului diferite conținuturi cu evidente valențe de propagandă sau diverse atacuri (cele mai multe, DDoS[1]), permițându-le astfel atât comunicarea, cât și răspândirea mesajelor lor, deopotrivă, a inițiativelor pentru colecte de fonduri, recrutarea aderenților sau susținătorilor diferitelor entități criminale, creând cadrul pentru inspirație și coordonând atacurile asupra diferitelor ținte, specifice sau nespecifice.

2. Era digitală: oportunități și limite în utilizarea inteligenței artificiale

În ultimii ani, integrarea inteligenței artificiale în viața de zi cu zi a crescut într-un ritm extraordinar, prin exacerbarea utilizării rețelelor sociale, în special de către tineri. În timp ce această tendință oferă o gamă largă de oportunități de dezvoltare, libertate de exprimare, participare politică și acțiune civică, este constatată o creștere proporțională a riscului ca persoane vulnerabile (îndeosebi, tinerii) să fie expuși terorismului sau conținutului online produs de entități teroriste sau extremiste. În plus, acest fenomen de translatare a potențialului criminogen în spațiul online, a făcut ca instituțiile statului cu competențe în zona combaterii și reprimării amenințărilor hibride și a celor asimetrice să fie din ce în ce mai forțate să se adapteze la transformările din interiorulo acestui ecosistem criminogen, generând, proporțional, o necesară și utilă implicare a specialiștilor în drept, pentru crearea cadrului normativ al legalității și a unei eficiente reacții în plan normativ.

Inteligenței artificiale și digitalizării, în genere, i-a fost acordată o atenție importantă la nivel internațional, ca instrument care poate procesa cantități mari de date și identificare a modelelor și corelațiilor în datele invizibile omului neinteresat, care pot aduce eficiență în analiza informațiilor complexe, beneficii ce pot fi valorificate în domeniul combaterii amenințărilor hibride, asimetrice dar, mai ales, a amenințărilor hibride cu element asimetric, ca expresie a nelimitării laturii exploratorii asupra potențialului contributor la necesitatea și locul dreptului în societate.

[1] Conform M247, DDoS reprezintă prescurtarea pentru Distributed Denial of Service. Reprezintă un atac în care mai multe sisteme infectate (de obicei cu un virus Troian), sunt folosite pentru a compromite un singur sistem sau o aplicație. Atacatorul folosește sistemele infectate pentru a trimite cereri către sistemul țintă până când acesta nu mai poate gestiona încărcarea de trafic și se blochează (*https://m247.com/ro-ro/servicii/protectie-ddos-administrata/?gad_source=1&gclid=Cj0KCQiAyKurBhD5ARIsALamXaHG7AVW9Pm7T1t07g3kVmsR8maB89rnYIfvUIvuqK-ykgRzZqft7toaAlY0EALw_wcB*, accesare 03.12.2023).

Nu mai este un secret faptul că, astăzi, statele se confruntă cu diversificarea amenințărilor neconvenționale, aceasta incluzând atât planul amenințărilor asimetrice (cu cele mai vizibile dintre ele, radicalizarea, extremismul și terorismul), cât și noile arme utilizate pentru demoralizarea și atragerea populației de partea unei idei, scop, prin dezinformare și manipulare.

Nevoia unei reacții juridice în acest areal de interes este cu atât mai mare, cu cât, astăzi, fenomene esențiale propagării terorismului (ex. radicalizarea) reprezintă un risc tot mai crescut la nivel mondial și național, multe din actele teroriste din ultima perioadă, având la bază acțiunea unui subiect activ izolat („*lone wolf*"), situației specifice asociindu-i-se factorul „pandemia COVID-19", cu rol în diversificarea laturii comisive precum și în accelerarea procesului de digitalizare.

Desigur, aceste evoluții prezintă o gamă largă de oportunități, în măsura în care sunt corect și eficient valorificate, Internetul și rețelele sociale constituind variante comunicaționale inclusiv în procesul de învățământ. În același timp, trebuie spus că, „avantajele" internetului și rețelelor sociale care sprijină activ mișcările societății le fac, în egală măsură, dependente pentru actorii rău-intenționați, constituind o multitudine de provocări pentru autorități. Atât actori precum cei statali, cât și alții, non-statali, alături de diverse categorii de terorişti, extremişti sau pur și simplu oameni cu un comportament viciat de diverse afecțiuni, s-au adaptat noilor paradigme digitale ale acestui secol, învățând utilizarea tehnologiei informației și comunicațiilor, în special, despre spațiul online și nenumăratele aplicații interactive și platforme *social media*, pentru promovarea obiectivelor sau scopurilor (de exemplu, manipularea sau dezinformarea opiniei publice în legătură cu diverse atitudini ale unor șefi de stat, înregistrarea anumitor succese inexistente ale unei entități, în detrimentul alteia, „invadarea" societății unui stat de „idei nocive", toate duse în scopul exclusiv al răspândirii unor curente, ideologii, a propagandei-inclusiv a celei de ură - pentru recrutarea noilor aderenți, simpatizanți (ulterior, membri), dar și pentru organizarea modalităților de sprijin financiar și operațional.

A devenit o realitate: utilizarea unor astfel de tehnologii a devenit paralelă cu utilizarea rețelelor sociale și conținut specializat, adaptat și „răspunzător" la nemulțumirile locale, disponibil în limbile de circulație internațională și în cele naționale.

Dincolo de acest tablou situațional, apare necesitatea - normală socialmente - de oferire a unui răspuns juridic, care, de cele mai multe ori, se dovedește a fi adaptabil contextului societal, atât legislativul, cât și instituțiile cu atribuții în domeniu, fiind „testate" cu noi provocări (de exemplu, investigații tot mai complexe și extinse, care includ medii din ce în ce mai dificil de penetrat, și situații diferite de domeniile lor tradiționale de expertiză), uneori, cazuistica reținând ani de muncă pentru a căuta și verifica, în mod profesionist, informațiile relevante în caz. Acesta este și motivul afirmației conform căreia, instituțiile competente sunt forțate să țină pasul cu transformarea digitală, cu pătrunderea inteligenței artificiale, în aest sens, existând un interes major pentru eliminarea lacunelor legislative, spun, proporțional cu necesitatea adaptării cadrului normativ în domeniul respectării drepturilor și libertăților fundamentale ale omului.

Pe de altă parte, trebuie spus că inteligența artificială poate fi un instrument puternic în combaterea acestor tipuri de amenințări, permițând structurilor informative ca și celor de aplicare a legii să efectueze cercetări amănunțite care pot duce la creșterea eficacității, creșterea capacităților existente, permițându-le, în final, să se descurce cu creșterea masivă a datelor (ex. asistarea analiștilor prin formularea de predicții privind viitoarele scenarii cu potențial criminogen, identificarea tranzacțiilor financiare suspecte care pot fi indicative pentru finanțarea înarmării unor state sau entități teroriste; precum și monitorizarea spațiului virtual, pentru prevenirea comportamentului extremist-terorist.

De aceea, astăzi, sensibilizarea la potențialul de avansare socială cu inteligența artificială este și trebuie pusă, totuși, în echilibru cu preocupările referitoare la posibile efecte negative și consecințe negative ce pot reieși din implementarea acestui tip de tehnologie, fapt pentru

care, în prezent, constituie subiectul unor serioase dezbateri care cuprinde zona teoriei și aplicării unor ramuri de drept, etica și factorii de decizie din întreaga lume.

Consider că problematica este departe de a fi clarificată, și numai dacă este privită din perspectiva protecției drepturilor omului. Cu toate acestea, din perspectiva asigurării securității unui stat, necesitatea unei adaptări, în care apare și elementul inteligență artificială, transformarea digitală există cu siguranță, pe fondul ratei crescute de digitalizare și prezența tot mai mare a vârstei tinere, cu potențial vulnerabil.

Înțelegerea unei utilități a elementului digital poate fi pusă în context doar prin caracterul util al suportului pe care anumite disponibilități tehnice îl pot conferi unui ansamblu informațional sau de date, deja stabilit.

Astfel, inteligența artificială poate fi utilă prin procesarea limbajului natural (NLP), o aplicație de învățare profundă care se referă la procesarea și analizarea amplă a unei cantități de date naturale ale limbajului uman, pentru a permite dispozitivelor „să citească", „să înțeleagă" și „să obțină" sens de la limbajul uman.

O altă funcție a inteligenței artificiale este cea de a recunoașterii obiectelor, funcție care se bazează pe algoritmi de învățare profundă pentru a procesarea imaginilor și identificarea forme geometrice, respectiv a obiectelor.

Analiza predictivă este o altă funcție a inteligenței artificiale care vizează latura anticipativă a unui eveniment viitor sau a necunoscutelor posibile, prin perspectiva evenimentelor deja petrecute, din aceasta, extrapolând rezultatele probabile în contexte conexe. Include mai multe tehnici statistice și învățare automată care analizează faptele actuale și istorice, fundamente ale predicțiilor[1].

Modelele predictive captează relațiile dintr-o serie de variabile pentru a permite evaluarea riscului asociat cu un anumit set de condiții. Instrumentele bazate pe învățarea automată pot prezenta rezultate folosind diagrame simple, grafice și scoruri care indică probabilitatea evenimentelor în viitor, ghidând procesele de luare a deciziilor.

O altă funcție este cea a analizei rețelelor sociale (SNA), în fapt, o abordare extinsă și cuprinzătoare utilizată în înțelegerea și modelarea structurilor de rețea și comportamentul actorilor din acestea. Una din etapele implementării acestui instrument a constat în decizia platformelor Facebook, Twitter, Google și Microsoft au anunțat planuri de a aborda conținutul extremist (decembrie 2016) folosind PhotoDNA.

3. Exemple în utilizarea „inteligenței artificiale și potențialul de utilitate juridică în era digitală

În textul *Strategiei globale de combatere a terorismului a Națiunilor Unite* (adoptată la data de 8 septembrie 2006), statele membre au decis să colaboreze cu Organizația Națiunilor Unite cu respectarea confidențialității, respectarea drepturilor omului precum și cu respectarea altor obligații conform dreptului internațional, explorând modalități de coordonare a eforturilor la nivel internațional și regional de combatere a terorismului, sub toate formele și manifestările fenomenului, inclusiv în spațiul virtual, utilizând Internetul ca instrument de combatere a răspândirii terorismului. În același timp, strategia recunoaște că statelor membre li se poate acorda asistență pentru îndeplinirea acestor angajamente.

Reala amenințare generată de dezvoltarea amenințărilor hibride și asimetrice a impus examinarea tendințelor și evoluțiilor esențiale conexate erei digitale, analizând ce înseamnă aceasta prin directă raportare la utilitatea manifestă în zona instituțiilor cu competențe în studiul și monitorizarea acestor tipuri de amenințări.

În raport cu imprevizibilitatea comportamentului uman și starea actuală a dezvoltării tehnologice, aplicarea de algoritmi pentru a „prezice" comportamente la nivel individual va

[1] **H. Smolic, „What is Predictive Analytics? A Definition and Overview", articol în platforma Graphite, 31.10.2023 (**https://graphite-note.com/what-is-predictive-analytics-a-definition-and-overview**, accesare 29.11.2023).**

rămâne, foarte probabil, de o valoare foarte limitată. În plus, la nivelul juriștilor, experți în respectarea drepturilor și libertăților fundamentale precum și al organizațiilor societății civile, au fost sesizate mai multe preocupări de valență etică referitoare la potențialele „puncte slabe" pentru activitatea de judecată, cu referire la tratamentul discriminatoriu. Cantitățile mari de date referitoare la o persoană necesare algoritmului, pentru a funcționa cu acuratețe, dă naștere, în continuare la preocupări în privința posibilității unei supravegheri în masă nejustificate și nelegale.

În accepțiune proprie, analiza predictivă poate contribui la combaterea ambelor forme de amenințări, chiar dacă într-un mod diferit, astfel, o monitorizare a persoanelor în mediul virtual, fiind înlocuită cu o prognoză comportamentală, modele predictive bazate pe statistici din surse online care au fost complet anonimizate sau cel puțin pseudonimizate, în scopul legal al protejării confidențialității. Totodată, instrumentul are capabilitatea de a fi utilizat pentru prognoză, identificarea și stabilirea tendințelor comportamentule ale diverșilor subiecți de interes în activitatea structurilor de informații sau aplicare a legii, în situația desfășurării activităților specifice cu resurse limitate, ca suport operațional, luarea de decizii strategice sau furnizarea de avertismente diverșilor beneficiari legali. În acest sens, mi se pare sugestiv exemplul unei entități implicată în colectarea datelor și oferirea unor analize predictive asupra evoluțiilor înregistrate în interiorul unei entități teroriste sau actor *proxy* utilizat în realizarea campaniilor de dezinformare, intuirea fragmentărilor și crearea de politici menite să reducă atacurile. Spre exemplu, INSIKT Intelligence, start-up tehnologic activ în domeniul de interes, utilizează diferite modele de învățare automată pentru a detecta potențialele amenințări online prin tehnici SNA (Social Network Analysis) și NLP (Natural Language Processing) efectuate pe conținut provenit din surse deschise, existent pe rețelele sociale și alte surse. În acest exemplu, perspectivele derivate, urmare a analizei textului și rețelei, sunt valorificate pentru identificarea conținutului periculos ori cu potențial periculos, corespunzător, a potențialelor amenințări, sau pentru a prescrie modele de relații între indivizi sau organizații. Folosind SNA, INSIKT are capacitatea de a evalua activitatea unui grup de utilizatori dintr-o rețea, determinând nodurile de influență și nivelurile sau eficacitatea difuzării, prin aceste rețele, a informațiilor, spre exemplu, din zona propagandei. Cu ajutorul surselor deschise analiza permite structurilor specializate ale statului utilizarea *big data*, odată cu un mai bun management al resurselor limitate, în funcție de potențiala amenințare, acțiunea de anonimizare sau pseudonimizarea datelor îmbunătățind conformitatea cu principiile de protecție a datelor cu caracter personal.

Un alt exemplu este utilizarea Sistemului de detectare și alertă timpurie în timp real, finanțat de Uniunea Europeană (UE) pentru conținutul terorist online (*RED-Alert*)

Proiectul reprezintă exemplul de instrument care urmărește detectarea stadiilor incipiente ale fenomenului radicalizării, concomitent, încercând asigurarea unei ridicate confidențialități și standarde de securitate. RED-Alert utilizează procesarea prin tehnici de SNA (*Social Network Analysis*) și NLP (*Natural Language Processing*), alături de evenimente complexe, pentru a colecta, procesa, vizualiza și stoca date online legate de grupurile teroriste, inclusiv stadiile incipiente ale radicalizării bazate pe conținutul rețelelor sociale.

Instrumentul este utilizat în căutarea cuvintelor-cheie sau subiectelor cunoscute în conținut, care nu au fost încă identificat ca relevante. În plus, instrumentul include un proces de anonimizare și de-anonimizare a datelor care se adaptează la organizații, activitatea organelor specializate, ceea ce poate constitui ceva promițător și pentru alte domenii care se ocupă cu managementul datelor sensibile.

Proiectul RED-Alert, încheiat la finele anului 2020, a oferit o nouă viziune a instrumentelor folosite pentru gestionarea și contribuția la răspunsul juridic oferit de state, în legătură cu amenințările asimetrice din prezent. În ciuda acestui fapt, este important de reținut că platforma a fost utilizată doar într-o fază de testare și, prin urmare, operabilitatea sa, în afara mediilor de testare, rămâne a fi stabilită.

Un alt exmplu este legala utilizare a unui start-up tehnologic, denumit Moonshot, dezvoltat în Marea Britanie, specializat în combaterea extremismului violent și al identificării persoanelor vulnerabile la radicalizare. Similar unei „red alert", Moonshot își propune să identifice persoanele predispuse la radicalizarea online, încercând să le pună în contact prin transmiterea unor „mesaje pozitive".

4. Amenințările hibride în scopuri strategice

Deși fenomenul dezinformării nu este nou, capacitatea de răspândire a unui conținut constituit din „știri sau informații false", este fără precedent. Este cunoscut faptul că fabricarea sau denaturarea informației nu este circumscrisă neapărat zonei sancționatorii, însă poate fi cu siguranță dăunătoare și are potențialul de a contribui la răspândirea diferitelor tipuri de conținuturi în *discursul mainstream*.

În timpul „operațiunii militare speciale" din Ucraina, derulată de forțele armate ale statului invadator, entități *proxy*, afiliate acestuia au creat și amplificat, la scară largă, mai multe conținuturi înșelătoare, profitând de vulnerabilitatea ecosistemului rețelelor sociale și prin manipularea oamenilor, propunându-le narative conspiraționiste și știri false, menite să asigure subminarrea încrederii în guvernul statului ocupat, simultan, consolidându-și narațiunile referitoare la necesarea trecere de partea noilor autorități din teritoriile ocupate, implicit, față de strategiile de recrutare a noilor suporteri.

Efectivitatea utilizării inteligenței artificiale în combaterea amenințărilor hibride și a celor asimetrice în spațiul online este dovedită, mai ales, când se face referi la indivizi și grupuri expuse riscului. Cu toate acestea, instrumentele utilizate nu pot fi decât o parte a soluției, activitate de colectare și analiză a datelor și informațiilor, inteligența artificială având calitatea de a sprijini la conectarea punctelor, contracararea, cu adevărat, a narativelor asociate acestor zone necesitând însă o *înțelegere mult mai nuanțată* a căilor indivizilor către o atitudine sau criminal, pe care astfel de instrumente și le pot permite. Mai mult, rolul important al organizațiilor societății civile și al unor astfel de inițiative, în aceste procese, nu poate fi ignorat.

5. Respectarea drepturilor și libertăților fundamentale - între permisivități și limite

Principala preocupare legată de utilizarea inteligenței artificiale în complexul proces de instrumentare a unei amenințări hibride și asimetrice este cea legată de potențialul de implementare a acestor tehnologii, prin raportare la drepturile și libertățile fundamentale ale persoanei. Prin forța normativă a documentelor juridice ale Adunării Generale a Națiunilor, s-a statuat faptul că statele au obligația respectării și îndeplinirii garanțiilor referitoare la respectarea drepturilor omului, respectiv să protejeze persoanele împotriva abuzurilor comise de actori statali și non-statali, în contextul combaterii acestor forme de manifestare a criminalității. De asemenea, prin rezoluție, Consiliul pentru Drepturile Omului și-a reafirmat promovarea, protecția și exercitarea drepturilor omului în spațiul virtual, afirmând că exercițiul respectării drepturilor omului se aplică online la fel de mult ca și offline. Structurile statului cu rol în combaterea activă a amenințărilor hibride și asimetrice urmăresc explorarea capacităților inteligenței artificiale, fapt care implică o necesară și legitimă asigurare că această activitate este realizată cu respectarea drepturilor și libertăților omului și cu cea a garanțiilor procesuale. Pe lângă necesitatea abținerii de la utilizarea inteligenței artificiale într-o manieră aparent ilegală, cum ar fi implementarea supravegherii, dincolo de ceea ce este necesar și proporțional pentru un scop legitim, autoritățile trebuie să ia în considerare alte pericole mai puțin vizibile, cum ar fi potențialul de utilizare a algoritmilor de învățare automată, pentru a amesteca rezultate subiective prin procese automate, prin urmare, pentru a produce rezultate discriminatorii, în fapt, care să conducă la afectarea dreptului la intimitate, libertatea de gândire și de exprimare și nediscriminare.

În acest context, Rezoluția 68/167 a Adunării Generale a Națiunilor referitoare la dreptul la viață privată în era digitală reține activitatea de „colectare ilegală sau arbitrară de date cu

caracter personal", drept act extrem de intruziv, cu încălcarea dreptului la viață privată și libertatea expresie, intrând în contradicție cu principiile unei societăți democratice. În plus, datele introduse în algoritmi pot, adesea, contamina cu părtiniri umane, iar implementarea acestor modele poate genera amplificarea părtinirilor, afectând dreptul la nediscriminare.

Cu toate acestea, spre șansa științei, în mod fericit, nu toate tehnologiile proprii inteligenței artificiale prezintă un risc similar pentru drepturile omului. Bunăoară, dreptul la intimitate, la libertatea de gândire și de exprimare, și cel de nediscriminare, sunt prevăzute în Declarația Universală a Drepturilor Omului precum și în diferite tratate internaționale și regionale, inclusiv Pactul internațional cu privire la drepturile civile și politice, ratificat de România, prin Decretul nr. 212 din 31 octombrie 1974.

Este încă un solid argument de ordin juridic prin care statului - prin instituțiile cu atribuții în domeniu - i se solicită, în mod constituțional și democratic, grijă deosebită față de potențialul pericol de încălcare și afectare a altor drepturi ale omului, prin discreționara și abuziva utilizare a instrumentelor inteligenței artificiale, în procesul de combatere a amenințărilor hibride și asimetrice, referindu-mă, îndeosebi la dreptul la un proces echitabil și prezumția de nevinovăție, prin vulnerabilizarea procesului de utilizare a probelor generate de inteligența artificială, care poate fi dificil de contestat în instanță.

În general, limitările drepturilor omului, prevăzute în Pactul internațional cu privire la drepturile civile și politice - inclusiv viața privată, libertatea de exprimare și nediscriminarea - sunt permise doar atunci când astfel de limitări sunt expres stabilite în lege, sub o necesară, legală și proporțională utilitate, pentru atingerea unui scop legitim. După cum este descris în raportul fostului raportor special pentru promovarea și protecția dreptului la libertate de opinie și exprimare, Frank La Rue, dreptul la viață privată protejează „sfera privată" a fiecărui individ, o „zonă a dezvoltării autonome, interacțiunii și libertății", unde sunt protejate „de intervenția statului și de intervenție excesivă nesolicitată a altor indivizi neinvitați"[1]. În spiritul acestor idei, dreptul la intimitate implică, în mod corespunzător, „capacitatea persoanelor de a determina cine deține informații despre ei și cum sunt utilizate acele informații".

Pentru a da substanță dreptului la confidențialitate într-un ev din ce în ce mai „digital", zonele de confidențialitate a datelor au fost aprobate la nivel internațional, unional și național, astfel, multe state adoptând legi privind protecția datelor cu caracter personal. Așa după cum este reținut din textul Raportului Înaltului Comisar al Națiunilor Unite pentru Drepturile Omului privind dreptul la confidențialitate în era digitală, în timp ce legile și alte normative diferă în conținut, cele mai multe dintre ele urmează un *corpus* comun de principii, inclusiv acela conform căruia prelucrarea datelor cu caracter personal ar trebui să fie „corectă, legală și transparentă", precum și limitată la ceea ce este „necesar și proporțional cu un scop legitim", cu sublinierea unei potențiale și necesare observații, conform căreia, tehnici precum anonimizarea datelor, ar trebui implementate, similar, cea a pseudonimizării.

Instrumentele de inteligență artificială care implică colectarea în masă a datelor personale nețintite riscă, într-o manieră inerentă, să dezvolte un caracter intruziv la nivelul vieții private. Este, de asemenea, situația investigațiilor derulate în cazurile în care securitatea - fie că este națională, unională sau internațională, este adusă într-o stare de pericol, când, potrivit unor reguli instituite (unul din exemple fiind cel al Manualului ONUCT și INTERPOL privind investigațiile online împotriva terorismului), este inserat că activitatea de „colectare masivă, nețintită și nediscriminată de date este puțin probabil să îndeplinească cerințele de necesitate și proporționalitate. În mod similar, reținerea datelor, mai mult decât este necesar, poate aduce încălcare drepturilor universale ale omului sau protecția legală a datelor". Este încă un

[1] Pe larg în raportul elaborat în cadrul Adunării Generale a ONU, de Frank La Rue, intitulat „Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue", 17.04.2013 (*https://www.ohchr.org/sites/default/files/Documents/HRBodies/HRCouncil/RegularSession/Session23/A.HRC.23.40_EN.pdf*, accesare 02.12.2023).

temeinic motiv pentru care susțin că legislația specifică în domeniul reținerii datelor cu caracter personal ar trebui să includă detalii normative referitoare la scopul pentru care sunt colectate datele, modul în care sunt utilizate, cine are acces la date, scopul sau scopurile pentru care pot fi utilizate și durata de timp în care acestea pot fi stocate, pentru stricte rațiuni de aplicare a legii.

Dintr-o altă postură a dezbaterii, pot fi reținute contra-argumentele care aduc în discuție problema „profilării algoritmice", apreciată mult mai intruzivă decât profilarea umană, și, prin urmare, care aduce o stare accentuată de discriminare în zona drepturilor și libertăților fundamentale ale omului. Totodată, este de subliniat faptul că, în general, colectarea datelor online în masă, pentru obținerea informațiilor dezvoltă riscul ca, în mod substanțial, să contribuie la degradarea relației cetățean-stat, prin caracterul opozabil esenței unui raport general de încredere, contribuind, astfel, la construcția unei imagini deformate a înțelesului aplicării anumitor legi, în detrimentul respectării normelor fundamentale. În concret, consider că o intruziune atribuită statului, constând în activitatea de monitorizare a platformelor online, poate atașa unui stat inclusiv calitatea de „stat digital autoritar"[1]. Atât tipul sau forma tehnologiei utilizate, cât și procesul efectiv de colectare și stocarea necesară a datelor private sau cu potențial de a constitui date cu caracter privat, generează implicații juridice diferite și semnificative asupra dreptului la viață privată. Instrumente automate care sprijină aplicarea legii în analiza legală a datelor colectate și găsirea de modele sau potrivirea fețelor de la un suspect cu date provenite din surse deschise sau colectate în alt mod legal din conturile de rețele sociale, trebuie să fie diferențiate de tehnologiile care urmăresc să monitorizeze rețelele sociale și alte surse online în timp real pentru a identifica piste relevante pentru operațiunile hibride ori în paleta amenințărilor asimetrice.

Cred însă, că starea de securitate națională a unui stat, împreună cu rigoarea măsurilor dispuse în temeiul legii, în oricare sistem de drept, nu poate exclude faptul ca statul să nu poată, în mod legal și temporar, limita libertatea „exterioară" a propriilor cetățeni în exprimarea convingerilor sau de a le pune în aplicare, în anumite circumstanțe, inclusiv prin soluții de inteligență artificială, indiferent de forma sub care informația este transmisă. De aceea, o clarificare a ceea ce înseamnă „conținut ilegal", în comparație cu un „conținut legal", se impune, în mod cert. Și pentru a oferi un simplu exemplu, spun că Tech Against Terrorism (o inițiativă a Direcției executive a Comitetului de combatere a terorismului al Națiunilor Unite), a solicitat factorilor de decizie oferirea unor necesare și clare reglementări referitoare la înțelesul termenului „conținut ilegal", în context, solicitând promovarea modalității de acțiune în legătură cu acest aspect, cu evitarea eliminării conținutului protejat prin libertatea de exprimare. Însă, aici, sub proprie rezervă, subliniez faptul că elementele interesate aleg, tot mai frecvent, comunicarea prin platforme mai mici, utilizând un mediu divers al serviciilor online, de la stocare în *cloud*[2], la servicii de mesagerie criptate (ex. *WhatsApp*, *Telegram*, *Signal* etc.) pentru a ocoli impedimentele normative, implicit eliminarea conținutului rău intenționat de pe platformele online, cu o mai mare întindere.

Lipsa persistentă a unor definiții universal acceptate atât în privința amenințării hibride, cât și în cea a amenințării asimetrice (așa cum este și cea a terorismului, unde autorul a manifestat constanță în identificarea conținutului ideal, aplicabil tuturor sistemelor de drept), rămâne un semnificativ obstacol pentru democrația statelor și completitudinea dreptului, precum și pentru diferitele entități, și reflectă tensiunea dintre necesitatea de a asigura moderarea și impunefrea unui conținut legal și dreptul la libertatea de exprimare. Dreptul la libertatea de gândire, în plinătatea dimensiunii „interne", devine drept absolut, ce nu poate fi limitat sau care nu poate reține, în vreo împrejurare, intervenția statului, fapt deosebit de

[1] Expresia aparține autorului Boaz Ganor, evidențiată în lucrarea „Artificial or Human: A New Era of Counterterrorism Intelligence?, publicată în seria *Studies in Conflict & Terrorism*, Edit Routledge Tailor & Francis Group, Florida, 2019, p. 5.

[2] *Cloud*-ul este format din servere din centrele de date din întreaga lume.

relevant de remarcat în situația evaluării potențialului unor tehnologii, inclusiv a celor bazate pe inteligența artificială, cu unic scop, de influențare a gândurilor și deciziilor unei persoane.

Altfel spus, implementarea oricărei aplicații automate pentru contracararea utilizării amenințărilor hibride și a celor asimetrice, într-o eră digitală, prin maniera de monitorizare a conținutului generat de utilizatori online, rămâne în siajul unui rezultat socialmente periculos, ca o consecință juridică a încălcării libertății de gândire, prin faptul că poate genera acțiuni (acte, fapte) bazate pe un comportament viciat, profund subiectiv, atribuit unui persoanei prezente în mediul virtual, în fapt, nimic altceva decât emergențe ale inteligenței artificiale, în condițiile unei constante interpretări instrumentalizate a activității virtuale, apreciind-o drept un *trigger* al unui gând interior, într-un prezumat proces de indicare, fie a unei persoane, fie a ceea ce reprezintă, prin imaginea unui risc de securitate, motiv pentru a permite intervenția legală a instituțiilor statului pentru oprirea transformării unui gând, într-un act sau faptă cu caracter penal.

În mod similar, opinez că toate instituțiile de forță, cu atribuții de monitorizare a tehnologiilor bazate pe inteligența artificială pentru utilizatorii direcți expuși riscului de radicalizare la conținutul contra-narativ, ar trebui să nu „lase garda jos" și să nu ia în considerare posibilitatea ca astfel de tehnologii să poată avea, ca rezultat, ilegala interferență cu dreptul la libertatea de gândire prin manipularea modului de acțiune a utilizatorilor, așa după cum am precizat, sub garanția statului de drept conform căreia *dreptul la nediscriminare este garantat*, astfel că o persoană va fi tratată în afara criteriilor de rasă, sex, origine etnică sau religie, cu excepția faptului când tratamentul diferențiat este justificat pentru un scop legitim și limitativ, motivat în fapt și în drept, scop legal satisfăcut prin mijloace aprobate, derulate în mod necesar și proporțional.

6. Inteligența artificială, în complexul exercițiu al fenomenului juridic

Deși, în principiu, există mai multe cazuri de utilizare a instrumentelor digitale care pot fi relevante pentru serviciile de informații, utilitatea practică a oricărui astfel de caz de utilizare fiind nemijlocit legată de capacitatea acesteia de a contribui la urmărirea penală în fața unei instanțe. În condițiile în care acțiunile întreprinse pe baza tiparelor și corelațiilor identificate de sistemele de inteligență artificială nu sunt considerate de natură probatorie, prezumatul benefici al utilizării instrumentelor de inteligență artificială este limitat de la perspectiva utilizatorilor finali.

Probele obținute prin activități specifice inteligenței artificiale rămân susceptibile de a fi modificate, fie intenționat, fie neintenționat. Mai mult, preocupările privind drepturile fundamentale sunt de natură a afecta proporționalitatea acestor tipuri de probe utilizate în cadrul unui proces penal.

În concluzie, avantajele utilizării inteligenței artificiale, ca parte a epocii digitale pentru interesele securității și justiției, alături de valoarea probantă a probelor obținute din utilizarea acestui instrument, poate să nu justifice riscurile pentru drepturile omului pe care le prezintă utilizarea de către serviciile de informații și instituțiile de aplicare a legii, implicațiile utilizării acestui tip de instrumente pentru colectarea datelor și informațiilor, respectiv de a asigura sau a contribui la asigurarea probatoriului, este mai mult decât probabil să se confrunte cu provocări și critici, îndeosebi la nivel procedural, în cadrul activității diverselor tipuri de instanță. De aceea, consider că, proporțional cu prezumata utilitate a inteligenței artificiale, este esențial ca statele să genereze îndrumări adecvate și suficiente referitoare la situațiile de admisibilitate a probelor obținute prin sau cu instrumente de inteligență artificială, evaluându-se, neîntârziat, impactul și rezultatele acestor tipuri de probe, prin stricta raportare la garantarea respectării drepturilor omului, în general, a statului de drept. Altfel, evaluarea riscurilor reținute în legătură cu seria rigorilor care trebuie îndeplinite de instituțiile competente, referitoare la preocupările în legătură cu acuratețea evaluării riscurilor trebuie clarificate, astfel încât menținerea prezumției de nevinovăție să se bucure de efectivitate.

Trebuie menționat faptul că, în urmă cu doi ani (aprilie 2021), Comisia Europeană a prezentat o propunere de regulament care stabilește norme armonizate privind inteligența artificială care, în condițiile adoptării de către Parlamentul European și de Consiliul UE, vor deveni primul cadru juridic supranațional referitor la acest instrument de obținere a datelor. Mai trebuie spus că actualul proiect stabilește că regulile se aplică atât furnizorilor, cât și utilizatorilor de sisteme de inteligență artificială, chiar dacă aceștia sunt regăsiți în afara spațiului unional, atâta timp cât sistemele sau rezultatele lor sunt utilizate în arealul unional, în acest sens, deși vorbim despre un proiect al Uniunii, constituind reper la nivel internațional.

O concluzie importantă din substanța acestui proiect este abordarea sa centrată pe respectarea drepturilor omului, pentru clasificarea sistemelor de inteligență artificială în categorii: „inacceptabil", „ridicat" sau de „risc scăzut", prin raportarea acestor „calificative" la caracterul textului, prin raportare la garantarea drepturilor și libertăților fundamentale ale omului, una din probleme fiind cea a expertizării tehnice, obligatorii, în această situație juridică, un demers obligatoriu pentru dezvoltarea și întreținerea oricărei aplicații din zona inteligenței artificiale, astfel, care să conducă la menținerea unui înalt nivel de încredere la nivelul instituțiilor specializate ale statului, ale organelor de aplicare a legii, deopotrivă, la nivelul societății civile. Astfel, corectitudinea în inteligența artificială devine obiectiv declarat și asumat în părți extinse ale industriei tehnologice, la nivelul diverselor politici, în mediul academic și la nivelul societății civile, respectiv unul al principiilor-cheie promovate, în raport cu utilizarea responsabilă a inteligenței artificiale, dar și a oricărui alt instrument juridic, specific erei digitale, care implică faptul că deciziile și rezultatele acestui instrument nu vor fi menite să creeze un impact discriminatoriu sau nedrept asupra utilizatorilor finali[1].

7. Considerații finale

Importanța utilizării instrumentelor de inteligență artificială în cadul înfăptuirii dreptului rămâne cu un potențial considerabil de a contribui la combaterea amenințărilor hibride cât și a celor asimetrice. De asemenea, poate fi de utilitate în suportul acordat diverselor instituții cu atribuții în asigurarea securității și a aplicării legii, prin faptul că pot avea capabilitatea gestionării unor semnificative cantități de date colectate prin vizualizarea și interpretarea rezultatelor, extragerea tiparelor, semnalarea sau avertizarea timpurie a diferitelor categori de riscuri și amenințări, precum și orice aspecte care țin de evoluția informațională, putând concura la identificarea și stabilirea anumitor modele predictive, pentru sancționarea unor

[1] **Unul din celebrele exemple relevă concluziile unei investigații realizate de o redacție independentă (ProPublica), prin care s-a demonstrat că algoritmul utilizat de magistrații și ofițerii de eliberare condiționată din Statele Unite pentru evaluarea probabilității unui inculpat de a recidiva a fost părtinitor, în raport cu anumite grupuri rasiale. În urma evaluării instrumentului s-a constatat că inculpații afro-americani au fost, în mod incorect, apreciați mai probabil de a fi considerați expuși unui risc mai ridicat al recidivei, decât inculpații caucazieni. În concret, au fost înregistrate considerabil mai multe valori fals pozitive în rândul comunității afro-americane, decât în rândul inculpaților caucazieni, astfel, acuzații americani fiind incorect marcați cu un risc scăzut, ceea ce înseamnă că rata fals-negativă a fost recurent mai mare în comunitatea caucaziană, creându-se un tratament diferențiat în rândul celor două grupuri (cazul COMPAS - Correctional Offender Management Profiling for Alternative Sanctions - relevat, pe larg în articolul autorilor Jeff Larson, Surya Mattu, Lauren Kirchner and Julia Angwin intitulat „How We Analyzed the COMPAS Recidivism Algorithm", 2019, regăsit la adresa electronică** https://www.propublica.org/article/how-we-analyzed-the-compas-recidivism-algorithm**, accesare 04.12.2023).**

asemenea fapte, respectiv să contribuie la tragerea la răspundere penală, fie că vorbim despre subiecți activi state dar și alte categorii de persoane juridice sau persoane fizice.

Apreciez că o încredere totală în efectele și produsele rezultat al inteligenței artificiale este și trebuie să fie exclusă, însă, în mod obligatoriu, una, parțială, este de utilitate concretă. Chiar în contextul unui acceptat progres tehnologic, pe întreg palierul erei digitale (inclusiv în domeniul inteligenței artificiale) consider că precizări pentru serviciile de informații și instituțiile de aplicare a legii referitoare la cadrul normativ aplicabil, precum și cu referire la importanța, locul și, mai ales, gradul, respectiv nivelul de utilitate procedurală a acestor date, în cadrul instrumentării acestor două tipuri de amenințări, sunt obligatorii, fie că vorbim de informații clasificate sau informații neclasificate, provenite din surse deschise ori oficiale.

Eforturile autorităților în stabilirea utilității acestor date trebuie să includă, în mod continuu și obligatoriu, aportul cercetării științifice juridice, direcționate, cu deosebire, înspre stabilirea precisă a utilității, legalității, dar, mai ales, a întinderii, în timp și spațiu, a colectării efective a datelor.

Din perspectiva unională, abordarea amenințărilor hibride și a celor asimetrice, ar trebui să fie un proces continuu, prin care dezvoltarea rezilienței la nivel societal, național și european, să joace un rol cheie, un model de pregătire preemptivă bazată pe noțiunile de „întreaga societate" și „reziliență[1] societală", tetrmeni care au câștigat tot mai mult teren în activitatea politică a UE[2].

În plan internațional, normativul internațional și politicile ar trebui puse într-un *acord normativ efectiv*, primordial, urmărindu-se definiția instituției inteligenței artificiale, în care să fie prezentă, explicativ, de o manieră accesibilă, utilitatea combaterii amenințărilor hibride și a celor asimetrice, printre altele, din rațiunea evitării riscului unei utilizări greșite a acestor instrumente (cu rea credință sau nu) cm ar fi, de exemplu, persecutarea diverselor entități, a jurnalismului, și pentru a minimiza riscul deformării funcției normative, sub forța controlului democratic, primordial, din perspectiva impactului asupra drepturilor și libertăților omului, cu efecte definitive asupra democrației înseși.

Bibliografie selectivă

Ganor, Boaz „Artificial or Human: A New Era of Counterterrorism Intelligence?, publicată în seria *Studies in Conflict & Terrorism*, Editura Routledge Tailor & Francis Group, Florida, 2019.

Countering Terrorism Online With Artificial Intelligence. An overview for Law Enforcement and Counter-Terrorism Agencies in South Asia and South-East Asia, 2021.

[1] În filosofia conceptuală a Uniunii Europene, conceptul de „reziliență" reprezintă „capacitatea unui individ, a unei gospodării, a unei comunități, a unei țări sau a unei regiuni de a rezista, de a face față, de a se adapta și de a se recupera rapid după stres și șocuri precum violența, conflictul, seceta și alte dezastre naturale, fără a compromite dezvoltarea pe termen lung". În documente programatice și declarative, NATO delimitează reziliența ca referindu-se la o „combinație a pregătirii civile și a capacității militare" în care pregătirea civilă este descrisă ca fiind compusă din „toate măsurile și mijloacele luate în timp de pace, de agențiile naționale și aliate, pentru a permite unei națiuni să supraviețuiască unui atac inamic și să contribuie mai eficient la efortul de război comun". Amândouă abordările înțeleg cooperarea civil-militară ca fiind esențială pentru a face față oricărui tip de criză. Deși consolidarea rezilienței prin elaborarea și implementarea comună, civil-militară, de politici de pregătire, prevenție, protecție este obligatorie pentru asigurarea succesului în fața stresurilor interne și externe de toate tipurile, un alt palier este esențial în dezvoltarea unei rezilienței sustenabile: unitatea de efort cu statele partenere, asigurată prin implicarea acestora în atingerea deziderateloș și prin transferul de expertiză în combaterea amenințărilor. Pe larg în articolul lui Rufin Zanfir, intitulat „Reziliența în fața amenințărilor de tip hibrid. Un „sport de echipă" în care nimeni nu trebuie lăsat în urmă", 07.06.2022, disponibil pe platforma E-Arc (*https://e-arc.ro/2022/06/07/rezilienta-in-fata-amenintarilor-de-tip-hibrid-un-sport-de-echipa-in-care-nimeni-nu-trebuie-lasat-in-urma/#_ftnref12*, accesare 02.12.2023).

[2] În articolul „Best Practices in the whole-of-society approach in countering hybrid threats", prezent în format electronic, la adresa *https://www.europarl.europa.eu/RegData/etudes/STUD/2021/653632/EXPO_STU(2021)653632_EN.pdf* (accesare 03.12.2023).

Smolic, Hrvoje, „What is Predictive Analytics? A Definition and Overview", articol în platforma *Graphite*, 31.10.2023.

La Rue, Frank, „Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue" raport în cadrul Adunării Generale a ONU/ report to the UN General Assembly, 17.04.2013.

Kolodziej, Mchael L. „Commentary The Asymmetric Threat".

Văduva, Ghe. „Amenințări asimetrice sau amenințări hibride: delimitări conceptuale pentru fundamentarea securității și apărării naționale/ Asymmetric threats or hybrid threats: conceptual delimitations for the foundation of national security and defense", Universitatea Națională de Apărare „Carol I", București, 2013.

Larson, Jeff, Mattu, Kirchner, Surya Lauren, Angwin, Julia, „How We Analyzed the COMPAS Recidivism Algorithm", 2019.

Zanfir, Rufin, „Reziliența în fața amenințărilor de tip hibrid. Un „sport de echipă" în care nimeni nu trebuie lăsat în urmă/ Resilience to hybrid threats. A "team sport" where no one should be left behind", articol, platforma E-Arc, 07.06.2022.

*** „Best Practices in the whole-of-society approach in countering hybrid threats", study conducted by the European Parliament (Think Tank), 2021.

Cilevičs, Boriss, „Legal challenges related to hybrid war and human rights obligations", propunere de rezoluție a Adunării Parlamentare a Consiliului Europei/ motion for a resolution of the Parliamentary Assembly of the Council of Europe (Doc. nr. 14523 din 6 aprilie 2018).

(*https://ec.europa.eu/commission/presscorner/detail/it/MEMO_16_1250*.

(*https://assembly.coe.int/nw/xml/XRef/Xref-XML2HTML-en.asp?fileid=24547&lang=en*).

(*https://www.sciencedirect.com/topics/social-sciences/artificial-intelligence*.

https://m247.com/ro-ro/servicii/protectie-ddos-administrata/?gad_source=1&gclid=Cj0KCQiAyKurBhD5ARIsALamXaHG7AVW9Pm7T1t07g3kVmsR8maB89rnYIfvUIvuqK-ykgRzZqft7toaAlY0EALw_wcB,.

https://www.ohchr.org/sites/default/files/Documents/HRBodies/HRCouncil/RegularSession/Session23/A.HRC.23.40_EN.pdf.

https://graphite-note.com/what-is-predictive-analytics-a-definition-and-overvie.

https://www.propublica.org/article/how-we-analyzed-the-compas-recidivism-algorithm

https://e-arc.ro/2022/06/07/rezilienta-in-fata-amenintarilor-de-tip-hibrid-un-sport-de-echipa-in-care-nimeni-nu-trebuie-lasat-in-urma/#_ftnref12.

https://www.europarl.europa.eu/RegData/etudes/STUD/2021/653632/EXPO_STU(2021)653632_EN.pdf.

https://assembly.coe.int/nw/xml/XRef/Xref-XML2HTML-en.asp?fileid=24547&lang=en.

https://assembly.coe.int/nw/xml/XRef/Xref-XML2HTML-en.asp?fileid=24547&lang=en.

https://cssas.unap.ro/ro/pdf_studii/amenintari_asimetrice_sau_amenintari_hibride.pdf