10.12753/2065-8281-20-32

ACTUALIZAREA LEGISLAȚIEI DIN DOMENIUL SECURITĂȚII NAȚIONALE – ADAPTAREA LA NOILE REALITĂȚI. NECESITATE ȘI PROVOCĂRI

UPDATE OF LEGISLATION IN THE FIELD OF NATIONAL SECURITY – ADAPTING TO THE NEW REALITIES. NEEDS AND CHALLENGES

MISE À JOUR DE LA LÉGISLATION NATIONALE DE SÉCURITÉ – ADAPTATION AUX NOUVELLES RÉALITÉS. EXIGENCE ET DÉFIS

Georgian POP*

Legislația românească din domeniul securității naționale este, în bună măsură, învechită. Legile au fost elaborate în anii ’90 și sunt tributare logicii specifice Războiului Rece. Între timp, atât criza generată de COVID-19, cât și evoluțiile tehnologice și geopolitice din ultimele decenii au relevat necesitatea adaptării legilor la noile realități. Față de acum trei decenii, au apărut riscuri de securitate noi, cum sunt riscurile cyber, de pildă. Noua Strategie de Apărare a Țării (din 2020) relevă necesitatea actualizării acestor legi.

Marea provocare pentru demersul legislativ constă în găsirea echilibrului corect dintre nevoia de a preveni/contracara aceste riscuri, pe de o parte, și, pe de altă parte, necesitatea de a proteja libertățile fundamentale și de a asigura respectarea drepturilor constituționale ale cetățenilor. Lipsa acestui echilibru poate să deschidă calea fie înspre abuzuri împotriva cetățenilor, fie înspre ineficiență instituțională. Consolidarea democrației și a statului de drept sunt legate, în bună măsură, de conținutul acestor legi.

Pentru a avea o legislație modernă și adecvată climatului democratic, principiul constituționalității (protejarea libertăților și a drepturilor fundamentale) trebuie să fie baza procesului de reglementare juridică a noilor riscuri de securitate.

Romanian legislation specific to the national security is, at a great extent, quite obsolete. The laws were established in the 90s’ and are submitted to the logic specific to the Cold War. In the meantime, not only the crisis generated by COVID – 19 but also the technological and geopolitical evolutions appeared during the latest decades have emphasized the need to adapt the laws to the new realities. Comparing the situation specific to the three decades before, new security risks have shown up, for example cyber risks. The New Defence Strategy of our country (the one of 2020), emphasizes the keen need to update these laws.

The great challenge for the legislative initiative consists in finding a right balance between the need to prevent/counteract these risks, on the one hand, and, on the other hand, the need to protect the fundamental freedom and to assure the care to respect the constitutional rights of the citizens. The lack of this balance can open the way either towards abuse against the citizens or towards institutional inefficiency. Consolidation of democracy and state are dependent, greatly, on the content of these laws.

To have a legislation modern and adequate, adapted to the democratic environment, the principle of constitutionality (namely to protect the freedom and fundamental rights), must be the base of the legally regulation specific to new security risks.

La législation roumaine dans le domaine de la sécurité nationale est dans une grande mesure périmée. Les lois ont été élaborées dans les années ’90 et sont basées sur la logique de la guerre froide. Pendant ce temps, la crise générée par le COVID-19, ainsi que les développements technologiques et géopolitiques des dernières décennies ont mis en évidence la nécessité d’une adaptation des lois aux nouvelles réalités. Au cours de trois décennies, de nouveaux risques de sécurité sont apparus, tels que les cyber-risques, par exemple. La stratégie de défense du pays (de 2020) montre la nécessité de mettre à jour toutes ces lois.

Le grand défi de l’approche législative est de trouver un équilibre entre la nécessité de prévenir/contrer ces risques, d’une part, et la nécessité de protéger les libertés fondamentales et de garantir le respect des droits constitutionnels des citoyens, d’autre part. Le manque de cet équilibre peut ouvrir la voie soit à des abus contre les citoyens, soit à une inefficacité institutionnelle.

Afin d’avoir une législation moderne adaptée au climat démocratique, le principe de constitutionnalité (protection des libertés et des droits fondamentaux) doit être le fondement du processus de réglementation juridique des nouveaux risques pour la sécurité.

Cuvinte-cheie: securitate; legislație; riscuri; provocări; adaptare.
Keywords: *security; legislation; risks; challenges; adaptation.*
Mots-clés: *sécurité; législation; risques; défis; adaptation.*

**** Deputat în Parlamentul României***
e-mail: *georgianpop75@gmail.com*

O analiză a factorilor care au determinat, de-a lungul timpului, modificarea și îmbunătățirea legislației reprezintă o călătorie fascinantă în istoria universală. Dacă în teoria și practica legislativă anumite concepte și principii au rămas valide din Antichitate până în prezent, conținutul efectiv al legilor a cunoscut, în fiecare etapă istorică, modificări consistente.

Cu viteze mai mari sau mai mici, războiul și pacea, crizele pe care le-a traversat umanitatea, descoperirile științifice, invențiile și inovațiile tehnologice, dinamica geopolitică sau evoluțiile sociale au modelat fiecare perioadă istorică. Adaptarea legilor la aceste evoluții a fost, în permanență, atât o necesitate, cât și o provocare pentru legiuitorii din toate timpurile.

În ultimele decenii, evoluțiile tehnologice au fost spectaculoase, influențând economia, industria, politica, cercetarea științifică, divertismentul, stilurile de viață, interacțiunea socială etc.

Acum 30 de ani, de exemplu, consideram *science-fiction* tehnologia *smart phone*, pe care astăzi o folosim, cotidian, într-un mod firesc. Ca efect, ritmul schimbărilor politice, economice și sociale a fost unul accelerat.

În ultimele decenii, dezvoltările tehnologice și dinamica geopolitică au făcut ca riscurile de securitate să devină tot mai complexe. Practic, niciodată în istorie nu au existat asemenea evoluții și provocări, greu de imaginat cu câteva decenii în urmă. Riscurile de tip cyber, utilizarea dronelor pentru a produce incidente de securitate, războiul de tip hibrid și, în general, noile riscuri de tip asimetric nu au fost definite în legislația specifică securității naționale.

Criza generată de COVID-19 a relevat, în plus față de evoluțiile ultimelor decenii, necesitatea actualizării legislației. Tehnologiile inovatoare (roboți, drone, aplicații IT etc.) au facilitat acțiunea umană și, implicit, managementul pandemiei. Prin comparație, acum 100 de ani, în timpul pandemiei reținute de istorie drept „gripa spaniolă”, nimeni nu își putea imagina că roboții pot face dezinfecția în spitale, că dronele pot livra medicamente în zonele de risc pentru oameni, că aplicațiile mobile pot fi utilizate pentru identificarea interacțiunii sociale a persoanelor infectate. Dar, în mod evident, utilizarea noilor tehnologii poate să fie duală, în funcție de intențiile utilizatorului: pe lângă avantaje, noile tehnologii pot fi utilizate pentru limitarea drepturilor și a libertăților fundamentale.

De la salvarea de vieți până la abuzurile împotriva libertăților fundamentale este, în unele cazuri, o linie foarte fragilă, care trebuie reglementată, corect și precis, în legislație. Dacă legile nu sunt suficient de clare, comiterea unor abuzuri intră, în mod indezirabil, în sfera arbitrariului uman.

Necesitatea actualizării legislației

Una dintre marile provocări pentru parlamente, nu doar în România, ci în majoritatea statelor lumii, este legată de adaptarea legislației din domeniul securității la evoluțiile din ultima perioadă, inclusiv la evoluțiile generate de criza COVID-19.

Legislația românească a fost elaborată și adoptată în anii ’90[1]. În linii generale, logica specifică acelei perioade era una de tip „război rece”, principalele riscuri de securitate fiind agresiunea militară, spionajul, terorismul, acțiunile ostile statului, răspândirea de informații false, propaganda pentru război, riscurile de secesiune, diversiunea, atentatele contra ordinii constituționale etc.

Ultimele trei decenii au adus schimbări semnificative. Dacă, de pildă, acum 30 de ani am fi definit o agresiune militară preponderent în termeni convenționali, astăzi o agresiune împotriva unui stat/comunitate poate să fie de tip cyber. Adică, în locul tancurilor clasice, un atac poate fi făcut în mediul virtual, cu arme din arsenalul cyber, care să distrugă sau să paralizeze anumite infrastructuri critice. Efectul produs, politic și militar, este, în majoritatea cazurilor, comparabil cu daunele pe care le produc armele clasice. Spionajul s-a schimbat foarte mult. Dacă în timpul Războiului Rece statele își trimiteau spionii să obțină documente secrete și informații, astăzi se poate face prin instrumente cyber, de la distanță, nu doar prin agenți trimiși la fața locului.

Dacă în anii ’90 potențialii agresori erau, preponderant, entitățile statale sau organizațiile teroriste clar definite, relativ simplu de identificat, astăzi ne confruntăm cu o serie de amenințări difuze, asimetrice, neconvenționale, ai căror autori sunt mai dificil de identificat și contracarat: fabricile/fermele de troli, hackerii, lupii singuratici, care se autoradicalizează pe rețelele de socializare și comit atentate teroriste etc. Pentru aceste noi riscuri, legislația elaborată acum 30 de ani nu prevede definiții și încadrări juridice.

Prevenția este regula de aur a intelligence-ului modern. Să luăm, ca exemplu, spionajul. Prevenția eficientă înseamnă manipularea și deturnarea spionilor unei puteri ostile, pentru a nu reuși să obțină informațiile secrete pe care le vizează sau pentru a nu reuși racolarea/influențarea unor lideri importanți. Dacă s-a produs acțiunea de spionaj/trădare, prevenția a eșuat. Chiar dacă, ulterior, justiția condamnă vinovații, atât spionii, cât și trădătorii, paguba a fost produsă. La fel se întâmplă în cazul atentatelor teroriste. Prevenția înseamnă ca orice tentativă să fie dejucată, blocată, pre-întâmpinată, adică atentatul efectiv să nu se producă, să nu avem victime umane și infrastructuri distruse. Este de preferat ca teroriștii să fie blocați, expulzați, arestați preventiv decât să fie judecați și condamnați după ce au comis atentate, pentru că, în astfel de cazuri, prevenția înseamnă salvare de vieți omenești.

Legislația actuală oferă instrumentele juridice necesare prevenției/contracarării unor riscuri de tip clasic, precum spionajul sau terorismul. Însă nu acoperă noile riscuri, cum sunt „fabricile de troli”, de exemplu, utilizate de o putere ostilă pentru a crea diversiuni și destabilizare.

O simplă lecturare, în anul 2020, a legislației românești din acest domeniu ne relevă faptul că riscurile de securitate au evoluat și s-au diversificat, în timp ce prevederile legislative au rămas în urma acestor evoluții. Legislația perimată, inadecvată reprezintă, intrinsec, o vulnerabilitate, întrucât nu oferă instrumentele juridice pentru prevenirea și contracararea acestor riscuri.

Provocările pentru procesul legislativ

Rolul fundamental al legislației este de a reglementa, în mod adecvat, toate domeniile vieții sociale. Din perspectiva legislației securității naționale, avem, în momentul de față, câteva provocări majore.

O primă provocare vizează dimensiunea exhaustivă a viitorului pachet legislativ, astfel încât să acopere marea diversitate de riscuri survenite în ultimii ani. Este necesară, astfel, o completare a listei riscurilor de securitate națională prin includerea celor survenite în ultimele decenii. Demersul trebuie să fie echilibrat, pentru a evita atât eludarea unor riscuri reale, cât și introducerea abuzivă, forțată a unor riscuri de securitate.

În al doilea rând, o provocare semnificativă asociată legislației din acest domeniu o reprezintă respectarea principiului constituționalității, adică găsirea echilibrului corect dintre, pe de o parte, nevoia de eficiență în asigurarea securității naționale (adică prevenirea riscurilor) și, pe de altă parte, protejarea drepturilor și a libertăților fundamentale ale omului.

Cum elaborăm noua legislație astfel încât să ne permită să exploatăm la maximum avantajele tehnologiei IT&C (legislația să nu fie o frână pentru dezvoltare) și, totodată, să minimizăm riscurile ca aceste tehnologii să fie folosite ca o armă împotriva cetățenilor, comunităților sau statelor? Cum elaborăm noile legi pentru a evita posibilitatea ca, prin intermediul acestor tehnologii, guvernele să-și spioneze în mod ilegitim cetățenii?

În al treilea rând, managementul crizei COVID-19 ne-a relevat posibilitatea, practicată în unele state, ca tehnologii din sfera spionajului, utilizate pentru monitorizare și supraveghere informativă, să poată fi folosite, în numele securității medicale și al stopării răspândirii focarelor, pentru supravegherea în masă a cetățenilor[2], generând, implicit, o imixtiune în sfera dreptului la viață privată.

Provocarea legislativă este extrem de complexă. Este o pandemie un motiv suficient pentru legiferarea utilizării tehnologiilor de supraveghere în masă? Cum ar fi, de pildă, obligativitatea instalării aplicației STOPCOVID pe smartphone-urile personale? Parlamentul Franței a legiferat, în anul 2020, această obligativitate[3].

Care este limita peste care afectarea democrației și a libertăților fundamentale devine ireversibilă? Dacă astfel de aplicații IT sunt aprobate pentru managementul unei pandemii (COVID-19), există rațiuni suficiente pentru extensia utilizării lor în scopul combaterii terorismului, de pildă, a spionajului cibernetic sau a războiului hibrid?

Fără o reglementară clară și responsabilă, putem asista, în viitor, la fenomene extreme, fie neutilizarea optimă a resurselor tehnologice pentru managementul unor riscuri (o pandemie, de exemplu), fie „suprautilizarea” resurselor tehnologice pentru monitorizarea ilegitimă a cetățenilor (de guverne sau de companii private).

COVID-19 și implicațiile în sfera securității naționale

Dacă până la apariția COVID-19 principala paradigmă de abordare a legilor securității naționale căuta echilibrul dintre libertățile civile și securitatea

națională, pandemia a modificat conceptele de referință, discutând, în acest moment, despre găsirea echilibrului dintre sănătatea publică și libertățile fundamentale. În Franța, de pildă, legalizarea folosirii aplicației STOPCOVID pe telefoanele de tip smart este elocventă, pentru relevanța noii paradigme.

O analiză a măsurilor adoptate sau propuse, în diverse state ale lumii, pentru utilizarea tehnologiilor de monitorizare în masă, în scopul managementului pandemiei, ne relevă faptul că provocarea pentru parlamentele naționale este una extrem de complexă.

Conform *Tratatului de funcţionare a UE*, legislația din domeniul securității naționale este un domeniu de suveranitate națională. De aceea, în spațiul UE, fiecare stat va trebui să decidă forma specifică de transpunere în legislație a acestor provocări. De la stat la stat, unele tehnologii vor fi permise, altele interzise. De exemplu, spre deosebire de Franța, în România nu se pune problema legiferării obligativității instalării aplicației STOPCOVID pe telefoanele smart personale.

Pe lângă aplicațiile instalate pe telefoanele smart ale cetățenilor, unele state, sub motivația protejării elevilor, au impus purtarea obligatorie, în școli, a unor brățări electronice, folosite pentru managementul distanțării sociale și pentru a emite avertizări, în cazul în care un elev are febră[4]. În alt stat a fost lansată ideea implantării de cipuri elevilor, motivația fiind protejarea elevilor de pericolul COVID-19[5]. Compania spaniolă Herta Security dezvoltă un sistem complex de recunoaștere facială în spații publice, inclusiv în condițiile purtării unei măști medicale[6]. Compania franceză Outsight dezvoltă un sistem, pe bază de laser, care va permite managementul distanțării sociale în spațiile publice[7]. Dronele sau căștile speciale pe care le poartă polițiștii[8] pot fi echipate cu camere care scanează, în timp real, temperatura oamenilor aflați în spații publice. Unele dintre aceste tehnologii sunt, în diverse state, aprobate prin legislație și aplicate. Altele sunt doar în stadiul de propunere/proiect.

Mai devreme sau mai târziu, parlamentele vor trebui, în fiecare stat, să abordeze aceste subiecte. Provocarea este evidentă. Reglementează sau NU posibilitatea utilizării unor astfel de tehnologii, în scopul managementului pandemiei COVID-19? Dacă da, în ce condiții? Cine gestionează astfel de tehnologii? Cine exercită controlul democratic, astfel încât să nu existe abuzuri sau utilizări ale tehnologiilor în scopuri politice, comerciale etc.? Dacă astfel de tehnologii pot fi utilizate pentru salvarea de vieți în fața pericolului reprezentat de pandemie (COVID-19), ar putea fi folosite aceleași tehnologii pentru salvarea de vieți în fața pericolului terorist? Dar pentru salvarea/protejarea infrastructurilor critice în fața riscurilor de tip cyber sau hibrid? Unde este, în acest caz, echilibrul corect dintre libertate, dreptul la viață privată, pe de o parte, și protejarea sănătății publice sau protejarea vieții cetățenilor, protejarea infrastructurilor critice (sanitare, energetice, de comunicații), pe de altă parte?

O altă temă legată de impactul crizei COVID-19 în sfera securității naționale privește implicarea serviciilor secrete în efortul național de management al unei pandemii. În Israel, de exemplu, serviciile secrete s-au implicat masiv în acțiuni comerciale pentru a aduce, în Israel, milioane de echipamente medicale necesare managementului COVID-19, inclusiv din țări cu care Israelul nu are relații diplomatice[9], serviciile secrete (Mossad) primind felicitări oficiale pentru această implicare[10]. Este legitimă o astfel de implicare? Ce soluție vom stabili în legislația românească? Cine stabilește ce tipuri de implicări comerciale/economice sunt legitime sau ilegitime? Cine controlează posibilele depășiri ale mandatului de securitate națională într-un astfel de caz? Interzicem/păstrăm interdicția ca serviciile secrete să poată desfășura activități comerciale? La toate aceste întrebări, noul pachet legislativ va trebui să găsească răspunsurile corecte.

Un alt subiect de controversă publică a fost legat de informarea de către serviciile secrete a decidenților politici despre pericolele COVID-19. În SUA[11] și în principalele state din UE, s-a degajat, în dezbaterea publică, această temă: Cum stabilim, prin legislație, sarcina serviciilor secrete de a informa, din timp, decidenții politici asupra riscurilor de tip pandemic și cum utilizează decidenții politici informațiile pentru a genera măsurile/politicile publice pentru managementul adecvat al unei pandemii?

Evoluția riscurilor de securitate în ultimele decenii

Pentru că trăim a patra revoluție industrială[12], ba chiar ne aflăm la începuturile celei de-a cincea[13], actualizarea legislației înseamnă, în forma cea mai

simplistă, adaptarea la noua lume definită prin virtual și tehnologie smart.

Pe lângă dezvoltările tehnologice, influențe semnificative asupra noilor riscuri de securitate au avut și evoluțiile geopolitice recente: anexarea Peninsulei Crimeea de către Federația Rusă, evoluțiile politice și militare din Orientul Apropiat sau nordul Africii, presiunile migraționiste asupra UE sau tensiunile latente din Marea Chinei de Sud.

Fără a avea pretenția exhaustivității și fără a încerca să sugerez anumite soluții, am ales, pentru exemplificare, câteva dintre noile riscuri de securitate, încercând să relev provocările de tip legislativ care se asociază fiecăruia dintre aceste noi riscuri.

Războiul de tip hibrid

Acum 30 de ani, discuțiile despre un război de tip hibrid ar fi fost preponderent teoretice. Între timp, după anexarea Crimeii de către Federația Rusă, războiul hibrid a devenit un fenomen politico-militar cât se poate de real. Atacurile de tip hibrid reprezintă o combinație, extrem de eficientă, de atacuri cyber, acțiuni ale unor trupe speciale fără însemne și neasumate de către state (celebrii „omuleți verzi” din Crimeea, de exemplu), propagandă ostilă, campanii fake news, stimularea minorităților sau a grupurilor extremiste dintr-o regiune, pentru a genera instabilitate și a revendica anumite obiective politice, utilizarea pârghiilor energetice și economice etc.

Obiectivele urmărite prin războiul hibrid vizează destabilizarea socială, prăbușirea încrederii populației în autoritățile legitime, tensiunile și conflictele sociale, influențarea masivă a opiniei publice pentru a genera o „paralizare strategică” a decidenților politici, adică incapacitatea de a adopta decizii. Armele utilizate în războaiele hibride nu mai sunt tancurile sau rachetele, ci „armele” cyber, campaniile fake news, propaganda ostilă, pârghiile energetice etc.

În noua legislație a securității naționale și, subsecvent, în capitolul din codul penal care definește infracțiunile la adresa securității naționale, acest fenomen (războiul hibrid) trebuie definit în mod distinct.

Provocările legislative sunt multiple. În primul rând, cum definim dușmanul, în cazul incidentelor de tip hibrid? Mai exact, cum definim, pentru a putea încadra juridic, fenomene, precum propaganda ostilă sau fake news prin social media, coordonate de către o entitate statală ostilă? Cum încadrăm juridic „omuleții verzi”, neasumați de niciun stat, sau mercenarii armatelor/firmelor private[14]? Cum definim juridic „fabricile de troli”, dintr-un alt stat, ca risc pentru securitatea națională? Cum stabilim că un grup extremist sau o minoritate este manipulată de către o putere străină ostilă, pentru a genera tensiuni și conflicte locale? Cum definim juridic, în termenii unui posibil instrument de agresiune hibridă, securitatea energetică?

În al doilea rând, va trebui să evaluăm în ce măsură o definire incompletă sau exagerată a acestor fenomene poate să ducă la abuzuri în respectarea și protejarea drepturilor și libertăților fundamentale? Este foarte important ca statul să aibă, de pildă, instrumentele necesare contracarării unei campanii fake news, orchestrate de o putere ostilă împotriva intereselor sale strategice. În timpul pandemiei COVID-19, în primăvara anului 2020, România a fost țința unor astfel de campanii de tip hibrid. A confirmat, oficial, Ministrul de Interne al României[15].

Dar este la fel de important ca astfel de instrumente să nu poată fi folosite pentru afectarea libertății de expresie într-o societate democratică. Cum realizăm, prin prevederile legislative, ambele deziderate, adică găsirea echilibrului corect?

În al treilea rând, va trebui să identificăm și să definim mecanismele optime de cooperare interinstituțională. Mai precis, să stabilim, prin legislație, responsabilitățile distincte, dar concurente pentru armată, poliție, servicii secrete, poliție de frontieră, jandarmi etc. De exemplu, în 10 mai 2019 un elicopter de mici dimensiuni, utilizat de contrabandiștii cu țigări, s-a prăbușit în nordul României[16], într-o pădure, și a fost găsit după 3 zile de la prăbușire, întâmplător, de niște localnici. Ne întrebăm, evident, cum e posibil ca un aparat de zbor să pătrundă, nedetectat, în spațiul aerian al României? Și, desigur, din perspectiva unei posibile agresiuni hibride, ne punem întrebarea ce s-ar fi întâmplat, dacă în loc de țigări de contrabandă acel elicopter introducea „omuleți verzi” pe teritoriul național? Ce instituție este responsabilă pentru astfel de incidente: armata, poliția de frontieră, jandarmeria?

În mod cert, noul pachet legislativ va trebui să reglementeze juridic toate aceste fenomene și situații, inclusiv responsabilitățile instituționale

pentru prevenirea și contracararea lor. Cazul elicopterului descoperit, întâmplător, în 10 mai 2019 este elocvent. Nicio instituție nu și-a asumat oficial acest eșec și nicio instituție nu a propus, oficial, un set de măsuri pentru a preveni repetarea unui astfel de incident.

Riscurile de tip cyber

În ultimele două decenii, dezvoltarea IT&C a fost, practic, exponențială. Ca efect, calitatea vieții, dezvoltarea socială și comunitară, cercetarea, medicina, sectoarele financiar-bancare, transporturile și infrastructura au cunoscut evoluții greu de anticipat acum 20 de ani.

În mod indubitabil, viața omului contemporan nu mai poate fi concepută în afara internetului și a tehnologiilor IT. Efectele pozitive se regăsesc atât la nivel individual, cât și la nivel comunitar și societal. Însă, pe lângă certele avantaje, dezvoltarea tehnologiilor IT&C implică și o serie de riscuri. Protejarea datelor personale capătă o nouă dimensiune în era informațională. De pildă, datele medicale ale cetățenilor erau păstrate, acum 30 de ani, pe suport de hârtie, în sertarele medicilor. Acum, majoritatea datelor despre pacienți sunt stocate și gestionate informatic. Este evident faptul că niciun pacient nu și-ar dori ca datele lui medicale să fie accesate de hackeri.

Sistemele educaționale evoluează. Temele elevilor nu mai sunt exclusiv cele clasice, din manual/caiet. Criza generată de COVID-19 a făcut ca, timp de câteva luni, școala să se desfășoare exclusiv online. Elevii primesc virtual teme, le rezolvă și transmit virtual răspunsurile. Aplicația *classroom*[17] este un exemplu. Evident, niciun părinte nu și-ar dori ca datele confidențiale ale propriilor copii, privind performanța școlară, să fie accesate de persoane neautorizate.

Am folosit aceste exemple pentru a evidenția faptul că, în procesul de dezvoltare socială, tehnologiile IT au o natură bivalentă, atât de factor generator de progres, cât și de vulnerabilitate, de risc pentru securitatea națională sau pentru interesele comunităților, ale familiilor și ale indivizilor.

Viitorul ne îndreaptă înspre orașe smart[18] și societăți smart. Digitalizarea reprezintă, fără îndoială, viitorul sistemelor administrative. Beneficiile induse sunt evidente. Este o chestiune de timp până când statele reușesc să parcurgă toți pașii tehnici ai digitalizării. Estonia, din acest punct de vedere, reprezintă un model[19].

Însă, pe lângă certele avantaje, ultimul deceniu ne-a demonstrat că domeniul cyber poate fi utilizat și ca o armă redutabilă. Dacă, în mod clasic, spațiile de confruntare militară erau aerul, solul și marea, odată cu Summitul NATO de la Varșovia, din 2016, cyber a devenit oficial, la nivelul Alianței, cel de-al patrulea spațiu de confruntare militară.

Exemplele din ultimul deceniu sunt elocvente. În anul 2010, un virus cyber inovativ, Stuxnet, a fost utilizat pentru a ataca sistemele informatice ale instalațiilor nucleare din Iran[20]. Efectul a constat în blocarea ritmului de dezvoltare al programului nuclear iranian. Acum 30 de ani, doar o operațiune a forțelor speciale sau un sabotaj de tip clasic ar fi putut produce un asemenea efect. Dar Stuxnet, un virus informatic, lansat de la distanță, greu de identificat și atribuit, a produs efectul militar și politic scontat. „Răspunsul” cyber este cunoscut sub numele virusului Shamon. În anul 2012, acest virus, Shamon, a fost lansat asupra sistemelor informatice ale companiei de stat saudite ARAMCO, din domeniul prelucrării petrolului și asupra unor rafinării din Qatar. Atacul cyber a produs daune majore prin compromiterea datelor din sistemele informatice atacate, care au generat o încetinire substanțială a producției de petrol, fiind necesară o resconstrucție completă a acestor sisteme informatice[21].

Nici infrastructurile critice civile, cum sunt rețelele de distribuție pentru populație, nu sunt ferite de riscurile cyber. De exemplu, în aprilie 2020, sistemele de furnizare a apei din Israel au fost afectate, în urma unui atac cyber[22]. În acțiunea militară clasică, de pildă, pentru a distruge distribuția de electricitate sau de aprovizionare cu apă potabilă a unui oraș, modalitățile efective erau atacul cu bombă/rachetă asupra nodurilor de rețea, atacul cu trupe speciale care să arunce rețeaua în aer.

Armele de tip cyber au demonstrat că același lucru se poate face de la distanță, fără nicio explozie de tip clasic, prin simpla trimitere a unor viruși informatici. S-a întâmplat în 23 decembrie 2015, în plin război hibrid în Ucraina, când sistemele informatice ale companiilor de distribuție a electricității au fost atacate și paralizate[23]. Efectul politico-militar a fost foarte mare: populația a rămas în beznă în plină iarnă.

Marea îngrijorare privind protecția infrastructurilor critice este legată de faptul că un atac cyber poate să compromită și să afecteze funcționarea

instalațiilor industriale prin atacarea sistemelor de control al tensiunii, presiunii și temperaturilor. Din acest punct de vedere, mii de instalații industriale din întreaga lume sunt vulnerabile, inclusiv instalații nucleare și de tratare a apei, rafinării de petrol sau centrale pe gaze, uzine chimice etc. La fel, sistemele informatice care gestionează traficul de călători (aeroporturi, gări, sisteme de dirijare a traficului rutier etc.) pot să reprezinte o țintă pentru atacuri de tip cyber.

Marea problemă, în astfel de cazuri, o reprezintă identificarea precisă a atacatorului. De obicei, sunt hackeri neasumați și nerecunoscuți de către state, chiar dacă acționează la comandă și în slujba interesului anumitor state.

Este dificil de definit și încadrat, în dreptul național sau internațional, un astfel de atac. Și mai ales, atacatorul. Întrucât atacatorul folosește servere proxy, rutere proxy, VPN-uri anonime. Acest aspect reprezintă, intrinsec, o provocare majoră pentru elaborarea noilor legi ale securității naționale. Cum definim și încadrăm juridic un astfel de agresor?

Dezvoltarea tehnologiilor cyber a revoluționat spionajul. Dacă acum câteva decenii accesul la documentele secrete ale unei entități statale se făcea prin metode clasice, de tip ”James Bond” sau de tipul racolării unor persoane care aveau acces direct la documente, în prezent tehnologiile IT permit realizarea unor acțiuni de spionaj[24] digital prin intermediul unor softuri sau al unor viruși informatici, cum e cazul Pegasus[25], sau chiar prin intermediul antivirușilor instalați pentru protecția informatică[26] a diverselor sisteme IT. Generic vorbind, statele/serviciile secrete nu mai trebuie neapărat să își trimită propriul James Bond în misiune, pe teren. Anumite date pot fi colectate de la distanță, digital, identificarea și atribuirea atacului fiind un proces dificil de realizat.

Nu doar datele clasificate ale statelor reprezintă o țintă în spațiul cybernetic. Datele sistemelor de sănătate publică, datele sistemelor bancare și financiare, datele digitale privind achizițiile publice și, în general, datele digitale ale administrațiilor publice reprezintă vulnerabilități care trebuie protejate și securizate. În anul 2020, o campanie masivă de spionaj cyber prin e-mail a folosit, fraudulos, nume mari de companii (Poșta Română, Banca Transilvania, DHL etc.) ca momeli pentru utilizatori, pentru a influența deschiderea unor e-mailuri care conțineau softul spion, țința fiind sustragerea de informații din calculatoarele aparținând diverselor *instituții publice din România*[27].

Din perspectivă legislativă, principala provocare o reprezintă găsirea echilibrului corect dintre, pe de o parte, stimularea procesului de digitalizare la nivel instituțional, comunitar, societal și, pe de altă parte, stabilirea prin lege a regulilor și a nivelului de protecție cybernetică, astfel încât datele digitale să fie apărate eficient și, în același timp, drepturile și libertățile fundamentale să fie protejate.

Ce instrumente legislative suplimentare oferim agențiilor care realizează *cyber defence* pentru a fi eficiente, dar, în același timp, pentru a nu deveni abuzive, în raport cu cetățenii? Vom impune prin legislație, ca măsură de prevenție a riscurilor cyber, reguli/niveluri obligatorii de securitate cybernetică diverselor instituții, cum ar fi, de pildă, casele de asigurări de sănătate, spitalele publice/private, instituțiile bancare, administrația publică locală etc.?

O altă provocare survine din nevoia reglementării mai eficiente a spațiilor ”dark” din mediul virtual. Cum definim și încadrăm juridic activitățile de trafic din zona dark internet (trafic de droguri, de arme, de materiale interzise etc.)? Pot fi incriminați posesorii de servere care găzduiesc, în mod voit, site-uri specializate pentru acțiuni specifice criminalității organizate transfrontaliere sau nu? Cazul recent al unui buncăr cyber din Germania este elocvent[28] și va reprezenta un caz important pentru tendințele de reglementare juridică din spațiul Uniunii Europene.

Nu în ultimul rând, vom legifera, în noul pachet al legilor securității naționale, dreptul guvernului, al armatei sau al serviciilor secrete de a ataca cybernetic agresorii cu care se confruntă? În noiembrie 2019, de exemplu, EUROPOL și poliția belgiană au atacat cyber sute de conturi care promovau propaganda jihadistă a Statului Islamic[29]. Vom permite, în noua legislație, instituțiilor statului român să efectueze atacuri cyber sau limităm intervenția explicit în sfera cyber defence?

Terorismul în era digitală – fenomenul autoradicalizării pe rețelele social media

Dezvoltarea tehnologică a permis apariția unor noi forme de manifestare a fenomenului terorist. În urmă cu câțiva ani, statele și agențiile de informații știau foarte clar cine este dușmanul din sfera

terorismului: organizațiile/grupările teroriste de pe toate meridianele globului, existând un index clar al acestora și al mercenarilor, gen Carlos „șacalul”[30], care se puneau în slujba intereselor unor state sau organizații teroriste. Atentatele presupuneau deturnări de avioane, atacuri cu bombă, atacuri cu arme de foc etc. Prevenția constă în monitorizarea organizațiilor/mercenarilor, arestarea, expulzarea atentatorilor, contracararea/anihilarea intențiilor de săvârșire a atentatelor. În mod evident, toate aceste riscuri clasice au rămas cât se poate de reale și sunt valabile, în continuare.

Însă dezvoltarea tehnologică și a social media a generat noi posibilități de manifestare a fenomenului terorist. Dacă, în trecut, racolarea și radicalizarea celor care, ulterior, comiteau efectiv atentatele se făceau în mod direct, nemijlocit, de către organizațiile teroriste, acum avem cazuri de autoradicalizare prin social media și prin comunicare virtuală cu liderii organizațiilor teroriste. Prin urmare nu mai este neapărat necesară întâlnirea efectivă dintre liderii organizațiilor teroriste și persoanele care, în urma radicalizării, devin atentatori. Ca efect, în astfel de cazuri, prevenția este mult mai dificil de realizat.

În trecut, multe atentate au fost prevenite prin monitorizarea eficientă a circuitului substanțelor explozive, a armelor care urmau să fie folosite în atentate și a activităților specifice rețelelor/organizațiilor teroriste. Dacă, acum câteva decenii, bombele sau armele de foc erau principalele arme folosite de teroriști, atentatele din ultimii ani, comise pe teritoriul european, au arătat că armele folosite pot să fie simple cuțite[31] sau camioane cu care atentatorii să intre în mulțimea oamenilor aflați pe stradă, așa cum s-a întâmplat la Nisa[32].

Un caz sugestiv pentru fenomenul autoradicalizării îl reprezintă atentatul, din 6 decembrie 2019, de la baza militară din Pensacola, Florida. Un tânăr saudit a ucis trei persoane și a rănit alte opt. Ancheta declanșată a prezentat faptul că, anterior atentatului, tânărul a postat pe rețelele de socializare mesaje anti-SUA și anti-Israel[33].

Provocarea de ordin legislativ este evidentă. Ar fi putut o posibilă monitorizare a conținutului postat pe social media de către atentator să prevină moartea unor persoane nevinovate? Unde este echilibrul corect, în acest caz, dintre prevenție și libertatea de expresie?

Prin contrast, în 6 iunie 2020, în Germania, poliția și serviciile secrete au arestat un tânăr islamofob care afirmase, într-o postare pe rețelele social media, că urmează să comită un atentat într-o moschee, pe modelul atacului islamofob din Noua Zeelandă, din 2019[34]. Nu a reușit să mai comită atentatul, pentru că poliția l-a arestat, în baza intențiilor postate în mediul virtual. La locuința tânărului, au fost găsite armele cu care urma să fie comis atentatul.

Analizând cele două cazuri, ne punem întrebarea legitimă: unde este, în astfel de cazuri, echilibrul corect dintre prevenție și libertatea de expresie?

Cu siguranță, o suprareglementare a posibilităților de prevenție ar conduce către un stat autoritar, către abuzuri și încălcări ale dreptului la viață privată și la opinie, garantate de Constituție! În același timp, viața este valoarea umană supremă, dreptul la viață fiind fundamental! Cum pot guvernele să apere mai bine viața cetățenilor nevinovați care cad victime radicalismului de tip teologic, fără a se transforma în ”Big Brother” de tip Orwellian?

Pandemia generată de COVID-19 a marcat o mutație de tip strategic în activitatea organizațiilor teroriste. Concret, asistăm la o mutare semnificativă a acțiunilor din spațiul real în mediul virtual: propaganda jihadistă, recrutarea de noi membri și adepți, organizarea atentatelor a căror țintă tinde să vizeze tot mai mult atacuri cyber asupra infrastructurilor critice. ISIS/DAESH a lansat, în premieră, în anul 2020 revista online „Securitatea suporterului”, al cărei conținut învață membrii și adepții organizației cum să evite/eludeze supravegherea serviciilor de informații în mediul online[35].

Un principiu antic pare să-și conserve relevanța și în contemporaneitate: „Legile date în vreme de pace sunt în mare parte anulate de război, iar legile date în vreme de război le anulează pacea”[36]. Marea provocare rezidă în găsirea formei juridice echilibrate, astfel încât să fie o legislație bună, elaborată în timp de pace, care să mențină pacea, democrația, drepturile fundamentale, dar și să prevină ororile războiului, în acest caz ororile generate de atentatele teroriste.

Utilizarea dronelor ca armă

În ultimele decenii, dezvoltarea tehnologiilor din domeniul dronelor a fost spectaculoasă. Ca efect, guvernele, companiile private sau cetățenii au, acum, acces la o gamă diversificată de drone. Pe

lângă beneficiile evidente din sfera transporturilor, a comerțului, a industriei de divertisment, ultimii ani au arătat că dronele pot fi folosite și ca arme veritabile[37].

Un incident major a avut loc în decembrie 2018, la Londra[38]. Aeroportul Gatwick a fost blocat timp de 32 de ore, iar peste 100.000 de pasageri au rămas blocați în aeroport. Cauza blocării avioanelor la sol a fost generată de drone neidentificate care au survolat constant spațiul limitrof pistelor aeroportului. Cu toate că forțe importante ale poliției și armatei au încercat să identifice autorii acestui incident, dronele au reapărut în apropierea aeroportului ori de câte ori s-a încercat redeschiderea pistei. Soluțiile imediate, lansate de autoritățile londoneze, s-au încadrat în sfera reacțiilor operative: desfășurarea unor lunetiști care să doboare imediat dronele, un bruiaj intens în acea zonă, pentru a bloca posibilitatea controlului dronelor de la distanță, cu riscul de a afecta alte activități din zona aeroportului, sau lansarea unor păsări special dresate să doboare dronele neautorizate din spațiul pistelor.

Un alt incident cu drone, din anul 2019, relevă potențialul ridicat al acestei tehnologii pentru a fi utilizată ca armă. În 14 septembrie 2019, industria petrolieră a Arabiei Saudite a fost atacată cu drone, care au incendiat instalațiile[39]. Pagubele estimate au fost de ordinul sutelor de milioane de dolari, iar producția a fost parțial oprită. Deși Arabia Saudită a investit masiv în sisteme de apărare antirachetă și, ca efect, toate atacurile cu rachetă, lansate de insurgenții huthi din Yemen asupra Arabiei Saudite, au fost contracarate, o tehnologie mult mai ieftină, dronele, au fost folosite de insurgenți cu un real succes, ca armă extrem de eficientă, imposibil de detectat de sistemele radar, și de neutralizat prin activarea sistemelor antirachetă.

Dacă acum 30 de ani nu se punea problema definirii dronelor ca risc de securitate națională, cu siguranță incidentele recente ne obligă să gândim și să inserăm, în legislația securității naționale, un punct distinct referitor la drone. Pe lângă destinațiile de tip militar, dronele pot fi utilizate cu succes de traficanții de droguri sau de traficanții de arme, de rețelele de criminalitate organizată transnațională, pentru a transporta produsele ilegale peste frontierele statelor.

De asemenea, imaginile din China, din timpul epidemiei COVID-19, au arătat posibilitățile tehnice prin care populația este supravegheată în timp real cu ajutorul dronelor, totodată, populația putând primi, prin intermediul megafoanelor instalate pe drone, în mod direct și personalizat, mesaje sau somații/instrucțiuni de conduită în spațiul social[40].

Astfel, în primul rând, o provocare legislativă va fi legată de stabilirea limitelor în care dronele pot fi utilizate de guverne pentru supravegherea populației sau în acțiuni de ordine publică. Unde apare echilibrul corect dintre nevoia guvernelor de a utiliza tehnologii moderne (drone) pentru prevenția unor fenomene infracționale sau antisociale, pe de o parte, și, pe de altă parte, dreptul la viața privată și protejarea libertăților fundamentale? Unde este limita peste care utilizarea lor se transformă în abuzuri și încălcări ale drepturilor și libertăților civile?

În al doilea rând, deși legislația europeană de reglementare a utilizării dronelor a fost îmbunătățită[41] și în România avem un nou Cod al Aviației[42], provocarea pentru legislația națională din sfera securității rămâne: Cum definim și încadrăm juridic dronele în rândul riscurilor de securitate națională? Cum ne apărăm de posibile atacuri cu drone? Care sunt instituțiile responsabile pentru prevenția și contracararea posibilelor atacuri cu drone asupra infrastructurilor critice? Cum reușim, prin legislație, să protejăm drepturile legitime ale cetățenilor și ale companiilor care folosesc dronele în scopuri civile, pentru dezvoltare? Cum reușim să prevenim utilizarea dronelor în scopuri criminale, fără să afectăm dezvoltarea acestei industrii, prin suprareglementare?

Influențarea rezultatelor alegerilor de către entități statale ostile

Constituțiile tuturor statelor democratice consacră dreptul cetățenilor de a-și alege reprezentanții și de a decide prin referendum în mod suveran. Pentru guverne, unul dintre testele fundamentale ale democrației constă în capacitatea de a organiza alegeri/referendumuri libere și corecte, astfel încât voința suverană a națiunilor să nu fie alterată sau manipulată de entități statale ostile.

De-a lungul istoriei recente, din rațiuni geopolitice sau de promovare a unor interese strategice, au existat situații în care entitățile statale au încercat să influențeze, în beneficiul propriu, rezultatele proceselor electorale din țările vizate.

Statele democratice au început să prezinte poziții[43] și rapoarte oficiale[44] despre astfel de

ingerințe externe, iar instituțiile responsabile pentru apărarea Constituției dezvoltă strategii pentru contracararea unor ingerințe externe în procesele electorale[45].

Comisii de Anchetă ale unor asemenea ingerințe au fost înființate recent în SUA[46], în Marea Britanie[47] sau în Federația Rusă[48]. Preocuparea aceasta este extrem de actuală și în spațiul european. Avem, astfel, o propunere de rezoluție, depusă în octombrie 2019, în Parlamentul European, referitoare la ingerințele electorale externe și la dezinformarea în procesele democratice naționale și europene[49].

O reacție oficială a SUA este ilustrativă pentru dimensiunea și actualitatea acestui tip de risc. Pentru a preveni ingerințe externe în procesul electoral, SUA propun, oficial, recompense substanțiale, de ordinal milioanelor de dolari, pentru oricine contribuie la identificarea actorilor externi care, la comanda unor guverne străine, încearcă să influențeze scrutinul prezidențial din noiembrie 2020[50].

Acum 30 de ani, de exemplu, influențarea rezultatului alegerilor/a voinței populației într-un stat suveran de către o putere străină (ostilă) se putea face prin mijloace clasice: finanțarea secretă a anumitor partide/lideri, a unor grupări extremiste sau minoritare, a unor organizații care promovau o anumită agendă, coruperea/racolarea unor lideri politici sau a unor formatori de opinie etc. Rezultatele efective erau, în astfel de cazuri, relativ limitate.

Astăzi, tehnologiile IT și dezvoltarea globală a rețelelor social media permit ca intențiile de influențare a opiniei publice și, implicit, a rezultatului alegerilor să poată fi realizate, cel puțin teoretic, de la distanță.

„Fabricile de troli” pot genera și lansa în spațiul virtual adevărate campanii, bazate pe fake news. Algoritmii informatici și motoarele de căutare pot direcționa, teoretic, serii de mesaje de manipulare/dezinformare către un public bine țintit dintr-o țară/regiune/comunitate.

Controversele legate de rolul pe care Cambridge Analytica l-a jucat în cadrul fenomenului Brexit[51] sunt relevante. Astfel, compania Cambridge Analytica a fost acuzată că a utilizat, în scopuri politice, fără consimțământ, datele personale a peste 50 de milioane de utilizatori de facebook[52]. Ceea ce partidele politice nu au reușit prin instrumentele tradiționale (metodele clasice de campanie electorală) algoritmii și softurile Cambridge Analytica se pare că au reușit. Mai precis, 3.000.000 de cetățeni care nu au votat niciodată au fost convinși să iasă la vot cu peste 1 miliard de mesaje personalizate, transmise prin social media, bazate pe datele personale ale utilizatorilor[53].

Nu este scopul acestui articol de a stabili dacă implicarea Cambridge Analytica a fost sau nu decisivă pentru succesul taberei ”Leave” din cadrul Brexit. Dar dacă ne uităm la rezultatele de la urne, unde diferența a fost în marja de 2 %, iar 3 milioane de cetățeni au ieșit pentru prima dată la vot, se pot trage anumite concluzii.

Ideea principală pe care vreau să o subliniez este că tehnologia actuală permite generarea unor instrumente de promovare a campaniilor electorale inexistente acum 30 de ani.

Mai exact, prin instrumentele tradiționale de campanie electorală (campanii door-to-door, distribuirea de materiale electorale, evenimente publice, mobilizarea simpatizanților etc.), aflate la îndemâna partidelor politice, este imposibil să generezi mesaje personalizate pentru milioane de oameni! Pentru a livra mesaje personalizate câtorva milioane de oameni prin mecanismele electorale clasice, ar trebui ca echipele de campanie electorală (documentare/creație/distribuție) să cuprindă mii și chiar zeci de mii de membri, ceea ce este imposibil pentru orice partid politic din spațiul european și euroatlantic.

Însă, pentru o firmă care deține softurile și algoritmii informatici necesari, distribuirea de mesaje personalizate pentru milioane de oameni devine o posibilitate reală.

Marea provocare, pentru legislația din domeniul securității naționale, este de a defini și de a încadra juridic o astfel de posibilitate, ca o entitate statală ostilă să utilizeze astfel de instrumente, pentru a manipula, în interes propriu, dreptul suveran de a alege al unei națiuni/comunități locale și de a genera instrumentele legislative, pentru ca orice guvern să poată preîntâmpina o asemenea situație.

În Spania, un judecător al Curții Supreme a demarat o anchetă judiciară privind posibilele ingerințe, prin astfel de instrumente, ale unor servicii secrete ostile în procesul separatist din provincia Catalonia[54].

Cum definim și cum încadrăm juridic astfel de fenomene în cadrul riscurilor de securitate națională?

Există riscul ca o suprareglementare să afecteze în mod indezirabil democrația și libertatea de expresie dintr-o societate? Cu siguranță, da! Ce instituție trebuie să primească responsabilitatea legală să prevină și să contracareze un astfel de risc? Autoritatea Electorală Permanentă (AEP), poliția, armata, serviciile secrete? Avem nevoie de o instituție nouă, special creată, pentru a gestiona astfel de fenomene? Cum stabilim, prin lege, mecanismele de prevenție? Unde este echilibrul corect dintre libertatea de expresie, libertatea comunicării, pe de o parte și, pe de altă parte, protejarea dreptului suveran al națiunii de a alege în mod liber?

Propaganda externă ostilă și campaniile fake news

În orice regim democratic, susținerea publică este esențială pentru consistența și coerența politicilor guvernamentale. Cu atât mai mult atunci când vorbim despre politici, proiecte și interese de natură strategică. Procesele de integrare a României în NATO și UE, de la finalul anilor ’90 și din deceniul următor, au avut o susținere publică extrem de importantă. Relevanța acestei susțineri s-a tradus în proiecte politice aplicate (modificări și adoptări legislative, politici publice, proiecte de reformă instituțională etc.), care au făcut posibilă integrarea.

Teoria schimbării atitudinale, din psihologia socială, ne spune că, la nivelul opiniei publice, schimbări semnificative se pot produce lent, dar progresiv, dacă stimulii de influențare a atitudinilor publice sunt transmiși constant către un grup țintă[55].

Un exemplu relativ recent pare sugestiv pentru a ilustra această teorie: evoluția susținerii publice a integrării în UE de către populația Republicii Moldova. Dacă, în anul 2007, în Republica Moldova, adepții integrării europene reprezentau 76%, în anul 2014 doar 44% mai susțineau acest proiect[56]. Iar rezultatele electorale ulterioare anului 2014 au consfințit acest trend.

În mod evident, există un complex cauzal, responsabil pentru scăderea susținerii publice de la 76% la 44%, iar propaganda ostilă (integrării europene) reprezintă unul dintre factori[57]. În mod evident, beneficiarul geopolitic al acestei scăderi nu este, în niciun caz, Republica Moldova.

Am prezentat acest exemplu pentru a ilustra situația în care o mare putere geopolitică își poate promova și proiecta interesele specifice într-un alt stat prin campanii fake news și propagandă ostilă. Deși, prin metoda sociologică a analizei de conținut, pot fi relevate corelații pertinente între anumite interese geopolitice și conținutul efectiv al unor campanii de propagandă ostilă, în practica legislativă încadrarea juridică și probarea „vinovăției” propagandei ostile se dovedesc a fi un demers extrem de dificil. De multe ori, granița dintre informare și dezinformare, dintre propagandă și simpla promovare (PR) este una extrem de subțire. Iar libertatea de exprimare, independența mass-mediei, libertatea de comunicare în spațiul virtual reprezintă drepturi fundamentale care trebuie apărate și întărite constant. Problema care se pune este că tocmai aceste principii și valori democratice pot fi exploatate, într-o manieră profesionistă, de către maeștrii propagandei aflați în slujba unor puteri geopolitice ostile.

Ca efect, o provocare legislativă majoră va fi de definire a acestui tip de risc securitar și de definire a responsabilităților instituționale pentru prevenirea/contracararea acestui fenomen? Totodată, stabilirea limitelor dincolo de care un astfel de demers s-ar putea transforma în abuz asupra liberei exprimări sau asupra independenței mass-mediei va trebui să stea la baza elaborării noilor prevederi legislative.

Campaniile fake news din timpul pandemiei COVID-19, operate în SUA sau UE, sunt elocvente[58]. Mecanismul tehnic de promovare a unei campanii implică mass-media oficială dintr-un stat, care lansează o temă, apoi mii de conturi social media (multe dintre acestea false) preiau mesajul în limbile de circulație internațională (engleză, germană, franceză, spaniolă etc.) și îl promovează masiv pe rețelele social media[59]. Campania fake news împotriva 5G , din timpul pandemiei COVID-19, a fost promovată prin mii de conturi Facebook, Twitter și Instagram, care au produs mii de postări cu un *reach* uriaș în timpul stării de urgență, având hashtagul #5Gcoronavirus[60].

În mod evident, „arma” fake news vizează generarea instabilității sociale, a contestării și a neîncrederii în autoritățile legitime ale unui stat. Ținta finală este blocarea unor decizii strategice care dezavantajează, geopolitic, statul ostil care promovează campania fake news respectivă.

Istoria recentă ne relevă faptul că principala metodă de combatere a fake news o reprezintă educația consistentă a populației „țintă”. Modelul

finlandez s-a dovedit a fi, de departe, cel mai performant[61].

„Finlanda este considerată țara europeană cea mai rezistentă în fața fenomenului fake news, întrucât, pe tot parcursul procesului educativ, este cultivată și stimulată gândirea critică. Abordarea critică, interpretarea, verificarea și evaluarea tuturor informațiilor pe care le primești, de oriunde apar, sunt cruciale. Programa școlară din Finlanda este parte a unei strategii mai ample, concepute de Guvernul de la Helsinki, după 2014, când țara a fost ținta unei campanii de știri false, lansate din Rusia. La orele de matematică, de exemplu, elevii învață cât de ușor pot fi manipulate statisticile. La orele de artă, pot vedea cât de ușor poate fi distorsionat mesajul unei imagini, la cele de istorie analizează cele mai notabile campanii de propagandă, în timp ce profesorii de limba finlandeză le arată în câte feluri pot fi utilizate cuvintele, pentru a deruta, a induce în eroare și a înșela. Chiar dacă nu citesc ziare sau nu urmăresc posturile TV de știri, elevii și cetățenii, în general, sunt bombardați zilnic cu sute de știri pe WhatsApp, YouTube, Instagram, Snapchat etc. Obiectivul de bază al sistemului educațional finlandez este că, în astfel de cazuri, studenții și elevii să-și pună întrebări, ca: Cine a produs această informație și de ce? Unde a fost publicată? Ce spune cu adevărat? Ce public țintește? Pe ce este bazată? Există dovezi că lucrurile stau așa sau este doar părerea cuiva? Poate fi verificată în altă parte?”[62]

Chiar dacă fascinația modelului educațional finlandez tinde să ne inspire, provocarea de ordin legislativ rămâne. Exceptând legislația specifică educației, cum definim și cum încadrăm juridic, în categoria riscurilor de securitate națională, propaganda ostilă și campaniile de fake news, coordonate de entități statale ostile? Căci fără o definire și o încadrare juridică adecvată, orice demers este complet inutil, ba chiar poate deveni periculos pentru mediul democratic! Ce instituție a statului primește o astfel de responsabilitate legală? Cum creăm mecanisme de control, astfel încât să putem evita producerea de abuzuri asupra mass-mediei independente, asupra libertății de expresie sau dreptului la opinie?

Riscul suprareglementării juridice este real și poate afecta, în mod indezirabil, democrația și libertățile fundamentale. Granițele dintre aceste categorii sunt extrem de subțiri și istoria ne relevă numeroase exemple, când demersuri care au pornit de la bune intenții au fost denaturate și au sfârșit prin abuzuri deplorabile și regimuri dictatoriale.

Dezvoltarea tehnologiilor de monitorizare în masă, a rețelelor SMART, criptomoneda și IA (inteligența artificială)

Evoluțiile tehnologiei digitale și ale inteligenței artificiale (IA) tind să ne plaseze într-o etapă nouă, definită ca începutul celei de-a *cincea revoluții industriale*[63]. Trăim o perioadă de uriașe transformări. Calculatoarele pot lucra mai repede, mai bine și mai mult decât oamenii, iar integrarea, în această ecuație, a IA ne aduce în situația în care roboții și mașinile vor putea să ia decizii. Asta nu înseamnă că roboții ne vor înlocui, ci ne vor fi parteneri în societățile de tip smart.

Viitorul înseamnă că vom locui în case de tip smart, ne vom deplasa cu mijloace de transport smart pe o infrastructură de transport de tip smart, orașele se vor schimba pentru a deveni smart, instituțiile se vor transforma și vor deveni smart, iar interconectarea se va face prin rețele inteligente (Smart Grids). Este vorba despre acel tip de rețea care implică cooperarea omului cu calculatorul și în care calculatoarele, în baza unor softuri avansate, pot lua decizii. Într-un oraș de tip SMART, comunicarea și informarea se bazează pe tehnologii avansate. Clădirile, sistemele de transport public, serviciile administrative și guvernamentale, rețelele de magazine comerciale, managementul traficului etc. sunt coordonate și controlate de tehnologii de tip IA (inteligență artificială) și IoT (Internet of Things).

În mod evident, această revoluție tehnologico-industrială va stimula dezvoltarea și va avea efecte pozitive asupra vieții oamenilor. Marea provocare legislativă este să reglementăm în mod adecvat toate aceste evoluții. Ca orice tehnologie inventată vreodată, utilizarea bivalentă (în scopuri pozitive sau distructive) va fi o opțiune explicită a utilizatorului. De aceea legislația trebuie să reglementeze adecvat toate aceste situații: să stimuleze dezvoltările pozitive și să contracareze utilizările negative. Cine protejează noile orașe/clădiri de tip SMART împotriva atacurilor cyber? Poate departamentul IT al unui orășel care investește masiv în tehnologii SMART să facă față unui posibil atac cyber, lansat de ”hackerii” unei mari puteri geopolitice ostile (neasumați oficial)?

Controversele legate de tehnologiile 5G sunt elocvente. Reprezintă anumite echipamente 5G vulnerabilități de securitate[64]? Cum reglementăm juridic astfel de riscuri? Pentru că sunt riscuri noi, neexistente acum câțiva ani, deci nereglementate prin legislația în vigoare. În anul 2019, am asistat la acuzații oficiale, făcute de SUA, privind riscurile ca adoptarea anumitor tehnologii 5G să prezinte vulnerabilități de spionaj digital[65]. Astfel, o provocare legislativă este să transformăm evaluările, analizele și afirmațiile/acuzațiile privind riscurile de spionaj digital în conținut juridic efectiv, în baza căruia putem să încadrăm juridic astfel de tehnologii în zona riscurilor de securitate națională și, astfel, să avem o bază legală pentru acceptarea sau respingerea anumitor tehnologii. În sens contrar, arbitrariul va juca rolul dominant.

Tehnologiile digitale au evoluat foarte mult în ultimul deceniu. Tehnologiile de recunoaștere facială pot fi aplicate, acum, la nivelul populațiilor de sute de milioane de oameni, iar în unele state, astfel de proceduri au devenit obligatorii prin lege[66]. În mod evident, guvernele, poliția, serviciile secrete vor dori o aplicare cât mai amplă a acestor posibilități, pentru a identifica rapid, în mulțime, infractorii, teroriștii, criminalii, persoanele date în urmărire, delicvenții violenți etc.

Recunoașterea facială, chiar și în condițiile purtării măștii medicinale, brățările electronice, softurile instalate pe telefoanele mobile (STOPCOVID, de exemplu) sunt tehnologii nereglementate, în prezent, de legislația românească. Este rolul Parlamentului României de a stabili, prin lege, care tehnologii pot fi permise și care NU pot, în ce condiții pot fi adoptate și prin ce mecanisme se exercită controlul democratic asupra utilizării lor. În acest caz, principiul constituționalității, aplicat în viitoarea legislație, va trebui să reprezinte garanția că instituțiile statului nu se transformă în veritabili ”Big Brother”[67], descriși de George Orwell în „1984”[68].

Este de așteptat ca, în domeniul financiar, moneda virtuală, criptomoneda, să ocupe, progresiv, un spațiu cât mai mare în cadrul tranzacțiilor interne și internaționale. LIBRA, de exemplu, este proiectată să funcționeze ca un nou sistem global de plată[69].

În mod evident, va mai trece o perioadă până când criptomoneda va juca un rol decisiv în sistemul financiar global. Dar tendința este evidentă. Întrebarea care se pune, din perspectivă legislativă, este dacă reglementarea proceselor care implică criptomoneda se face exclusiv în legislația specifică domeniului financiar-bancar? Putem identifica riscuri de securitate națională, generate de posibile atacuri speculative, având ca instrument criptomoneda? Sau atacuri cyber cu scopul unor fraude uriașe? Dacă da, cum definim și cum încadrăm juridic, în conținutul noii legislații, criptomoneda în rândul riscurilor de securitate națională?

Este deja un fapt comun să afirmăm că IA (inteligența artificială) va revoluționa toate aspectele vieții sociale, cu dezvoltări exponențiale în medicină, transporturi, comunicații, cercetare, industrie, divertisment etc. După ce informatizarea a fost considerată, în literatura de specialitate, ca fiind o a doua alfabetizare a instituțiilor și a comunităților umane, se pare că IA constituie un nivel nou, superior. IA (inteligența artificială) va crește, în mod exponențial, capacitatea de calcul, de analiză a informațiilor sau a imaginilor satelitare. Pe lângă dezvoltările civile, aplicațiile militare ale IA generează, în fapt, programe și proiecte cu un potențial uriaș. Astfel, IA utilizată în domeniile militar și de securitate, rolul acesteia este conceput să îmbunătățească, să prelungească posibilitățile intelectului uman, nu să le înlocuiască. Sistemele IA vor integra în parteneriat oamenii și mașinile, ceea ce va duce la perfecționarea culegerii de informații, la prelucrarea și interpretarea lor la parametri superiori, la perfecționarea nivelului de operativitate a armatelor, la sprijinirea proceselor de luare a deciziei și de management al acțiunilor de luptă, dar și la o creștere exponențială a posibilităților de spionaj virtual, de propagandă și de promovare a unor interese strategice prin instrumente virtuale[70].

Putem evita fenomenul IA în dezbaterea despre noua legislație a securității naționale? Cum vom reglementa juridic Inteligența artificială (IA), în general, și cum vom defini și încadra IA în lista riscurilor de securitate națională? Unde este echilibrul corect dintre promovarea și susținerea IA pentru dezvoltare economică, socială, pe de o parte, și capacitatea de prevenire a utilizării IA ca armă împotriva statului, instituțiilor, comunităților sau cetățenilor, pe de altă parte?

Concluzii

Mediul global de securitate s-a schimbat mult în ultimele decenii. Tendința generală a fost marcată de apariția și dezvoltarea riscurilor neconvenționale, asimetrice și hibride. Astfel, natura războiului și a agresiunilor, în general, s-a schimbat. Războiul nu a dispărut de pe harta geopolitică globală. Doar formele de manifestare s-au diversificat și au devenit mai sofisticate, utilizând la maximum posibilitățile oferite de tehnologie.

În secolul al XXI-lea o agresiune militară nu se mai face neapărat cu tancurile, pe modelul secolului al XX-lea. Agresorul poate să trimită un virus informatic, și paguba produsă sau efectul politico-militar să fie similar. Dacă deținătorii tancurilor (echipamentelor militare grele) sunt relativ simplu de stabilit, în cazul atacurilor informatice, identitatea atacatorului este dificil de probat, întrucât atacatorul folosește, de regulă, servere proxy, rutere proxy, VPN-uri anonime. Un atac aerian nu se mai face neapărat cu avioane sau rachete, acestea fiind în mod clar identificabile ca aparținând unei entități statale. Se poate realiza și cu drone, al căror cost este mult mai mic, apartenența putând fi atribuită unor entități nonstatale, de tip proxy[71], iar distrugerea produsă să fie la fel de mare.

Dacă în secolul al XX-lea statele își trimiteau trupele speciale în diverse operațiuni de atac al unor obiective strategice, în secolul al XXI-lea avem situații în care trupe speciale acționează fără însemne („omuleții verzi” din Crimeea și din estul Ucrainei) sau aparțin unor firme private de securitate, cum se întâmplă în Siria[72], în Libia[73] sau în alte zone de conflict armat[74].

Deși natura riscurilor s-a schimbat, este relevant să precizăm că importanța riscurilor de tip clasic rămâne ridicată. Mai precis, este necesar ca statele să-și dezvolte capacități de reacție și de contracarare pentru riscurile asimetrice și hibride, dar este important, în egală măsură, să-și modernizeze capabilitățile de contracarare a riscurilor de tip clasic. Ar fi o mare eroare strategică să minimalizăm importanța riscurilor și a amenințărilor de tip clasic. Ar fi greșit să investim exclusiv în apărare de tip cyber, pentru că s-ar putea, la un moment dat, să ne confruntăm cu tancuri la graniță. Prin urmare provocarea, pentru guverne, este de a găsi un echilibru în dezvoltarea capabilităților de apărare, între vechi și nou, între clasic și hibrid.

Am încercat să evidențiez faptul că evoluțiile tehnologice și geopolitice din ultimele decenii au generat necesitatea modificării legislației pentru adaptarea la noile realități. Istoria recentă din spațiul european și euroatlantic ne arată că modificarea legislației din domeniul securității naționale a fost făcută, preponderent, ca reacție la incidente de securitate și la atentatele teroriste. S-a întâmplat în SUA (Patriot Act, adoptat ca reacție la 9/11), în Franța, Germania, Marea Britanie, Belgia. Practic, demersul legislativ din acest domeniu a fost, preponderent, reactiv, și nu proactiv.

În România, nu am avut incidente de securitate semnificative în ultimele decenii. Din acest motiv, nici presiunea publică, pentru modificarea legislației, nu a fost una ridicată. Au existat inițiative și proiecte, însă contextele politice și electorale succesive au fost de natură să nu genereze finalizarea acestor proiecte legislative.

Ideea principală a acestui demers rezidă în provocarea uriașă pe care Parlamentul României o are în demersul de a reglementa juridic noile riscuri de securitate. Conceptul integrator va trebui să fie principiul constituționalității, principiu, care, în mod evident, reprezintă esența oricărei democrații. Nevoia de prevenție a riscurilor de securitate și de protejare a vieții cetățenilor nevinovați nu trebuie, nicidecum, să conducă spre o suprareglementare, generatoare de abuzuri și comportamente opresive. Istoria ne arată că marile regimuri dictatoriale și-au fundamentat existența și consolidarea puterii pe ideologii prezentate ca fiind salvatoare și eliberatoare. Doar că practica a fost complet opusă teoriei și ideologiilor pe care s-au clădit.

Demersul actual are ca scop relevarea acestor provocări legislative. Riscurile clasice de securitate rămân o constantă. Doar că guvernele au o experiență îndelungată în contracararea lor, iar parlamentele au legiferat aceste fenomene și există o experiență legislativă în acest sens.

Când abordăm noile riscuri de securitate, experiența legislativă este extrem de limitată. Va trebui să inovăm și să producem definiții și încadrări juridice, pentru fenomene nereglemetate până acum. Fabricile de troli, utilizate de o entitate statală ostilă, ca armă împotriva intereselor noastre naționale, tehnologiile care permit monitorizarea în masă (softuri, aplicații, brățări electronice, sisteme face recognition etc.), atacurile cyber împotriva infrastructurilor critice, autoradicalizarea în

mediul virtual sunt câteva exemple ilustrative pentru dificultatea și complexitatea acestui demers legislativ.

Așa după cum s-a întâmplat în ultima perioadă, dezbaterea și adoptarea noilor legi ale securității naționale pot fi amânate sine die. În fiecare ciclu parlamentar din ultimele decenii, s-a vorbit despre necesitatea adoptării noilor legi, însă demersul a rămas strict la nivel de intenție. Este foarte posibil ca în contextul crizei generate de COVID-19, nimeni să nu își asume acest demers. Cine își asumă reglementarea juridică a noilor riscuri de securitate cu toate provocările legislative expuse mai sus, mai ales în context electoral?

Este posibil să rămânem cantonați în aceeași paradigmă a nonacțiunii. Însă, pe măsură ce timpul trece, dezvoltările tehnologice și geopolitice vor genera procese și fenomene tot mai greu de prevenit și de contracarat în baza unor instrumente legislative, elaborate acum 30 de ani. Legislația perimată este, intrinsec, o vulnerabilitate.

Vom evolua spre societatea de tip SMART în măsura în care ne vom adapta legislația, mentalitățile și practicile instituționale la provocările de tip SMART.

NOTE:

1 *L 51/1991 – Legea securității naționale*; *L 14/1992 – Legea de organizare și funcționare a SRI*; *L 1/1998 – Legea de organizare și funcționare a SIE*; *L 191/1998 – Legea de organizare și funcționare a SPP*; *L 92/1996 – Legea de organizare și funcționare a STS*; *L 535/2004 – Legea pentru prevenirea și combaterea terorismului*.

2 https://www.newmoney.ro/ce-tehnologii-de-supraveghere-folosesc-tarile-impotriva-coronavirusului-desi-o-parte-din-ele-afecteaza-anumite-drepturi-ale-omului/, accesat la 14.05.2020.

3 http://www.rador.ro/2020/05/28/parlamentul-frantei-a-votat-in-majoritate-pentru-aplicatia-stopcovid-pentru-telefoanele-mobile-smart/, accesat la 14.05.2020.

4 https://www.economica.net/elevii-de-gimnaziu-din-beijing-vor-purta-bra-ari-electronice-care-sa-trimita-avertizari-in-cazul-in-care-au-febra_184227.html, accesat la 14.07.2020.

5 https://adevarul.ro/international/in-lume/benjamin-netanyahu-vrea-cipuri-pielea-elevilor-expertii-securitate-cibernetica-opun-propunerii-1_5eb92e255163ec4271ab4810/index.html, accesat la 14.07.2020.

6 https://universul.net/tehnologii-infioratoare-invadeaza-europa-odata-cu-pandemia-analiza-bloomberg/, accesat la 14.07.2020.

7 *Ibidem*.

8 https://www.mediafax.ro/externe/politistii-cu-casti-de-supraveghere-ne-vor-identifica-si-ne-vor-lua-temperatura-din-mers-se-intampla-deja-in-china-dubai-si-italia-19144065, accesat la 14.07.2020.

9 https://www.mediafax.ro/externe/mossad-a-obtinut-10-milioane-de-masti-zeci-de-mii-de-teste-si-aparatura-medicala-din-surse-necunoscute-19031610, accesat la 18.07.2020.

10 https://www.jpost.com/israel-news/netanyahu-thanks-mossad-chief-for-purchasing-coronavirus-medical-gear-629161, accesat la 18.07.2020.

11 https://www.defenseromania.ro/serviciile-secrete-americane-i-israeliene-ar-fi-aflat-din-timp-de-coronavirus-us-army-neaga-raportul_602787.html, accesat la 18.07.2020.

12 Cele patru mari revoluții industriale (denumite în literatură *Industry 1.0* până la *Industry 4.0*): mecanizare, electrificare, digitalizare, conectivitate.

13 *Industry 5.0* : transformarea lumii într-una SMART. A 5-a revoluție industrială se va concentra pe relația dintre om și calculator, pe internetul lucrurilor și pe rețelele inteligente.

14 Armatele private, compuse din mercenari (de obicei, foști componenți ai forțelor speciale din poliție, armată, servicii secrete), reprezintă o modalitate nouă prin care unele guverne doresc atingerea scopurilor strategice, fără să fie, oficial, implicate în diverse conflicte. (https://monitorulapararii.ro/fortele-hibride-mercenari-armate-private-1-21023, accesat la 18.07.2020)

15 https://www.capital.ro/vela-sa-fim-responsabili-sa-nu-credem-ca-virusul-nu-exista.html, accesat la 18.07.2020.

16 https://www.digi24.ro/stiri/actualitate/evenimente/un-elicopter-sovietic-care-zburase-clandestin-in-romania-a-fost-gasit-intamplator-la-patru-zile-de-la-prabusire-1128328, accesat la 18.07.2020.

17 https://www.eduapps.ro/aplicatii-educatie/classroom/, accesat la 18.07.2020.

18 https://www.wall-street.ro/articol/Turism/230215/10-orase-smart-din-lume-transformate-ireprosabil-de-tehnologie.html#gref, accesat la 18.07.2020.

19 https://economie.hotnews.ro/stiri-it-22098274-estonia-ajuns-atat-departe-digitalizarea-serviciilor-incat-poti-ajunge-doar-trei-ori-viata-semnezi-hartii-diversele-autoritati.htm, accesat la 18.07.2020.

20 https://monitorulapararii.ro/atacurile-cibernetice-permanent-in-umbra-conflictelor-din-orientul-mijlociu-1-28373, accesat la 18.07.2020.

21 *Ibidem*.

22 https://www.mediafax.ro/externe/atac-cibernetic-masiv-in-israel-exista-suspiciuni-ca-ar-fi-fost-lansat-de-iran-19163989, accesat la 18.07.2020.

23 https://www.agerpres.ro/sci-tech/2016/02/12/atacul-cibernetic-ce-a-intrerupt-furnizarea-electricitatii-intr-o-regiune-a-ucrainei-a-fost-executat-din-rusia-17-06-10, accesat la 18.07.2020.

24 https://monitorulapararii.ro/pegasus-spionaj-prin-intermediul-telefonului-mobil-1-28477, accesat la 18.07.2020.

25 https://en.wikipedia.org/wiki/Pegasus_(spyware), accesat la 18.07.2020.

26 https://www.digi24.ro/stiri/sci-tech/lumea-digitala/spionii-israelieni-au-descoperit-ca-rusia-folosea-kaspersky-pentru-spionaj-809017, accesat la 18.07.2020.

27 https://universul.net/alerta-campanie-masiva-de-spionaj-prim-email-nume-de-mari-companii-folosite-ca-momeli/, accesat la 18.07.2020.

28 https://www.thelocal.de/20190927/germany-cracks-cyber-bunker-hosting-darknet-sites, accesat la 18.07.2020.

29 https://romanialibera.ro/international/justitia-belgiana-zadarniceste-propaganda-isis-prin-atacuri-cibernetice-815216

30 https://ro.wikipedia.org/wiki/Carlos_%C8%98acalul, accesat la 18.07.2020.

31 https://www.digi24.ro/stiri/externe/incident-de-natura-terorista-la-londra-un-barbat-a-injunghiat-mai-multe-persoane-pe-strada-1254062, accesat la 18.07.2020.

32 https://ro.wikipedia.org/wiki/Atentatul_de_la_Nisa_(2016), accesat la 18.07.2020.

33 https://stirileprotv.ro/stiri/international/autorul-atacului-de-la-pensacola-era-saudit-ce-a-publicat-acesta-pe-retele-sociale.html, accesat la 18.07.2020.

34https://www.news.ro/externe/plan-atac-vizand-musulmani-dejucat-germania-tanar-arestat-dupa-s-laudat-internet-vrea-comita-atac-islamofob-cel-christchurch-zeelanda-arme-confiscate-domiciliul-suspectului-hildesheim-fisiere-192240520800202006121938490 2, accesat la 18.07.2020.

35 https://islamro.com/topic/618-daesh-public%C4%83-primul-num%C4%83r-al-unei-reviste-dedicate-securit%C4%83%C8%9Bii-cibernetice/?tab=comments#comment-975, accesat la 18.07.2020.

36 Titus Livius, *Istoria Romei de la întemeierea cetății – Enciclopedia înțelepciunii*, Editura Roossa, 2013, p. 108.

37 https://monitorulapararii.ro/epoca-razboaielor-dronelor-aeriene-s-a-instalat-definitiv-1-31794, accesat la 18.07.2020.

38 https://www.hotnews.ro/stiri-international-22877928-haos-aeroportul-gatwick-inchis-peste-17-ore-din-cau za-unor-drone-neidentificate.htm, accesat la data de 18.07.2020.

39 https://www.mediafax.ro/externe/atacuri-cu-drone-in-arabia-saudita-doua-instalatii-petroliere-sunt-afectate-de-incendii-masive-insurgentii-huthi-din-yemen-revendica-atentatele-video-18398347, accesat la 18.07.2020.

40 https://www.digi24.ro/stiri/externe/autoritatile-ii-urmaresc-cu-drona-pe-chinezi-si-ii-someaza-sa-poarte-masca-bunico-nu-te-mai-holba-du-te-si-spala-te-pe-maini-1254243, accesat la 21.07.2020.

41 La 26 iunie 2018, Consiliul a adoptat noile norme proporționale și bazate pe riscuri, care vor permite sectorului aviației din UE să se dezvolte și să devină mai competitiv. Noile norme se referă și la pragul de înmatriculare pentru operatorii de drone: aceștia ar trebui înmatriculați, dacă dronele lor pot transfera o energie cinetică mai mare de 80 de jouli la impactul cu o persoană, https://www.consilium.europa.eu/ro/policies/drones/, accesat la 21.07.2020.

42 http://legislatie.just.ro/Public/DetaliiDocument/22 3897, accesat la 21.07.2020.

43 https://www.g4media.ro/marea-britanie-acuza-rusia-ca-a-incercat-sa-se-amestece-in-alegerile-parlamentare-din-2019-achizitionand-ilegal-si-difuzand-online-documente-sensibile-referitoare-la-acordul-de-liber-schimb-cu-statel.html, accesat la 21.07.2020.

44 https://www.stiripesurse.ro/democratiile-occidentale-o-resursa-imensa-pentru-rusia-kremlinul-a-incercat-sa-intervina-si-in-referendumul-pentru-independenta-scotiei_1487574.html, accesat la 21.07.2020.

45 https://www.stiripesurse.ro/avertismentul-nsa-cu-privire-la-alegerile-americane-vom-actiona-atunci-cand-vom-vedea-ca-adversarii-nostri-incearca-sa-se-amestece_1487511.html, accesat la 21.07.2020; https://www.stiripesurse.ro/serviciu-secret-detoneaza-bomba-china-rusia-si-iranul-incearca-sa-influenteze-rezultatul-alegerilor-din-sua_1488962.html, accesat la 21.07.2020.

46 https://www.euractiv.ro/extern/departamentul-justitiei-a-deschis-o-ancheta-penala-in-cazul-investigatiei-privind-ingerintele-ruse-16368, accesat la 21.07.2020.

47 https://www.stiripesurse.ro/democratiile-occidentale-o-resursa-imensa-pentru-rusia-kremlinul-a-incercat-sa-intervina-si-in-referendumul-pentru-independenta-scotiei_1487574.html, accesat la 21.07.2020.

48 https://www.caleaeuropeana.ro/duma-de-stat-a-rusiei-infiinteaza-o-comisie-de-ancheta-a-ingerintelor-externe-in-favoarea-protestelor-de-la-moscova/, accesat la 21.07.2020.

49 http://www.europarl.europa.eu/doceo/document/B-9-2019-0108_RO.html, accesat la 21.07.2020.

50 5 august 2020, Secretarul de Stat al SUA: „Statele Unite oferă o recompensă de până la 10 milioane de dolari pentru informații care permit identificarea sau localizarea oricărei persoane care, acționând la ordinele sau sub controlul unui guvern străin, intervine în alegerile americane”, https://www.g4media.ro/mike-pompeo-sua-ofera-o-recompensa-de-10-milioane-de-dolari-pentru-arestarea-oricarei-persoane-care-intervine-in-alegerile-din-noiembrie.html, accesat la 21.07.2020.

51 https://www.digi24.ro/stiri/externe/ue/cum-a-influentat-cambridge-analytica-referendumul-privind-brexit-902773, accesat la 21.07.2020.

52 *Ibidem*.

53 https://www.imdb.com/title/tt8425058/, accesat la 21.07.2020.

54 https://ziaristii.com/au-prins-spionajul-rus-implicat-haosul-din-catalunya-si-destabilizarea-europei-serviciile-secrete-din-ue-confirma-mana-rusiei-actiuni-grave-pe-continent/, accesat la 21.07.2020.

55 Andrei Holman, ”Cognitive fluency and attitudinal change mechanisms”, *Source:Social Psychology (Psihologia socială)*, Issue 10/2002, pp. 90-107.

56 http://www.viitorul.org/files/4392299_md_studiu_informa.pdf, accesat la 21.07.2020.

57 http://www.ziare.com/europa/moldova/alegeri-la-chisinau-fara-stat-de-drept-libertate-de-exprimare-si-deschidere-catre-lume-nu-vom-avea-nici-integrare-europeana-nici-unire-cu-romania-interviu-1551002, accesat la 21.07.2020.

58 https://www.digi24.ro/stiri/externe/ue/document-rusia-desfasoara-o-semnificativa-campanie-de-dezinformare-in-ue-cu-privire-la-coronavirus-1277347, accesat la 21.07.2020.

59 https://www.state.gov/briefing-with-special-envoy-lea-gabrielle-global-engagement-center-on-disinformation-and-propaganda-related-to-covid-19/, accesat la 21.07.2020.

60 https://www.nytimes.com/2020/04/10/technology/coronavirus-5g-uk.html, accesat la 21.07.2020.

61 http://m.ziare.com/media/finlanda-incepe-lupta-cu-fake-news-din-scoala-primara-si-da-rezultate-1595955, accesat la 21.07.2020.

62 http://m.ziare.com/media/finlanda-incepe-lupta-cu-fake-news-din-scoala-primara-si-da-rezultate-1595955, accesat la 21.07.2020.

63 *Industry 5.0* transformarea lumii într-una Smart. A 5-a revoluție industrială se va concentra pe relația dintre om și mașină.

64https://www.ft.com/content/8b48f460-50af-11e9-9c76bf4a0ce37d49, accesat la 21.07.2020.

65 https://www.mediafax.ro/economic/avertismentul-sua-in-legatura-cu-huawei-si-tehnologia-5g-ei-vor-doar-sa-fure-secrete-de-stat-18678540, accesat la 21.07.2020.

66 https://www.mediafax.ro/life-inedit/china-introduce-recunoasterea-faciala-obligatorie-pentru-utilizatorii-de-telefoane-mobile-18637109, accesat la 21.07.2020.

67 Personaj fictiv, ilustrând tendinţele dictatoriale, totalitariste, https://www.britannica.com/topic/Big-Brother-fictional-character, accesat la 21.07.2020.

68 George Orwell, *1984 Nineteen Eighty-Four*, Penguin Books Ltd, 1991.

69 https://libra.org/en-US/, accesat la 21.07.2020.

70 https://monitorulapararii.ro/inteligenta-artificiala-in-intelligence-si-nu-numai-1-28414, accesat la 21.07.2020.

71 https://scholarcommons.usf.edu/cgi/viewcontent.cgi?article=1701&context=jss, accesat la 21.07.2020.

72 https://monitorulapararii.ro/razboaiele-din-siria-si-afganistan-vor-fi-privatizate-1-11282, accesat la 21.07.2020.

73 https://www.digi24.ro/stiri/externe/mapamond/raport-onu-cum-lupta-armata-privata-a-lui-putin-in-libia-de-partea-fortelor-rebele-1303476, accesat la 21.07.2020.

74 https://www.g4media.ro/mercenarii-rusiei-ce-sunt-si-cum-actioneaza-micile-armate-private-comandate-de-moscova-cazul-wagner-sau-cum-a-decazut-cea-mai-mare-companie-rusa-de-securitate.html, accesat la 21.07.2020.

BIBLIOGRAFIE

Buzan Barry, *People State and Fears*, Brighton, Harvester Press, 1983.

Fox C. Amos, *Conflict and the Need for a Theory of Proxy Warfare*, https://scholarcommons.usf.edu/cgi/viewcontent.cgi?article=1701&context=jss

Fridman Ofer, Kabernik Vitaly, Pearce C. James, *Hybrid Conflicts and Information Warfare: New Labels, Old Politics*, 1st Edition, 2018.

Haacke Jürgen, *Asean's Diplomatic and Security Culture. Origins, development and prospects*, Antony Rowe Ltd., Chippenham, Wiltshire, Great Britain, 2003.

Hoffman G. Frank, *Conflict in the 21th Century: the Rise of the Hybrid Wars*, https://www.potomacinstitute.org/images/stories/publications/potomac_hybridwar_0108.pdf

Holman Andrei, ”Cognitive fluency and attitudinal change mechanisms”, *Social Psychology (Psihologia socială)*, Issue 10/2002, https://www.ceeol.com

Iancu N., Fortuna A., Barna C., Teodor M., *Countering Hybrid Threats: Lessons Learned from Ukraine* (NATO Science for Peace and Security), 2016.

Micossi Stefano, Tosato Gian Luigi, *The European Union in the 21st Century. Perspectives from the Lisbon Treaty*, Center for European Policy Studies, Brussels, 2009.

Orenstein A. Mitchell, *The Lands in Between: Russia vs. The West and the New Politics of Hybrid War*, 1st Edition, 2019.

Răducanu Gabriel, Anastasiei Traian, *Challenges To Global Security*, http://www.afahc.ro/ro/revista/2017_1/17-GabrielRaducanu, TraianAnastasiei.pdf

Dr. Russell W. Glenn, *Thoughts on ”Hybrid” Conflict”*, https://smallwarsjournal.com/jrnl/art/thoughts-on-hybrid-conflict

Stowell Joshua, *What is Hybrid Warfare?*, https://globalsecurityreview.com/hybrid-and-non-linear-warfare-systematically-erases-the-divide-between-war-peace/

Titus Livius, *Istoria Romei de la întemeierea cetăţii – Enciclopedia înţelepciunii*, Editura Roossa, 2013, https://www.newmoney.ro/

http://www.rador.ro/
https://www.economica.net/
https://adevarul.ro/
https://universul.net/
https://www.defenseromania.ro
https://www.capital.ro/
https://www.eduapps.ro/
https://www.wall-street.ro/
https://www.agerpres.ro/
https://en.wikipedia.org/
https://www.thelocal.de/
https://romanialibera.ro/
https://www.news.ro/
https://islamro.com/
https://monitorulapararii.ro/
https://www.hotnews.ro/
https://www.mediafax.ro/
https://www.digi24.ro/
https://www.consilium.europa.eu/
http://legislatie.just.ro/
https://www.g4media.ro/
https://www.stiripesurse.ro/
https://www.euractiv.ro/
https://www.caleaeuropeana.ro/
http://www.europarl.europa.eu/
https://www.imdb.com/
https://ziaristii.com/
https://www.state.gov/
https://www.nytimes.com/
https://www.ft.com/
https://libra.org/en-US/